

PRIVACIDAD, REEXISTENCIA Y PROCOMÚN FRENTE AL EXTRACTIVISMO DE DATOS PERSONALES

O cómo hacer democracia a través de
tácticas de litigación colectiva y
obfuscación expresiva

Tesis doctoral realizada por:
Fátima Solera Navarro
Tutor y director:
Florencio Cabello Fernández-Delgado

Doctorado en Educación y Comunicación Social
Facultad de Ciencias de la Comunicación
Universidad de Málaga
Marzo 2025

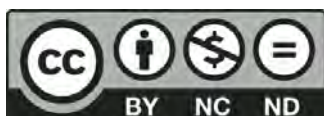


UNIVERSIDAD
DE MÁLAGA

AUTORA: Fátima Solera Navarro

 <http://orcid.org/0000-0002-1389-4889>

EDITA: Publicaciones y Divulgación Científica. Universidad de Málaga



Esta obra está bajo una licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional:

Cualquier parte de esta obra se puede reproducir sin autorización pero con el reconocimiento y atribución de los autores.

No se puede hacer uso comercial de la obra y no se puede alterar, transformar o hacer obras derivadas.

<http://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

Esta Tesis Doctoral está depositada en el Repositorio Institucional de la Universidad de Málaga (RIUMA): riuma.uma.es



DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR

D./Dña FÁTIMA SOLERA NAVARRO

Estudiante del programa de doctorado EDUCACIÓN Y COMUNICACIÓN SOCIAL de la Universidad de Málaga, autor/a de la tesis, presentada para la obtención del título de doctor por la Universidad de Málaga, titulada: "PRIVACIDAD, RESISTENCIA Y PROCOMÚN FRENTE AL EXTRACTIVISMO DE DATOS PERSONALES: O CÓMO HACER DEMOCRACIA A TRAVÉS DE TÁCTICAS DE LITIGACIÓN COLECTIVA Y OFUSCACIÓN EXPRESIVA"

Realizada bajo la tutorización de FLORENCIO CABELLO FERNÁNDEZ-DELGADO y dirección de FLORENCIO CABELLO FERNÁNDEZ-DELGADO (si tuviera varios directores deberá hacer constar el nombre de todos)

DECLARO QUE:

La tesis presentada es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, conforme al ordenamiento jurídico vigente (Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), modificado por la Ley 2/2019, de 1 de marzo.

Igualmente asumo, ante a la Universidad de Málaga y ante cualquier otra instancia, la responsabilidad que pudiera derivarse en caso de plagio de contenidos en la tesis presentada, conforme al ordenamiento jurídico vigente.

En Málaga, a 24 de abril de 2025

Fdo.: FÁTIMA SOLERA NAVARRO Doctorando/a	Fdo.: FLORENCIO CABELLO FERNÁNDEZ-DELGADO Tutor/a
Fdo.: FLORENCIO CABELLO FERNÁNDEZ-DELGADO Director/es de tesis	



UNIVERSIDAD
DE MÁLAGA



Escuela de
Doctorado

AUTORIZACIÓN DE LA TESIS PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR

Yo, FLORENCIO CABELLO FERNÁNDEZ-DELGADO, con DNI [REDACTED], en calidad de tutor y director de la doctoranda FÁTIMA SOLERA NAVARRO, me complazco en AUTORIZAR la presentación de su tesis, titulada “PRIVACIDAD, RESISTENCIA Y PROCOMÚN FRENTE AL EXTRACTIVISMO DE DATOS PERSONALES: O CÓMO HACER DEMOCRACIA A TRAVÉS DE TÁCTICAS DE LITIGACIÓN COLECTIVA Y OFUSCACIÓN EXPRESIVA”, para la obtención del título de doctora por la Universidad de Málaga.

Por la presente, certifico de igual forma que las publicaciones en coautoría que la doctoranda presenta como aval académico de dicha tesis no han sido incluidas en ninguna otra tesis doctoral con carácter previo.

Lo cual firmo para los efectos oportunos, en Málaga, a 24 de abril de 2025.

Fdo.: FLORENCIO CABELLO FERNÁNDEZ-DELGADO
Director y tutor



EFQM



AENOR



Edificio Pabellón de Gobierno. Campus El Ejido.
29071

Tel.: 952 13 10 28 / 952 13 14 61 / 952 13 71 10

E-mail: doctorado@uma.es



UNIVERSIDAD DE MÁLAGA

TESIS DOCTORAL

**Privacidad, res/xistencia y procomún frente al
extractivismo de datos personales:**

**O cómo hacer democracia a través de tácticas de litigación colectiva y
ofuscación expresiva**

*Privacy, res/xistance and commons in the face of
personal data extractivism*

*Or, how to make democracy through tactics of collective litigation and
expressive obfuscation*

Fátima Solera Navarro

Director / Tutor: Florencio Cabello Fernández-Delgado

Programa de Doctorado en Educación y Comunicación Social
Facultad de Ciencias de la Comunicación
Universidad de Málaga

Marzo 2025

Este trabajo (excepto en el caso de las ilustraciones, algunos de cuyos autores establecen condiciones diferentes) se publica bajo los siguientes términos:



Atribución/Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional

Usted es libre de:

1. **Compartir** — copiar y redistribuir el material en cualquier medio o formato
2. **Adaptar** — remezclar, transformar y construir a partir del material
3. La licenciente no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

1. **Atribución** — Usted debe dar crédito de manera adecuada , brindar un enlace a la licencia, e indicar si se han realizado cambios . Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciente.
2. **NoComercial** — Usted no puede hacer uso del material con propósitos comerciales .
3. **CompartirIgual** — Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajo la la misma licencia del original.
4. **No hay restricciones adicionales** — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

Índice de contenido

Resumen	6
Agradecimientos	7
Lista de tablas	8
Lista de figuras	9
Abstract	15
Introducción	22
1. Posicionamiento y diseño de la investigación	27
1.1. Delimitación del foco de estudio: Tácticas de resistencia frente al extractivismo de datos personales	29
1.1.1. Rematerialización de lo digital	30
1.1.2. Un nuevo extractivismo	39
1.1.3. El concepto de dato personal	42
Datos personales como materia prima	43
Datos personales como trabajo	43
Datos personales como infraestructura	44
1.1.4. Prácticas de resistencia	45
1.1.5. Ofuscación	48
1.2. Preguntas de partida y objetivos	50
1.3. Posicionamiento de la investigación	51
1.4. Diseño metodológico	56
1.4.1. Situaciones de conocimiento	56
1.4.2. Revisión bibliográfica	61
1.4.3. Estudios de caso	64
Selección de los casos de estudio	64
Técnicas de investigación empleadas y análisis de la información obtenida	67
1.4.4. Investigación-Acción Participativa. IAP	70
1.5. Estructura de la investigación	72
2. Marco teórico: Extractivismo de datos personales	73
2.1. Situando la vigilancia	75
2.1.1. Breve historia del origen de la vigilancia	76
Los primeros censos	76
El libro de Domesday	77
Las revoluciones campesinas en la Baja Edad Media europea	78
Algunas conclusiones sobre los orígenes de la vigilancia	81
2.1.2. Vigilancia en la época moderna	83
La creación del ejército moderno	83
El disciplinamiento de los cuerpos	86
El nacimiento del Estado nación: la burocracia	90
El control de la movilidad de la población	93
El registro: de la descripción a la biometría	95
La estadística como forma de control social	98
La vigilancia en el entorno laboral	102

<u>La vigilancia dentro del Estado de bienestar</u>	106
<u>Algunas conclusiones sobre la vigilancia moderna</u>	109
<u>2.1.3. Vigilancia digital y Sociedad de la Información</u>	112
<u>De la vigilancia moderna a la posmoderna</u>	113
<u>Marketing y Consumo: la clasificación social</u>	116
<u>La digitalización de la información</u>	120
<u>El papel de la vigilancia en la concepción de Internet</u>	123
<u>De la Digitalización a la Datificación</u>	130
<u>Abrazando al Gran Hermano</u>	134
<u>Las revelaciones de Snowden</u>	141
<u>La Era del Capitalismo de la Vigilancia</u>	144
<u>La pandemia de la COVID-19: un giro epidemiológico en la vigilancia digital</u>	152
<u>Algunas conclusiones sobre la vigilancia digital</u>	155
<u>2.2. Situando la privacidad</u>	159
<u>2.2.1. El valor de la privacidad</u>	161
<u>El control sobre la autopresentación</u>	163
<u>Reputación</u>	164
<u>Autonomía</u>	165
<u>Creatividad</u>	167
<u>Seguridad</u>	168
<u>Igualdad, justicia y bienestar</u>	169
<u>Democracia</u>	170
<u>Conclusiones sobre el valor de la privacidad</u>	171
<u>2.2.2. Cómo se ha conceptualizado la privacidad a lo largo del tiempo</u>	172
<u>El derecho a ser dejado en paz</u>	175
<u>La privacidad como un acceso limitado a uno mismo</u>	176
<u>La privacidad como secreto</u>	177
<u>El control sobre la información personal</u>	178
<u>Privacidad como forma de proteger la personalidad</u>	180
<u>Privacidad como intimidad</u>	181
<u>Conclusiones sobre los intentos de conceptualizar la privacidad</u>	181
<u>2.2.3. Taxonomía de la privacidad</u>	183
<u>Recopilación de la información</u>	187
<u>Procesamiento de la información</u>	189
<u>Diseminación de la información</u>	195
<u>Invasión de la privacidad</u>	200
<u>Conclusiones sobre la taxonomía de la privacidad</u>	203
<u>2.2.4. Privacidad como integridad contextual</u>	205
<u>2.3. De las sociedades de control al extractivismo de datos personales</u>	208
<u>2.3.1. Sociedades de control</u>	209
<u>2.3.2. El doble de datos</u>	212
<u>Imagen de Datos</u>	212
<u>Persona digital</u>	214
<u>Dobles de Datos</u>	215
<u>2.3.3. Servidumbre maquínica</u>	216
<u>Confesión maquínica</u>	218
<u>2.3.4. Datos y metadatos</u>	221
<u>“Datos en bruto” como oxímoron</u>	222

<u>Ir más allá: metadatos</u>	222
<u>Vigilancia maquina</u>	225
<u>2.3.5. Extractivismo de datos personales</u>	227
<u>2.4 Desimplantar Matrix de la matriz</u>	233
<u>2.5. ¿Cómo respondemos al extractivismo de datos personales?</u>	260
<u>2.5.1. Modos de hacer</u>	262
<u>Estrategias y tácticas</u>	262
<u>2.5.2. Formas de resistencia al extractivismo de datos</u>	264
<u>El intercambio de tarjetas de fidelidad de los supermercados</u>	266
<u>Resistencia en la economía de plataforma</u>	267
<u>Data fandom y Fan activism</u>	269
<u>2.5.3. Tácticas de resistencia contra el extractivismo de datos personales</u>	271
<u>3. Tácticas de litigación colectiva por la privacidad en la UE: NOYB y el marco europeo de protección de datos personales</u>	277
<u>3.1. Breve recorrido sobre la legislación en la UE en materia de protección de datos</u>	279
<u>3.1.1. La Declaración Universal de los Derechos Humanos</u>	282
<u>3.1.2. El Convenio Europeo de Derechos Humanos</u>	282
<u>3.1.3. El Convenio 108</u>	283
<u>3.1.4. La Directiva 95/46/CE: Directiva sobre protección de datos</u>	284
<u>3.1.5. Decisión 2000/520/CE: Puerto Seguro</u>	284
<u>3.1.6. El Reglamento (CE) nº 45/2001</u>	285
<u>3.1.7. La Directiva 2002/58/CE</u>	285
<u>3.1.8. La Directiva 2006/24/CE</u>	286
<u>3.1.9. La Carta de Derechos Fundamentales de la Unión Europea</u>	287
<u>3.1.10. El Tratado de Funcionamiento de la Unión Europea</u>	287
<u>3.1.11. Asunto C-131/12 : El derecho al olvido</u>	288
<u>3.1.12. Asunto C-362/14: Schrems I</u>	289
<u>3.1.13. Reglamento (CE) 2016/679: Reglamento General de Protección de Datos</u>	290
<u>3.1.14. Asunto C-311/18: Schrems II</u>	291
<u>3.1.15. Reglamento (UE) 2022/1925: Reglamento de Mercados Digitales</u>	291
<u>3.1.16. Reglamento 2024/1689: AI Act</u>	293
<u>3.2. NOYB (None of Your Business)</u>	295
<u>3.2.1. Quiénes son</u>	295
<u>3.2.2. Cómo trabajan</u>	298
<u>3.2.3. Proyectos</u>	300
<u>Transferencia de datos entre la UE y EEUU</u>	300
<u>Elaboración de perfiles y toma de decisiones automatizada</u>	301
<u>Seguimiento en línea y móvil</u>	302
<u>Identificación y autenticación</u>	304
<u>Seguridad de los datos</u>	304
<u>Calificación crediticia</u>	305
<u>Derechos de los titulares de los datos</u>	305
<u>Consentimiento forzado y omisión del consentimiento</u>	306
<u>Microsegmentación política, manipulación y seguimiento</u>	307
<u>Procedimientos administrativos nacionales e inactividad de las APD</u>	308
<u>Publicidad en línea</u>	308

<u>Datos biométricos</u>	308
<u>Inteligencia Artificial</u>	309
<u>Banners de cookies</u>	310
<u>Pay or Okay</u>	310
<u>3.2.4. GDPRhub</u>	313
<u>4. Tácticas de acción directa y expresiva frente al extractivismo de datos personales: Ofuscación como generación de ruido para vencer a la vigilancia digital</u>	315
4.1. Antecedentes históricos.....	317
4.2. Clasificación y casos.....	325
4.2.1. Ofuscación temporal.....	326
4.2.2. Ofuscación cooperativa.....	329
4.2.3. Ofuscación selectiva.....	333
4.2.4. Ofuscación por ambigüación.....	348
4.2.5. Tabla resumen de clasificación ejemplos de ofuscación.....	364
4.3. La dimensión expresiva de la ofuscación.....	367
<u>5. Tácticas recursivas para una democracia participativa: Ofuscación selectiva como generación de un procomún de datos a través de Decidim</u>	371
5.1. Qué es Decidim.....	373
5.1.1. Imaginar colectivamente la ciudad.....	373
5.1.2. Pensar colaborativamente los procesos de participación democrática.....	374
5.2. Cómo funciona.....	376
5.2.1. Articulación de la plataforma.....	376
5.2.2. Gobernanza: Decidir recursivamente Decidim.....	381
5.3. Privacidad y ofuscación selectiva para un procomún de datos a través de Decidim.....	387
5.3.1. Privacidad por diseño.....	387
5.3.2. Plan de Privacidad de Decidim.....	388
5.3.3. El proyecto DECODE y el caso del piloto Democracia Digital y Datos Comunes (DDDC).....	390
El proyecto DECODE.....	390
Democracia Digital y Datos Comunes (DDDC): la intersección entre DECODE y Decidim.....	394
Conclusiones en torno a la implementación de DECODE.....	398
5.4. Debates acerca de la privacidad y la protección de datos en Metadecidim.....	400
5.5. Contribuciones de Decidim al procomún.....	405
<u>6. Decidimos Educación Inclusiva</u>	409
6.1. Movimiento Quererla es Crearla y proyectos de investigación por la educación inclusiva.....	411
6.1.1. Quererla es Crearla.....	412
6.1.2. Proyecto de investigación “Narrativas emergentes para la construcción de escuelas inclusivas”.....	419
6.1.3. Por qué un Decidim para Quererla es Crearla.....	421
6.2. Cómo hacer un Decidim para Quererla es Crearla.....	426
6.3. Cómo nos organizamos.....	430

6.3.1. Cómo hemos articulado la plataforma	430
6.3.2. Primera gran prueba: el Workshop Cataliza 2024	431
6.4. Reflexiones sobre un proceso en marcha	439
Conclusiones	441
Conclusiones	443
Conclusions	458
Bibliografía	471
Bibliografía	473
Anexos	507
Anexo I: Transcripción de la entrevista a Martín Nadal	509
Anexo II: Acta charla Obfuscation is dead? Long Live Obfuscation!	522

Resumen

El presente trabajo aborda la relación entre privacidad y procomún a través de diferentes resistencias y reexistencias al extractivismo (material y de datos) imperante. Para ello he situado histórica y teóricamente los conceptos de vigilancia y privacidad para después avanzar hacia las relaciones entre las personas y la tecnologías mediadas por la vigilancia digital dentro de las sociedades de control, hasta el desarrollo teórico concreto del extractivismo de datos personales. A modo de digresión, este estudio incluye un caso que sirve para ilustrar de manera encarnada cómo a través de la intersección entre acecho legal y tecnológico a los cuerpos gestantes, podemos abordar el conflicto al que nos enfrentamos en relación a la salvaguarda tanto de nuestros datos personales como de nuestras interacciones. Dicha digresión sirve de enlace hacia el estudio teórico de cómo respondemos al extractivismo de datos personales, que luego da pie a los diferentes estudios de casos de carácter más exploratorio: las tácticas de litigación colectiva del centro europeo de derechos digitales NOYB y el marco de la regulación de la protección de datos personales en la UE; las tácticas de ofuscación que buscan generar ruido para vencer al extractivismo de datos; y Decidim como iniciativa para trascender las prácticas extractivistas a través de una plataforma basada en *software* libre para las prácticas democráticas participativas. Por último, como acción propositiva de cómo es posible integrar Decidim en un proyecto de investigación comprometido con la Investigación-Acción Participativa, emerge el último capítulo titulado *Decidimos Educación Inclusiva*.

This doctoral thesis addresses the relationship between privacy and the commons through different resistances and re-existences to the prevailing (material and data) extractivism. To this end, I have historically and theoretically situated the concepts of surveillance and privacy and then moved toward the relationships between people and technologies mediated by digital surveillance within societies of control, leading to the concrete theoretical development of personal data extractivism. As a digression, this study includes a case that serves to illustrate in an embodied way how, through the intersection of legal and technological stalking of gestating bodies, we can address the conflict we face in relation to the safeguarding of both our personal data and our interactions. This digression serves as a link to the theoretical study of how we respond to personal data extractivism, which then gives rise to the various more exploratory case studies: the collective litigation tactics of the European Center for Digital Rights NOYB and the framework of personal data protection regulation in the EU; the obfuscation tactics that seek to generate noise to defeat data extractivism; and Decidim as an initiative to transcend extractivist practices through a free software-based platform for participatory democratic practices. Finally, as a proactive action on how it is possible to integrate Decidim into a research project committed to Participatory Action Research, the final chapter, entitled "Decidimos Educación Inclusiva", emerges.

Agradecimientos

Este trabajo no hubiese sido posible sin muchas personas que, de un modo u otro, han colaborado en él, por lo que quisiera expresar aquí mi más sincero agradecimiento:

A Dani, mi compañero de vida, por motivarme a dar este paso, acompañarme y alentarme en el camino; y a mi madre, padre, hermana y hermanos, por su incondicional apoyo, gracias a todos por sostenerme y ser siempre mi lugar seguro.

A mi director, tutor y principalmente amigo, Floren, por todas las horas de dedicación, trabajo y debate, pero sobre todo, por siempre insuflarme optimismo, seguridad y energía en cada etapa de este viaje.

A Miguel (Rey) por su amistad y por siempre mantener el interés con cada caso nuevo de ofuscación que descubría, gracias también por ponerme en alerta sobre los debates en torno a las aplicaciones de control de ciclo en EEUU en junio de 2022 y por regalarme la idea para el título de “Desimplantar matrix de la matriz”.

A mis compañeras y compañeros del Proyecto de Investigación y de Quererla es Crearla, especialmente a Tere, Nacho, Luz, Marina y Mariana; y a los Pokecode, Iván y Pau, por hacer posible *decidimoseducacioninclusiva.uma.es*.

Gracias también a Carol por acogerme y enseñarme el lado más humano de Decidim; a Sergio Salgado por ponernos tras la pista del concepto de ofuscación; a Birgit por recibirme en Viena con los brazos abiertos y a Adam Harvey por tan fructíferas conversaciones que me permitieron desarrollar nuevos enfoques para esta investigación.

Por último, quisiera agradecer también su trabajo a los miembros del tribunal y a los evaluadores externos, así como a todo aquel que dedique su tiempo a leer esta tesis.

Lista de tablas

- **Tabla 1.** Tabla descriptiva de las 6 *apps* de control de ciclo menstrual estudiadas
- **Tabla 2.** Tabla analítica de información recopilada por las 6 *apps* de control de ciclo menstrual estudiadas
- **Tabla 3.** Recopilación de ejemplos de ofuscación
- **Tabla 4.** Tabla representativa de qué componentes pueden ir en cada espacio de Decidim
- **Tabla 5.** Tabla representativa de qué funciones tiene cada componente
- **Tabla 6.** Tabla representativa de qué acciones puede realizar cada participante
- **Tabla 7.** Tabla representativa de qué funciones tiene cada tipo de administradora
- **Tabla 8.** Resumen de las propuestas de nuevas funcionalidades relacionadas con la privacidad y/o la protección de datos
- **Tabla 9.** Panorámica de la ecología institucional de Decidim basada en las 3 capas que distingue Benkler (2006/2015, p. 449)

Lista de figuras

- **Figura 1.** Captura de pantalla de la web CloudMap
- **Figura 2.** Captura de pantalla de la web Submarine Cable Map
- **Figura 3.** Mapa de la cadena de suministro de la IA a través de los datos de NVIDIA
- **Figura 4.** Captura de pantalla del sitio *web* <https://carbolytics.org/web2x/>
- **Figura 5.** Ejemplo de información que aporta el sitio *web* <https://carbolytics.org/web2x/> sobre la huella de carbono que produce una *cookie*
- **Figura 6.** Diseño del panóptico de Bentham
- **Figura 7.** Esquema de la taxonomía de la privacidad de Solove (2009)
- **Figura 8.** Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Recopilación de la Información”
- **Figura 9.** Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Procesamiento de la información”
- **Figura 10.** Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Difusión de la información”
- **Figura 11.** Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Invasión de la privacidad”
- **Figura 12.** Mapa de las políticas sobre el aborto en EEUU a 9 de junio de 2022
- **Figura 13.** Mapa de las políticas sobre el aborto en EEUU *post* «*Roe vs. Wade*», a 24 de junio de 2022
- **Figura 14:** Neff, Gina. [@ginasue]. (2022, 24 de junio). *Right now, and I mean this instant, delete every digital trace of any menstrual tracking. Please.* [Tuit]
- **Figura 15:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Now that I have your attention: we have work to do. A* □ [Tuit]
- **Figura 16:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Americans lack fundamental privacy protections. Post-Roe makes that tragically clear. For many women, post-Roe privacy is more urgent. But privacy*

is even more important for ALL of us now. [Tuit]

- **Figura 17:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *“I don’t have anything to hide.” Post-Roe, you do. The Supreme Court has just made it clear that they consider that the Constitution does not guarantee rights to privacy. That should scare us ALL into action.* [Tuit]
- **Figura 18:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Here’s what you can do: 1) Pay attention to your apps. They are an easy target, and they affect many of us. What are their data policies? How are companies protecting their users? What are their data retention policies? What do app companies do with law enforcement subpoenas?.* [Tuit]
- **Figura 19:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Apps help us live better lives. I get that. (I co-wrote a book about that). But we should be able to balance risks and benefits on the things that help us keep track. Don’t give up, demand better!* [Tuit]
- **Figura 20:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Many apps collect data that can say intimate things about our health, but that data is not yet protected under US health privacy laws. Don’t give up, demand a policy fix for this gap! And don’t stop there.* [Tuit]
- **Figura 21:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Law enforcement agencies have already targeted Google searches for “abortion pills”, text messages, and DNA databases (Hello 23andMe! And <http://Ancestry.com>) in prosecuting women for abortions and miscarriages.* [Tuit]
- **Figura 22:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Big Tech is guilty too: The FTC recently called out Verizon, T-Mobile, Comcast Xfinity, Charter Spectrum, AT&T and Google Fiber— who provide 98% of the US mobile internet! — for collecting vast troves of personal data, not telling users, and failing to give them any real choice.* [Tuit]
- **Figura 23:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *So...* [Tuit]
- **Figura 24:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *2) Up your personal privacy game. One place to start is @Info_Activism’s “Security in a Box” <https://securityinabox.org/en/> Protect your communications, your passwords, your devices, your files.* [Tuit]
- **Figura 25:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Loads of handy tips online for smarter personal information security to protect you and your loved ones. We should not stop there — demand better from the companies you use and from our law makers. We deserve privacy! But don’t stop there.* [Tuit]
- **Figura 26:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Life in post-Roe America will be harder for*

poor women, Black women, Hispanic women, immigrant women, underage women, raped women, women in crisis.... I could go on and on. Deleting an app doesn't fix that cold and cruel reality. [Tuit]

- **Figura 27:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *3) Support the people and organizations supporting women.* [Tuit]
- **Figura 28:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *There are many great organizations working on national policy. Support them, they deserve our help. But I'd like to highlight just a few groups who are doing work on the ground with women in states with the most restrictive anti-abortion laws.* [Tuit]
- **Figura 29:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Close to my Appalachian heart, Holler Health Justice, @HollerHealth a BIPOC- & queer-led racial, economic & reproductive justice nonprofit in West Virginia.* [Tuit]
- **Figura 30:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *The Kentucky Health Justice Network builds the power of Kentuckians to achieve reproductive justice through direct support, education and outreach.* <https://kentuckyhealthjusticenetwork.org>. [Tuit]
- **Figura 31:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Texas Equal Access Fund @TEAFund, "making reproductive rights a reality", has been providing direct support in Texas. They are pausing their direct services for the moment, but are still very much in the fight for access to abortion for all.* [Tuit]
- **Figura 32:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *The Afiya Center @TheAfiyaCenter "Transforming the lives, health, and overall wellbeing of Black womxn and girls by providing refuge, education, and resources"* [Tuit]
- **Figura 33:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *The Midwest Access Coalition @MidwestAccess helps people traveling to, from, and within the Midwest access a safe, legal abortion with support in travel coordination and costs, lodging, food, medicine, and emotional support.* [Tuit]
- **Figura 34:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Local support is not enough, though. Don't stop there!* [Tuit]
- **Figura 35:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *4) Let's get our bodies back. There's work to be done and many more fights to fight for social and reproductive justice.* [Tuit]
- **Figura 36:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Reproaction @reproaction leads bold action to increase access to abortion and advance reproductive justice.* [Tuit]
- **Figura 37:** Neff, Gina. [@ginasue]. (2022, 26 de junio). *Finally, this is not an abstract problem. Or*

- even a technology problem (even though that's my lane, and what led to this tweet blowing up)....* [Tuit]
- **Figura 38:** Neff, Gina. [@ginasue]. (2022, 26 de junio). 5) *Take care of each other. That is one of the most feminist and radical things that we can do. There's no app for that.* [Tuit]
 - **Figura 39.** Mapa de las políticas sobre el aborto en EEUU *post* «*Roe vs. Wade*» a 25 de abril de 2024
 - **Figura 40.** Mapa de las políticas sobre el aborto en EEUU *post* «*Roe vs. Wade*» a 18 de febrero de 2025
 - **Figura 41.** Evolución histórica de la legislación en materia de protección de datos en la UE
 - **Figura 42.** Capturas de pantalla de la página de inicio de <https://gdprhub.eu/> y de la página de la base de datos de decisiones de GDPRhub https://gdprhub.eu/index.php?title=Advanced_Search
 - **Figura 43.** Barco de vapor *West Mahomet* con camuflaje disruptivo (1918)
 - **Figura 44.** Reflectores antirradar desplegados desde un bombardero de la RAF Lancaster
 - **Figura 45.** *Cyclosa mulmeinensis*
 - **Figura 46.** Anti-Paparazzi Clutch Prototype
 - **Figura 47.** *Wearable face projector* de Jing-Cai Liu
 - **Figura 48.** Representación gráfica de los nodos de *Tor*.
 - **Figura 49.** Imágenes del proyecto *Facial Weaponization Suite* de Zach Blas
 - **Figura 50.** Arquitectura de *FaceCloak*
 - **Figura 51.** Aspecto original *CV Dazzle* para su exposición en el máster de la Universidad de Nueva York.
 - **Figura 52.** CV Dazzle Look para DIS Magazine
 - **Figura 53.** Evaluación de prominencia de la sesión fotográfica *Op-Art* del *New York Times*.
 - **Figura 54.** *Anti-Drone Hijab*, pieza de la colección *Stealth Wear*
 - **Figura 55.** *HyperFace* de Adam Harvey para *Hyphen-Labs*
 - **Figura 56.** Ejemplo de cómo funciona *Adversarial Fashion* con un lector de matrículas

- **Figura 57.** Ejemplo de cómo funciona *Realface Glamouflage*
- **Figura 58.** *CHBL Jammer Coat* desarrollado por los arquitectos de la firma COOP HIMMELB(L)AU
- **Figura 59.** Captura de pantalla de la página de inicio de *FangøCam*
- **Figura 60.** Presentación de FangøCam por Martín Nadal en el Worklab 2023 en mur.at.
- **Figura 61.** Muestra de cómo funciona *Glaze*
- **Figura 62.** Imágenes generada a partir de diferentes indicaciones por un modelo SD-XL donde el concepto “perro” está “envenenado” por el empleo de *Nightshade*
- **Figura 63.** Captura de pantalla del panel de control de *TrackMeNot*
- **Figura 64.** Captura de pantalla de la visualización de la extensión AdNauseam cuando navegas una página con publicidad
- **Figura 65.** Captura de pantalla de mi página de estadísticas de *AdNauseam* de los últimos tres meses
- **Figura 66.** Captura de pantalla de la página del proyecto
- **Figura 67.** Imágenes de exposiciones de *Fangø*
- **Figura 68.** Ejemplo de cómo funciona *URME Surveillance*
- **Figuras 69 y 70.** Ejemplos de cómo funcionan *URME Paper Surveillance Mask* y *URME Facial Video Encryptor*
- **Figura 71.** Captura de pantalla de *ScareMail* agregando texto a un correo electrónico en Gmail.
- **Figura 72.** Ubicaciones de los grupos de datos para la suplantación de geolocalización de Wi-Fi del proyecto *Data Pools*
- **Figura 73.** DataPools en la exposición en Tropez. Muestra de cómo el móvil te localiza en la casa de Jeff Bezos en Beverly Hills
- **Figuras 74 y 75.** Ejemplos de cómo funciona Vortex
- **Figura 76.** Capturas de pantalla del proyecto BCNOW
- **Figura 77.** Resumen del proceso DDDC

- **Figura 78.** Esquema de integración técnica del DDDC
- **Figura 79.** Captura de pantalla del mensaje que aparece a la hora de crear una cuenta en Decidim
- **Figura 80.** Capturas de pantalla del apartado de configuración de privacidad y mensaje de consentimiento
- **Figura 81.** Captura de pantalla del *Peertube* de QeC: <https://creemoseducacioninclusiva.uma.es/>
- **Figura 82.** Captura de pantalla de la página de inicio de <https://creemoseducacioninclusiva.com/>
- **Figura 83.** Captura de pantalla de la caja de idiomas del pie de página de <https://decimoseducacioninclusiva.uma.es/>
- **Figura 84.** Captura de pantalla de la página de inicio de <https://decimoseducacioninclusiva.uma.es/>
- **Figura 85.** Horarios del *Workshop Cataliza* 2024
- **Figura 86.** Videos testimonios de América Latina para QeC
- **Figura 87.** Captura de pantalla de los diferentes tipos de inscripción en el *Workshop Cataliza*
- **Figura 88.** Captura de pantalla de a inscripción *online* en el *Workshop Cataliza*

Abstract

Perfluorooctanoic acid (PFOA), also known as C8 or perfluorooctanoate, is a synthetic compound consisting of long carbon chains to which fluorine atoms are strongly bonded (Perfluorooctanoic Acid, 2024). Thanks to its composition, PFOA has surfactant properties, as it reduces the surface tension of water. This is why this waterproofing compound has been used in a variety of consumer products, such as coatings for eyeglasses and tennis rackets, stain-resistant coatings for carpets and furniture, firefighting foam, fast-food wrappers, communication cables, pizza boxes, etc. However, perhaps its most famous use is as a coating for non-stick pans made with Teflon™, the brand name for this compound.

So far, everything indicates that we are talking about a great compound, with extraordinary benefits for our daily lives, as no one wants to have their omelet stick in our pan or to spend a lot of time and effort removing a stain from our carpet. However, another quality of PFOA is that it does not degrade, so it remains in our bodies and the environment indefinitely.

As cited in a World Wildlife Fund's (WWF) article, wherever scientists have looked for the presence of PFOA, they have found it. This compound is found in the vital organs of the Atlantic salmon, gray seals, Alaskan polar bears, sea turtles, eagles, and the bald eagles of the American Midwest, as well as in the vast majority of humans. In addition, I must highlight that various studies (Tudela and Delgado, 2025) have confirmed that PFOA acts as an endocrine disruptor, limiting the effects of hormones. This is why it is associated with different types of cancer, thyroid problems, and infertility in both humans and animals. In response to the slogan of a certain brand of frying pans: no, nobody lacks Teflon in their body.

We could be talking about yet another element that, over time, we have discovered to be seriously harmful to health and the ecosystem. However, thanks to the reports published by Natalie Rich (2016) in *The New York Times*, which served as the script for 'Todd Haynes' (2019) film *Dark Waters*, and by Sharon Lerner in *The Intercept*, the general public has been able to discover that PFOA is a story of knowledge, concealment, and power in favor of the economic profit of an American industrial giant, the chemical company DuPont.

This story begins in 1951 when DuPont began purchasing PFOA from the multinational 3M for its use in the manufacture of Teflon. Although the U.S. government did not classify PFOA as a hazardous substance, 3M sent DuPont a series of recommendations on how to dispose of it: it could be

incinerated or sent to a chemical waste facility, but it was clearly specified that it should not be dumped into surface waters or sewers.

Despite that fact, over the following decades, DuPont pumped vast amounts of PFOA dust into the Ohio River through the sewer pipes at its facility in Parkersburg, West Virginia (where the company was located). It also dumped 7,100 tons of PFOA-laced sludge into unlined open wells on their property, from where the chemical could seep directly into the ground. As a result, PFOA reached the groundwater that supplied drinking water to more than 100,000 people in total.

What is more, for decades DuPont also tried to hide its actions, knowing the material was harmful but dumping it into the water anyway. They certainly knew this because as early as the 1960s, their researchers had discovered that the chemical could increase liver size in rats and rabbits. In the 1970s, DuPont discovered high concentrations of the substance in the blood of its factory workers. And in 1981, 3M, which remained the supplier of PFOA to DuPont and other companies, discovered that ingesting the substance caused birth defects in rats. After 3M shared this information, DuPont tested it on their pregnant employees in their Teflon division, resulting in two out of seven births with eye defects. However, they never made any of these threatening findings public.

If DuPont has been able to get away with it all this time, it is because for decades, such corporations have relied on the erroneous public perception that if some chemical was dangerous, it was regulated. Under the Toxic Substances Control Act of 1976, the US Environmental Protection Agency (EPA) could report hazardous chemicals only when it had been provided with evidence of harm. This arrangement, which has largely allowed chemical companies to regulate themselves, is the reason the EPA has restricted only five chemicals out of the tens of thousands on the market over the past 40 years.

Thus, had it not been for the meticulous work of the attorney Rob Bilott, who decided to take on the case of Wilbur Tennant, a farmer whose land bordered the DuPont landfill and whose cows were dying under mysterious circumstances due to high concentrations of PFOA in the stream where his animals drank, we might never have learned the truth about this story. We would still be cooking on surfaces that are potentially toxic, especially for our aquifers and for the people exposed to it during its (thermally and legally self-regulated) manufacturing. Although this case concluded with an out-of-court settlement, the details of which have not been revealed, it led to another lawsuit in which, in August 2001, around 70,000 people, represented by Bilott, joined together to file a class-action against DuPont for contaminating the water they used, which came from the same plant, with PFOA (Tudela and

Delgado, 2025).

However, the story does not end there. Although the EPA negotiated with 3M in 2000 to stop producing these compounds, according to its 2023 corporate report (cited in Tudela and Delgado, 2025), manufacturing did not cease until 2002 in the US and 2008 in the rest of the world. 3M was also sued by the State of Minnesota for contamination of groundwater, surface water, fish, and other aquatic organisms, in addition to soil. In the first quarter of 2018, 3M reached an out-of-court settlement totaling \$897 million to resolve the matter. And in June 2023, the same company reached another agreement with plaintiffs in a class-action lawsuit to address a series of claims from several water utilities in hundreds of locations across the US. This agreement stipulates the allocation of more than \$10.5 billion for those who identify PFAS (per- and polyfluoroalkyl substances, including the aforementioned PFOA) in their drinking water sources between 2023 and 2036 (Tudela and Delgado, 2025).

In the case of the European Union (EU), this compound began to be used for household products in the 60s and it was not banned until 2020, thanks to the approval of Commission Regulation (EU) 2017/1000 of June 12, 2017. However, the individual ban of each compound has represented a significant achievement for the industry. According to data collected by Tudela and Delgado (2025), today there are still more than 10,000 varieties of PFAS on the market, and only by the end of 2022, and after several lawsuits, 3M announced that it would suspend the production of all PFAS by the end of 2025, although its reports indicate that this will not prevent its use of PFAS from other sources where there are no viable alternatives.

In Spain, despite not having PFAS factories thanks to a limited but highly relevant biomonitoring study carried out by a group of scientists led by the researcher Argelia Castaño, it was possible to confirm a 100% presence of PFOA in the samples analyzed (Tudela and Delgado, 2025). And at the beginning of 2025, another larger study with a sample of 3,800 participants from the Spanish population was announced with the aim of analyzing blood and urine in search of the hazardous chemicals accumulated in the body: «heavy metals, polycyclic aromatic hydrocarbons, PCBs, Bisphenols, dioxin, sacrolein, pesticides, and at least 12 PFAS» (Tudela Delgado, 2025).

As a result, we are now more aware of the environmental pollution produced by the chemical industry, which has become a major concern due to its significant impact on human health and the environment, especially on air and water quality. In contrast, new forms of pollution have proliferated in recent years that perhaps go more unnoticed. I am referring to pollution from digital services, which refers to the

negative impact of ICTs and the Internet, stemming from the management of electronic waste from obsolete devices and, above all, from the high energy and water consumption of data centers to power and cool the servers where massive amounts of information are stored and processed. This also contributes to carbon emissions and exacerbates the climate change.

What connects each of these stories is the desire for self-regulation of companies operating in both sectors. I have already discussed how the EPA in the US left the responsibility of reporting toxic substances to the companies that manufactured them, and the terrible results caused by this (in)action. But in the case of large companies in the digital environment (Meta, Google, Amazon, and Apple), the first attempt to regulate them in the US did not come until 2020 (Pérez Colomé, 2020), although deliberations focused more on the power of these companies as oligopolies than on the risks of excessive processing of the personal data they host and the resulting privacy risks.

For law professor Frank Pasquale (cited in Zuboff, 2019/2020, p. 152), this advocacy of self-regulation is a legacy of neoliberalism, giving rise to an approach that views privacy as a competitive value and assumes that users opt only for those services that provide them with the desired level of privacy. It is from this legacy that the notice and consent model is viewed favorably because it is believed to allow each person to clearly and thoroughly express their privacy preferences. In short, by treating privacy individually, we are forced to seek equally individual solutions.

But what if all this is not as it seems? In my thesis, far from defeatist perspectives, I aim to show how citizens are uniting from different axes —such as the legal framework, art and activism (both analogue and digital), or the development of alternative democratic platforms— to search for solutions that will enable us to resist and re-exist in a less aggressive and damaging way in the times in which we currently live. So this research has an expressive purpose, the primary goal of which is to highlight the active and collective defense of privacy against the tools of personal data extraction.

It is also important to note that this study is framed within the conceptual framework provided by Certeau (1990), which indicates that it is a mistake to assume that users are passive bodies that voluntarily abide by established rules. Therefore, I consider it appropriate to focus on everyday practices to discover how people operate, and how they behave in the face of power strategies, rather than focusing on technology as an abstract, depoliticized, and disembodied entity. To approach this dilemma from as global a perspective as possible, I begin with the framework of the four regulators (laws, social norms, markets, and technological architectures) referred to by Lawrence Lessig (2006/2009) in his studies on privacy.

The approach I adopt throughout this research is disciplinarily pluralistic, incorporating knowledge and ideas from diverse fields such as sociology, computer science, political science, law, and philosophy. However, rather than resulting in a discordant cacophony of divergent perspectives, this path has been theoretically fruitful and analytically complementary, providing me with insights from diverse perspectives that, while not always connected, have been interwoven throughout these lines thanks to a series of common threads that have articulated this study.

Along with this, I am always guided by Haraway's (1991/1995) epistemology of situated knowledge, where feminist objectivity addresses limited location and situated knowledge, not the transcendence and unfolding of subject and object. As well as the feminist standpoint theory, originally proposed by Nancy Hartsock (1983a; 1983b). The other thread that runs through and articulates the research is based on the postulates of Langdon Winner (1985) on the controversies about technology and society, more specifically, on whether technical artefacts have political qualities, complemented by the thesis of Judy Wajcman (2004/2006) that within the political qualities of artefacts we must pay attention specifically to their gender politics.

Based on all of the above, the general objective of this research is to analyze the tactics of resistance to data extractivism that emerge from citizens, that is, those who must navigate a space that is not their own, but who nevertheless invent different responses from different perspectives, such as legal, technological, or political.

But to achieve this goal, we must address a series of more specific objectives, such as delving into historical and theoretical understandings of surveillance and privacy and examining how the advent of digitalization has affected these concepts and, by extension, us as well. To this end, it is necessary to recognize the potential risks generated by the intersections between norms and technology, as well as to investigate how we respond to this extraction of personal data, without neglecting the reflection that the actors themselves—developers and collaborators—of these responses carry out and the consequences that their use entails for them.

In line with the research positioning, the research design emerges to access the necessary information to address the objectives proposed. Thus, I have chosen to begin with a narrative about how the determination to place the body in geographical spheres where a series of activities related to my focus of study took place led me to approach the research from an eminently qualitative perspective, which would have been impossible without having the opportunity to conduct this study in such a face-to-face manner. Therefore, in my opinion, it is essential to address the material conditions under which I

conducted this study, understanding that they have had a considerable impact on my work. Another consideration for developing the methodological strategy has to do with the combination of theory—primarily critical—and the chosen practices—of resistance—with which I establish an ongoing dialogue.

Hence, this study is divided into six chapters, plus the introduction and conclusions. The first Chapter deals with the research positioning and design. I have included the following: a delimitation of the focus of the study, which addresses recent studies related to extractivism (material and data) as well as its counterpart linked to various resistance tactics, and then concludes by explaining obfuscation, the concept with which I began to approach this work. After this delimitation, I proceed to develop the initial questions and objectives proposed, the positioning on which I base my research, its methodological design, and the analysis of the data obtained from this positioning.

The second Chapter corresponds to the theoretical framework of the research, which begins by historically and theoretically situating the concepts of surveillance and privacy and then moves on to the relationships between people and the technologies mediated by digital surveillance within control societies, leading to the theoretical development of so-called personal data extractivism. Following these inquiries, I include a section titled 2.4. *Desimplantar Matrix de la matrix* (*Deimplant Matrix from the matrix*) as a digression to illustrate in an embodied way how, through the intersection of legal and technological stalking of gestating bodies, we can address the conflict we face daily regarding the safeguarding of both our personal data and our interactions. This digression also serves as a link to the theoretical study of how we respond to personal data extractivism that culminates this chapter and leads to the more exploratory subsequent chapters on practical cases. Thus, chapters three, four, and five correspond to the case studies previously explained:

Chapter 3 is dedicated to the legal response and the study of NOYB and the framework for personal data protection regulation in the EU. NOYB is a non-profit organization based in Vienna, Austria, established in 2017 with a pan-European focus. Co-founded by Austrian lawyer and privacy activist Max Schrems, NOYB's mission is to promote both tactical class litigation (Cabello, 2024, p. 968) and media initiatives in support of the General Data Protection Regulation (GDPR). While many privacy protection organizations focus their attention on governments, NOYB focuses on privacy issues and their potential violations by the private sector. The NOYB group represents a unique example, both legally and communicatively, of privacy advocacy within the European regulatory framework. I considered it appropriate to review the most relevant legislation before presenting the case. I largely attribute this uniqueness to NOYB because the organization has a comprehensive free and open wiki

platform called GDPRhub where, for the purpose of shared knowledge and creative commons, it chooses to disseminate (most of) its research on the application of the GDPR in the EU and the European Economic Area (EEA) publicly and free of charge.

Chapter 4 addresses the technological response and the obfuscation tactics that seek to generate noise to defeat data extractivism. My inclination towards the study of obfuscation (defined in section 1.1.5) stems from my conviction of the ineffectiveness and impossibility of digital abstinence, given that it is increasingly difficult to avoid spaces belonging to data-extracting organizations while carrying out our educational, work, or social tasks. Given this, I consider it increasingly urgent to explore and raise awareness of the possible alternatives we can use to collectively protect our privacy, as well as to express our disagreement or critical presence. Throughout their research, Brunton and Nissenbaum (2011, paras. 29–50) made a clarifying distinction between different types of obfuscation—although they can later be combined—and presented examples of them. My particular contribution in this regard consists of an in-depth study of the work of two European-based researchers and activists, Adam Harvey and Martín Nadal. Not surprisingly, despite their different backgrounds, both agree on a representation of the problem of digital surveillance through art, especially through technological solutions that use free software to illustrate and challenge it.

Thirdly, Chapter 5 is devoted to the study of Decidim as a tool for transcending extractivist practices through a free software-based tool for participatory democratic practices. The drivers of Decidim (Barandiaran et al., 2024, pp. 1–3) define it as a digital infrastructure for participatory democracy. It is an initiative built entirely and collaboratively with free and configurable software to be used as a political network for democratic participation. However, the characteristic that makes the study of the Decidim platform even more stimulating is that its governance is organized around MetaDecidim: a meeting space, a participatory process, and a participatory community, oriented toward collaboratively and democratically deciding, designing, and producing multiple aspects of the project's future. During my research, I learned about the different processes in which this platform and its community were involved in defending the privacy of its users. Therefore, I am increasingly convinced that Decidim constitutes (in the broadest sense of the word) a key example for understanding how we can move from resistance to data-extracting organizations toward self-governing models whose preservation of privacy is the main axis of their construction.

Linked to this last proposal is Chapter 6, entitled *Decidimos Educación Inclusiva (We Decided Inclusive Education)*, as a proactive action on how to integrate the aforementioned tool into a research project that underpins Participatory Action Research.

Introducción

El ácido perfluorooctanoico (PFOA), igualmente denominado C8 y perfluorooctanoato, es un elemento sintético formado por cadenas largas de carbono a las que los átomos de flúor están fuertemente enlazados (“Ácido perfluorooctanoico”, 2024). Gracias a su composición, el PFOA tiene una capacidad “surfactante”, ya que reduce la tensión superficial del agua. Es por ello que este compuesto impermeabilizante se ha utilizado en multitud de productos de consumo, tales como revestimientos para gafas y raquetas de tenis, recubrimientos anti-manchas para alfombras y muebles, espuma contra incendios, envoltorios de comida rápida, cables de comunicaciones, cajas de pizza, etc. Con todo, quizá su uso más famoso es el del recubrimiento de sartenes antiadherentes de *Teflón™*, el nombre comercial de este compuesto.

Hasta aquí, todo indica que se trata de un gran compuesto, con unas ventajas extraordinarias para nuestro día a día, pues a nadie le gusta que se le pegue la tortilla o tener que emplear mucho tiempo y esfuerzo en eliminar una mancha de la alfombra. Ahora bien, otra de las cualidades del PFOA es que no se degrada, por lo que permanece en nuestros cuerpos y en el medio ambiente de manera indefinida.

Tal y como se cita en un artículo del Fondo Mundial para la Naturaleza (WWF por sus siglas en inglés), allá donde los científicos han buscado la presencia de PFOA, la han encontrado. Este compuesto se encuentra en la sangre o en los órganos vitales de, entre otros, el salmón del Atlántico, las focas grises, los osos polares de Alaska, las tortugas y águilas marinas y las águilas calvas del Medio Oeste estadounidense, así como en la gran mayoría de la especie humana. Unido a esto, debo destacar que diversos estudios (Tudela y Delgado, 2025) han confirmado que el PFOA actúa como un disruptor endocrino, es decir, que limita los efectos de las hormonas, por lo que está asociado con diferentes tipos de cáncer, problemas en la tiroides e infertilidad, tanto en seres humanos como en animales. Contestando al eslogan de cierta marca de sartenes: no, a nadie le falta *teflón* (en su cuerpo).

Podríamos estar hablando de un elemento más de los que, con el paso del tiempo, hemos descubierto que resultan gravemente perjudiciales para la salud y el ecosistema. Ahora bien, gracias a sendos reportajes de Natalie Rich (2016) para *The New York Times*, que sirvieron de guión para la película de Todd Haynes (2019) *Dark Waters* (*Aguas Oscuras* para los espectadores hispanohablantes), así como de Sharon Lerner para *The Intercept*, el gran público ha podido descubrir que la del PFOA es una historia de conocimiento, encubrimiento y poder a favor del lucro económico de un gigante industrial estadounidense, la empresa química DuPont.

Esta historia comienza en 1951, cuando DuPont empezó a adquirir PFOA de la multinacional 3M para

su uso en la fabricación de teflón. Aunque el gobierno estadounidense no clasificó al PFOA como una sustancia peligrosa, 3M le envió una serie de recomendaciones a DuPont sobre cómo deshacerse de él: podían incinerarlo o enviarlo a instalaciones de desechos químicos, pero se especificaba claramente que no debía arrojarse a aguas superficiales o alcantarillas.

Pese a ello, durante las décadas siguientes DuPont bombeó multitud de polvo de PFOA a través de las tuberías de desagüe de las instalaciones de Parkersburg, en Virginia Occidental (donde se situaba la empresa) al río Ohio. Igualmente vertió 7.100 toneladas de lodo con PFOA en pozos abiertos sin revestimiento de su propiedad, desde donde el químico podría filtrarse directamente al subsuelo. Como consecuencia de ello, el PFOA llegó a las aguas subterráneas que suministraban agua potable a más de 100000 personas en total.

También durante décadas estuvo DuPont tratando de ocultar sus acciones, pues sabían que este material era dañino y lo vertieron al agua de todos modos. Y lo sabían porque ya en los años 60 sus investigadores habían descubierto que el químico podía aumentar el tamaño del hígado en ratas y conejos. En la década de 1970, DuPont descubrió que había altas concentraciones de esta sustancia en la sangre de los trabajadores de su fábrica. Y en 1981, 3M, que seguía siendo el proveedor de PFOA de DuPont y otras empresas, descubrió que la ingesta de la sustancia provocaba anomalías congénitas en ratas. Después de que 3M compartiese esta información, DuPont probó con empleadas embarazadas en su división de teflón, con el resultado de que de siete nacimientos, dos tenían defectos oculares. Sin embargo, nunca hizo nunca público ninguno de estos amenazantes hallazgos.

Si DuPont pudo salirse con la suya todo este tiempo es porque durante décadas corporaciones como la suya se han amparado en la errónea percepción pública de que si una sustancia química era peligrosa, estaba regulada. Bajo la Ley de Control de Sustancias Tóxicas de 1976, la Agencia de Protección Ambiental de Estados Unidos (EPA, por sus siglas en inglés) podía informar de sustancias químicas peligrosas solo cuando se le había proporcionado evidencia de daño. Este acuerdo, que en gran medida ha permitido que las empresas químicas se autorregulen, es la razón por la que la EPA ha restringido solo cinco productos químicos de las decenas de miles que pueblan el mercado en los últimos 40 años.

Así pues, de no ser por el minucioso trabajo del abogado Rob Bilott, que decidió aceptar el caso de Wilbur Tennant, un granjero cuyas tierras lindaban con el vertedero de DuPont y cuyas vacas estaban muriendo en extrañas circunstancias debido a las altas concentraciones de PFOA en el arroyo del que bebían sus animales, quizá no hubiésemos llegado a conocer la verdad sobre esta historia y seguiríamos cocinando sobre superficies potencialmente tóxicas, sobre todo para nuestros acuíferos y para las

personas que estuvieron expuestas al mismo durante su (técnica y legalmente autorregulada) fabricación. Aunque este caso concluyó con un acuerdo extrajudicial cuyos pormenores no han sido revelados, condujo a otro por el que en agosto de 2001 alrededor de 70000 personas, representadas por Bilott, se agruparon para interponer una demanda colectiva contra DuPont por contaminar con PFOA el agua que utilizaban, proveniente de la misma planta (Tudela y Delgado, 2025).

Sin embargo, la historia no acaba aquí, dado que si bien en el año 2000 la EPA negoció con 3M que esta empresa dejaría de producir este tipo de compuestos, según su informe corporativo de 2023 (citado en Tudela y Delgado, 2025), la fabricación no cesó hasta 2002 en EEUU y hasta 2008 en el resto del mundo. 3M también fue llevada a juicio por el Estado de Minnesota por la contaminación de aguas subterráneas, superficiales, así como de peces y otros organismos acuáticos, además del suelo. En el primer trimestre de 2018, 3M alcanzó un acuerdo extrajudicial por un total de 897 millones de dólares para resolver el asunto. Y en junio de 2023, la misma empresa llegó a otro acuerdo con los demandantes de un litigio colectivo para abordar una serie de reclamaciones de varias empresas de abastecimiento de agua en cientos de localidades de EEUU. Este acuerdo estipula la asignación de más de 10500 millones de dólares para aquellos que identifiquen PFAS (sustancias perfluoroalquiladas y polifluoroalquiladas, entre las que destaca el ya mencionado PFOA) en sus fuentes de agua potable entre 2023 y 2036 (Tudela y Delgado, 2025).

En el caso de la Unión Europea (UE), este compuesto empezó a utilizarse para productos domésticos en la década de los 60 y no fue prohibido hasta 2020, gracias a la aprobación del Reglamento (UE) 2017/1000 de la Comisión de 12 de junio de 2017. Sin embargo, la prohibición de manera individual de cada compuesto ha representado un logro significativo para la industria. Según los datos recogidos por Tudela y Delgado (2025), hoy en día, existen más de 10000 variedades de PFAS en el mercado, y solo a finales de 2022, y después de varios juicios, 3M anunció que suspendería la producción de todos los PFAS hacia finales de 2025, aunque en sus informes indica que esto no evitará el uso de PFAS de otras fuentes donde no existan alternativas viables.

En el caso de España, a pesar de no contar con fábricas de PFAS en su territorio, gracias a un limitado pero muy relevante estudio de biomonitorización llevado a cabo por un grupo de científicos, con la investigadora Argelia Castaño a la cabeza, se pudo constatar que existía un 100% de presencia de PFOA en las muestras analizadas (Tudela y Delgado, 2025). A comienzos de 2025 se anunció que en los próximos meses se esperaba realizar otro estudio de mayor extensión con una muestra de población del territorio español de 3800 participantes para analizar en sangre y orina los químicos de riesgo acumulados en el organismo: «metales pesados, hidrocarburos aromáticos policíclicos, PCBs, Bisfenoles,

dioxina, sacroleína, pesticidas y al menos 12 PFAS» (Tudela Delgado, 2025).

A consecuencia de todo ello, hoy tenemos una mayor conciencia de la contaminación ambiental producida por la industria química, la cual se ha vuelto una preocupación importante por el impacto significativo en la salud humana y el medio ambiente, especialmente en la calidad del aire y del agua. En contraste, en los últimos años han proliferado nuevas formas de contaminación que quizá pasan más desapercibidas. Hablo de la contaminación derivada de los servicios digitales, la cual se refiere al impacto negativo de las TIC e Internet, provenientes de la gestión de los desechos electrónicos de dispositivos obsoletos y, sobre todo, del alto consumo de energía y agua de los centros de datos para alimentar y enfriar los servidores donde almacenan y procesan cantidades masivas de información, lo cual contribuye a las emisiones de carbono y exacerba el cambio climático.

Aquello que conecta las historias de ambas industrias es el afán por parte de las empresas que operan en ambos sectores por la autorregulación. Ya he hablado de cómo la EPA en EEUU dejaba la responsabilidad de informar sobre una sustancia tóxica a las propias empresas que las fabricaban, y los terribles resultados ocasionados por esta (in)acción. Pero en el caso de las grandes compañías del entorno digital (Meta, Google, Amazon y Apple), la primera vez que se las intentó regular en EEUU no llegó hasta el 2020 (Pérez Colomé, 2020), aunque las deliberaciones se centraban más en el poder de estas empresas como oligopolios que en los riesgos del tratamiento excesivo de datos personales que albergan y los riesgos para la privacidad que ello supone.

Para el catedrático de Derecho Frank Pasquale (citado en Zuboff, 2019/2020, p. 152), esta apuesta por la autorregulación es un legado del neoliberalismo, dando lugar a un enfoque que considera la privacidad como un valor competitivo y que asume que los “usuarios” optan solo por aquellos servicios que les brindan el grado de privacidad deseado. Es a partir de este legado que el modelo de “aviso y consentimiento” es visto de manera favorable porque se cree que permite a cada persona expresar de manera clara y detallada sus preferencias en lo que respecta a la privacidad. En pocas palabras, al tratar la privacidad de manera individual nos vemos abocados a la búsqueda de soluciones igualmente individuales.

Pero ¿y si todo esto no es así? En mi tesis doctoral, lejos de perspectivas derrotistas, pretendo mostrar cómo la ciudadanía se asocia desde distintos ejes, como el marco jurídico, el arte y *artivismo* (analógico y digital) o el desarrollo de plataformas democráticas alternativas, para la búsqueda de soluciones con las que podamos resistir y reexistir de una manera menos agresiva y dañina los tiempos en los que nos vemos envueltos.

1. Posicionamiento y diseño de la investigación

1.1. Delimitación del foco de estudio: Tácticas de resistencia frente al extractivismo de datos personales

A lo largo de estas páginas he creído conveniente detenerme en algunas creencias fervientemente asentadas sobre determinados conceptos que guardan relación con el foco de estudio. Con ello mi intención ha sido, a veces directamente desmontarlas, y otras simplemente entender cuáles son sus orígenes y por qué las pensamos de esta manera. Pero antes de entrar en el desarrollo, quisiera detenerme primero en el excesivo uso que he podido percibir cuando hablamos del ámbito digital de quizá la figura retórica más utilizada, la metáfora:

Las metáforas son imprescindibles en el lenguaje —de hecho, ningún lenguaje, salvo quizá el matemático, puede prescindir de ellas—. Parece que no podemos comprender el mundo sin dar esos saltos imaginativos que nos permiten pensar una cosa en términos de otra, con las cualidades de otra muy diferente, en una forma que hace surgir de esa diferencia un rasgo común que enriquece nuestra comprensión previa (Peñamarín, 2020, párr. 19).

Y es que, si bien las metáforas se utilizan a menudo para simplificar ideas complejas y hacerlas más comprensibles para un público más amplio, cuando se toman de manera literal, suponen el riesgo de pasar por alto ciertos matices o complejidades de la realidad. Las metáforas pueden ser útiles para proporcionar un marco, para comprender conceptos abstractos, pero también pueden limitar nuestra capacidad de ver la imagen completa.

Así pues, si esta reflexión sobre la tecnología ha de transitar por el «lugar de los pre-su-puestos, es decir, de aquello que cada cultura y cada grupo social se encuentra puesto previamente (pre-) debajo de (sub-) sus elaboraciones reflexivas y conscientes» (Lizcano, 2006, p. 48), el mejor modo de hacerlo consiste en reparar en las metáforas que de modo directo o indirecto nos conducen a sus sentidos profundos. En suma, se trata de atender a las «métaforas que nos piensan» (Lizcano, 2006, p. 12), pero no tanto desde un registro retórico sofisticado como desde el empleo más cotidiano del término en griego como “transportes en común” (de significados):

En la Atenas de hoy día, los transportes en común se llaman *metaphorai*. Para ir al trabajo o regresar a casa, se coge una “metáfora” —un autobús o un tren. Los relatos podrían portar igualmente tan bello nombre: [...] cotidianos o literarios, son nuestros transportes en común, nuestras *metaphorai* (Certeau, 1990, pp. 170-171).

El problema de la expansión de metáforas como “nube”, “inteligencia artificial” o “gases de escape digitales” es que son ideas que están conducidas por marcos ideológicos que tienen unas claras intenciones, hacernos olvidar la materialidad que existe detrás de estos juegos de palabras. Es por lo que a lo largo de este epígrafe, vamos a ir haciendo algunas paradas para poder ir bajándonos de ellas y dilucidar qué intentan dejar por el camino.

1.1.1. Rematerialización de lo digital

Comenzaremos entonces por uno de los ejemplos más claros, el citado concepto de la “nube”, empleado de manera amplia como eufemismo para intentar transportarnos o hacernos levitar de la idea de aparatos, cables y demás *hardware* a espacios livianos y, con suerte, más limpios. De esta manera, se nos ha intentado hacer creer que, si nuestra información viaja de manera digital en lugar de ser transportada por nuestros cuerpos en contaminantes medios de transporte, estamos haciendo “un favor al medio ambiente”.

Sin embargo, no es tan clara y esponjosa esa nube a la que nos quieren hacer subir. No en vano, detrás del relato construido sobre este cúmulo, no hay más que un ordenador más grande, más potente y centralizado que el nuestro, con el cual se pretende controlar este nuevo clima, y acelerar su cambio, tal y como nos hace ver Edward Snowden (2019, p. 265):

Ya no importaba en realidad qué tipo de ordenador personal tuvieses, porque los auténticos ordenadores de los que dependíamos estaban guardados en los enormes centros de datos que las empresas basadas en la nube construyeron en todo el mundo. [...] Como resultado, tus datos ya no son tuyos de verdad. [...] No hay ninguna propiedad menos protegida, y pese a ello ninguna propiedad es más privada.

Ahora sabemos, gracias a la *web* CloudMap de la consultora Telegeography, que estos enormes centros de datos están controlados principalmente por ocho empresas, cinco de origen estadounidense y tres de origen chino:

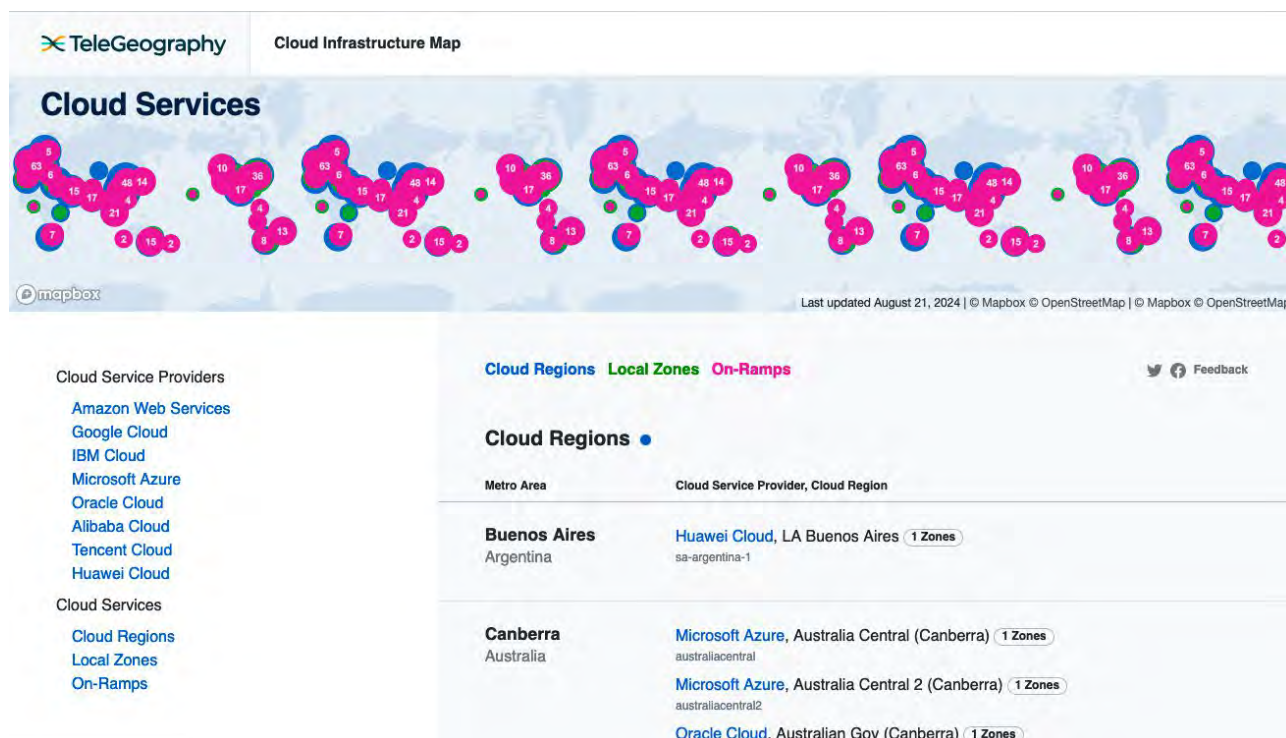


Figura 1. Captura de pantalla de la *web* CloudMap. Recuperado el 30 de noviembre de 2024.

Fuente: <https://www.cloudinfrastructuremap.com/>

Y es que, por mucho que nos intenten hacer creer que la tecnología nos viene caída del cielo, este conglomerado gaseoso bien se asemeja a las reservas de gas natural del subsuelo tan disputadas en la geopolítica mundial, y a cómo éste se transporta realmente: «las comunicaciones, los flujos financieros y el acceso a los datos almacenados en la ‘nube’ dependen de los cables submarinos» (Perragin y Renouard, 2021, párr. 9). Si visitamos la *web* Submarine Cable Map de la citada Telegeography, podremos ver que en el control y construcción de estos particulares gaseoductos también participan las mismas empresas protagonistas del oligopolio digital, con propiedad exclusiva o con una inversión importante en ellos:

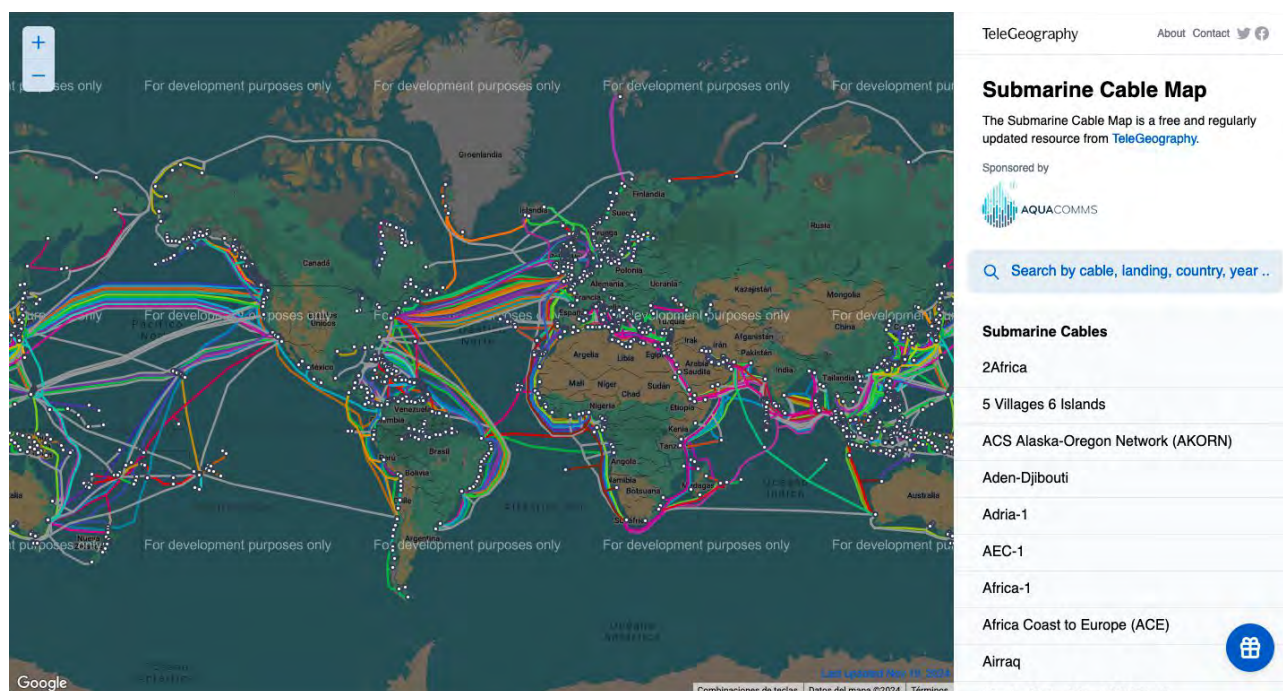


Figura 2. Captura de pantalla de la *web* Submarine Cable Map. Recuperado el 30 de noviembre de 2024.

Fuente: <https://www.submarinecablemap.com/>

De este modo, tal y como apunta el sociólogo Sébastien Broca (2020, párr. 1): «la economía digital no es ‘inmaterial’ ni ‘verde’», y como ejemplo cita al gran líder de la (mal)llamada nube, Amazon, cuyo principal centro de datos, situado en Virginia, adquiere la mayor parte de su electricidad del carbón extraído de la cordillera de los Apalaches. Pero incluso si, con suerte, esta situación llegara a cambiar, Broca recuerda que los tres principales proveedores de la “nube” colaboran, junto a las principales petroleras, con estrategias dirigidas a optimizar la localización y explotación de nuevos yacimientos de hidrocarburos. En último término, el periodista Guillaume Pitron (2021) apunta a que las industrias digitales triplicarían la huella de carbono de países como Francia y Reino Unido y que sus centros de datos consumen del 1% al 3% de la electricidad mundial.

Asimismo, los servidores de los centros de datos, además de consumir energía producen calor durante su operación. La concentración de tantos ordenadores en un mismo lugar no hace sino potenciar ese efecto. Si bien es posible realizar su refrigeración mediante sistemas de ventilación, parecidos a los que emplean los ordenadores personales, resulta más económico refrigerar los procesadores con otro bien escaso: el agua. De esta manera, numerosos centros de datos utilizan torres de enfriamiento para prevenir el citado sobrecalentamiento, el mismo método que se utiliza en otras industrias. Este proceso consiste en exponer una corriente de agua a un flujo de aire en un intercambiador de calor, de tal forma que la evaporación enfríe el circuito. Si bien el citado procedimiento es más eficaz en términos

energéticos que los refrigeradores eléctricos, éste requiere que un volumen considerable de agua se evapore, es decir, que no regrese al circuito. Según el investigador Shaolei Ren, profesor asociado de ingeniería eléctrica y computacional de la Universidad de California:

Esa es el agua que figura como “consumida” en los registros de las tecnológicas. Dependiendo de la temperatura exterior del bulbo húmedo, una torre de refrigeración suele consumir entre uno y cuatro litros de agua (hasta nueve en verano) por cada kWh de energía del servidor (citado en Pascual, 2023, párr. 14).

Además, alrededor del 20% del agua empleada —de la que no se evapora en los sistemas de enfriamiento— se vierte al concluir el ciclo en las instalaciones de aguas residuales. Según este mismo investigador (citado en Pascual, 2023, párr. 15) esta agua posee enormes volúmenes de minerales y sal, por lo que no puede ser utilizada para el consumo humano sin previo tratamiento. Resulta necesario en este momento indicar también que el agua que se requiere para este proceso debe ser agua limpia y tratada, para prevenir atascos o el desarrollo de bacterias en los conductos, y en los casos en los que se utiliza agua marina o depurada, es necesario tratarla antes de introducirla en los sistemas de enfriamiento. De nuevo según Ren (citado en Pascual, 2023, párr. 15), «en el caso de Google, casi el 90% de su consumo en EEUU procedió de fuentes potables».

Estudios situados como el de Ana Valdivia (2024) nos ayudan aquí a entender qué supone este ingente consumo de un bien cada vez más escaso para mantener y proliferar los centros de datos. En su caso, la investigadora se centró en el dilema que todo esto supone para la comunidad indígena y rural de Maconí en Querétaro (México).

El dilema que presenta comienza con el hecho de que Querétaro se está convirtiendo en el lugar de América Latina donde mayor número de centros de datos están siendo ubicados, con diez ya operativos y dieciocho más en proyección. Esto es debido al amplio legado industrial de la región, a su situación geográfica propicia y a la clara apuesta del gobierno local por este tipo de infraestructuras (Valdivia, 2024, p. 9). Sin embargo, esta región también experimenta ya una escasez de agua, con el 100% de su territorio en riesgo de sequía (Valdivia, 2024, p. 10). Para solventar este problema, desde 2006 el gobierno local desarrolló una estrategia para obtener el agua potable de los manantiales de Maconí a través de un trato con la población local: la extracción del agua de sus tierras a cambio del suministro de agua potable (Valdivia, 2024, p. 9).

Tras la firma del acuerdo, el gobierno de Querétaro construyó una de las infraestructuras hidráulicas más grandes de México: el Acueducto II, una tubería de 123 km de longitud que bombea agua desde las

montañas de Maconí y la lleva a los ciudadanos de Querétaro y sus parques industriales. Sin embargo, actualmente no solo el gobierno local no ha cumplido con su promesa, sino que los recursos hídricos de Maconí se están agotando debido a la cantidad de agua que el acueducto extrae diariamente de los manantiales de la región. Como resultado, la comunidad indígena y rural de Maconí sufre escasez de agua y deben realizar largos trayectos a pie para conseguir agua potable (Valdivia, 2024, p. 10).

Investigaciones como la citada demuestran también cómo el desarrollo de productos avanzados de lo que han denominado inteligencia artificial (IA) se basan en un sistema de extractivismo que genera tanto riqueza como pobreza. Y es que, para entrenar algoritmos sofisticados como los modelos extensos de lenguaje (LLM por sus siglas en inglés), los centros de datos donde se albergan deben estar equipados con unidades de procesamiento gráfico (GPU por sus siglas en inglés). Las GPU están hechas principalmente de silicio y cobre, junto con tantalio, aluminio o tungsteno, los cuales se extraen de diferentes territorios en todo el mundo (Valdivia, 2024, p. 3), con el correspondiente daño medioambiental que suponen este tipo de minas.

Pero además, explica la autora, estos dispositivos tienen una vida promedio de cinco años, lo que genera desechos electrónicos significativos que también presentan graves riesgos ambientales. Si bien es cierto que algunos componentes se recuperan, muchos equipos se desechan de manera que contaminan el agua y el suelo con sustancias peligrosas. Algunos de estos dispositivos son incinerados mientras que otros son enviados a vertederos en regiones distantes de donde se extrajeron sus materias primas, cerrando un ciclo de extractivismo que acarrea problemas ambientales, sobre todo en las regiones del Sur Global.

Para ilustrar la cadena de suministro de la IA como un fenómeno global y complejo, Valdivia (2024, p. 6) utiliza el ejemplo de NVIDIA, empresa encargada de diseñar las unidades de procesamiento de gráficos con lo que funcionan estos programas. Los recursos naturales, los componentes y los materiales para construir estas GPU se extraen, envían, fabrican y producen en todo el mundo. En el caso que nos ocupa, esta empresa obtiene tungsteno de Brasil, oro de Colombia y tantalio de Kazajistán. Por su parte, TSMC, empresa con sede en Taiwan que fabrica más del 60% de los *microchips* a nivel mundial y que cuenta con acuerdos con NVIDIA desde los años noventa, es la encargada de ensamblar los minerales para fabricar estos *microchips*, que luego aquella se encarga de vender a centros de datos de todo el mundo. Dadas las citadas frecuencias de actualización de estos materiales, los centros de datos envían los componentes que ya no les son útiles a plantas de reciclaje o vertederos.

Dentro de este ciclo extractivista, debemos tener también en cuenta el trabajo humano involucrado en

esta cadena. Etiquetadores de datos, conductores logísticos, científicos de datos, mineros, operadores de centros de datos y desmanteladores de desechos electrónicos, todos estos oficios también están dispersos en diferentes geografías del mundo con condiciones laborales muy dispares, lo cual resume la autora de manera ilustrativa de la siguiente manera:

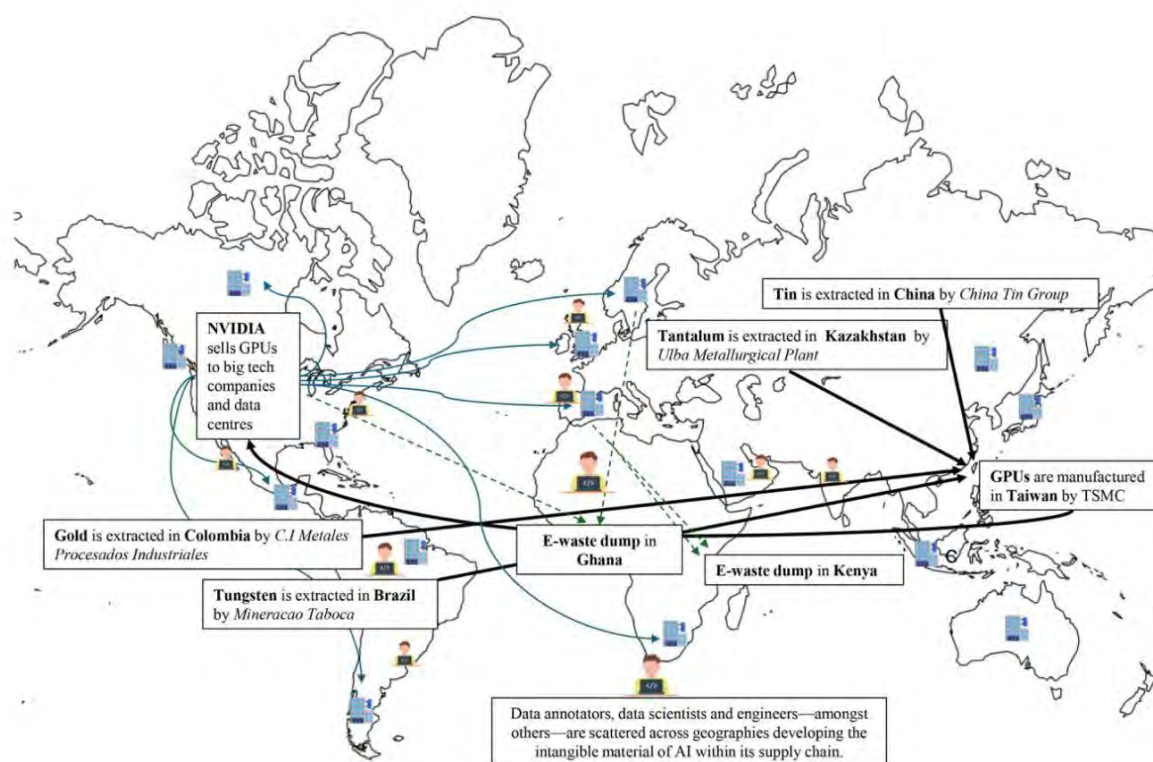


Figura 3. Mapa de la cadena de suministro de la IA a través de los datos de NVIDIA. Fuente: Valdivia, 2024, p. 6.

Y de las planetarias y atmosféricas metáforas de la “nube” pasamos ahora a otras más pequeñas y cotidianas, las *cookies*. Una *cookie* (literalmente en inglés “galletita”) es un archivo de texto que el servidor al que te conectas deposita en tu disco duro a través del navegador y que sirve para que la página *web* en cuestión obtenga información de tu visita y te reconozca cuando vuelvas a acceder a ella.

Debemos tener en cuenta que existen diferentes tipos de *cookie*: si atendemos a su temporalidad, encontramos por un lado las *cookies* temporales, que expiran cuando abandonas la página *web* visitada, y por otro las *cookies* permanentes, que tras dejar el sitio siguen depositadas en tu dispositivo, aunque suelen tener una fecha de expiración determinada (en todo caso, siempre posterior a la de las *cookies* temporales).

Existe otra diferencia en función de quién es su responsable, de esta manera encontramos las *cookies* propias de un sitio *web* y las denominadas *cookies* de terceros, que son las implantadas por entidades o

servicios *web* ajenos a la página que se visita.

Por último, encontramos la fundamental distinción basada en la funcionalidad de dichas *cookies*, a partir de la cual diferenciamos cuatro tipos: el primero son las *cookies* técnicas, que son las necesarias para optimizar el funcionamiento de una *web* que requiera controlar el tráfico o almacenar información entre distintas interacciones. En segundo lugar, encontramos las *cookies* de preferencia, que permiten personalizar la apariencia, la funcionalidad, el idioma, la moneda de pago o demás aspectos de una página *web* para no tener que modificarlos cada vez que regreses. En tercer lugar, tenemos las *cookies* analíticas o de rendimiento, que son las que permiten que el servidor de la *web* recoja información sobre tus hábitos de navegación para generar analíticas de tráfico. El último lugar, las *cookies* publicitarias son aquellas propias de la página, pero sobre todo de terceros, mediante las cuales tus conductas de navegación a través de diversos sitios *web* son sometidas a seguimiento, recopilación, agregación, procesamiento y clasificación para crear un perfil de usuario, más o menos preciso, que utilizan directamente o se venden para fines promocionales vinculados a la llamada publicidad segmentada.

A partir de esta definición, la cuestión principal es, según Lawrence Lessig, estudioso de las formas en que el código informático y las políticas públicas se relacionan, que «[a]ntes de las *cookies*, la *web* era esencialmente privada. Después de las *cookies*, la *web* se convierte en un espacio capaz de un monitoreo extraordinario» (citado en Schwartz, 2001, párr. 12).

Y es que, por lo general, aunque los datos que se recopilan a través de *cookies* (y otras tecnologías de seguimiento integradas en los dispositivos, páginas *web*, aplicaciones y todo tipo de contenido digital interactivo y audiovisual) son creados y almacenados en el dispositivo del usuario, en su mayoría son opacos y, a veces, indetectables para este. Ello provoca que sea relativamente fácil extraer grandes cantidades de datos de estas tecnologías de seguimiento. Además, a pesar de su tamaño relativamente pequeño, estas *cookies* son responsables de activar una gran cantidad de procesos algorítmicos a escala global, explotando los datos del comportamiento del usuario con un impacto directo en el consumo de energía de los dispositivos del usuario (Cucchiatti *et al.*, 2022, párr. 6).

De esta problemática surge el proyecto Carbolytics, realizado por la artista Joana Moll en colaboración con el Barcelona Supercomputing Center (BSC). Este proyecto pretende concienciar y llamar a la acción sobre el impacto ambiental de la vigilancia generalizada dentro del ecosistema de la tecnología publicitaria (*AdTech*), así como proporcionar una nueva perspectiva para abordar los costes sociales y ambientales de las prácticas mayoritariamente opacas de la recopilación de datos personales.

Para Cucchiatti *et al.* (2022), pese a que las actividades cotidianas afectadas por este seguimiento del

comportamiento del usuario (como leer las noticias, comprar artículos, interactuar en las redes sociales o simplemente hacer una búsqueda en línea), conllevan unos grandes costes energéticos y ambientales, las empresas rara vez revelan información sobre la huella ambiental de tales operaciones. Además, según estos autores, parte de los costes energéticos de las prácticas de recopilación de datos recaen sobre el usuario, quien también asume involuntariamente una parte de esa huella ambiental.

Frente a esto, la investigación de Carbolytics identifica y analiza las emisiones de carbono del total de *cookies* del millón de sitios *web* identificados como los más importantes. De aquí surgió una base de datos de más de 21 millones de *cookies* por visita única a todos estos sitios *web*, pertenecientes a más de 1200 empresas diferentes, que se traduce en un promedio de 197 billones de *cookies* por mes, lo que resulta en 11442 toneladas métricas mensuales de emisiones de CO₂. Con todo, estas mareantes cifras reflejan solo el tráfico de *cookies* basado en el navegador y no incluye otras herramientas de publicidad conductual, como la actividad de seguimiento de aplicaciones o los algoritmos de creación de perfiles, por lo que los autores estiman que la cantidad real de emisiones de las tecnologías de seguimiento es drásticamente mayor.

Los desarrolladores del proyecto (Cucchiatti *et al.*, 2022) definen Carbolytics como una instalación interactiva basada en la *web* que muestra el tráfico promedio global de *cookies* en tiempo real, es decir, muestra cómo las *cookies* “parasitan” los dispositivos de los usuarios para extraer datos personales y alimentar una red masiva y opaca de organizaciones. Con ello buscan agregar una capa a la crítica tradicional basada en los derechos individuales de la industria de *AdTech*, al tiempo que proporcionan evidencias sólidas para brindar información a las comunidades que abogan por la responsabilidad tecnológica y la lucha contra el cambio climático.

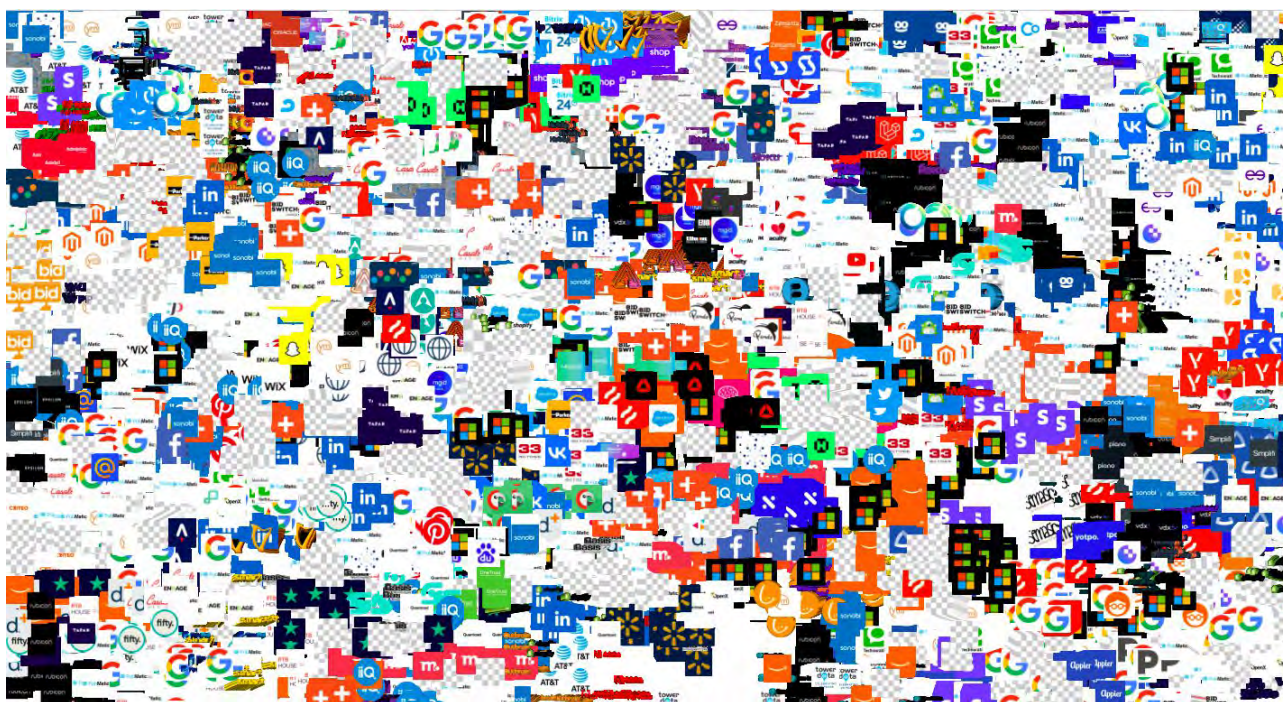


Figura 4. Captura de pantalla del sitio web <https://carbolytics.org/web2x/>. Recuperado el 6 de diciembre de 2024



Figura 5. Ejemplo de información que aporta el sitio web <https://carbolytics.org/web2x/> sobre la huella de carbono que produce una *cookie*. Recuperado el 6 de diciembre de 2024

1.1.2. Un nuevo extractivismo

Frente a las relaciones tradicionales de extractivismo, que vemos que se continúan dando en la fabricación y empleo de las tecnologías de las que se componen tanto las redes digitales como los centros de datos, nos enfrentamos en nuestros días a lo que Ulises Mejías y Nick Couldry (2019, pp. 80-81) han denominado, un nuevo colonialismo de datos:

El colonialismo de datos combina las prácticas extractivas depredadoras del colonialismo histórico con los métodos abstractos de cuantificación provenientes de la computación. [...] Así como el colonialismo histórico a largo plazo proporcionó las condiciones esenciales para el surgimiento del capitalismo industrial, con el tiempo, podemos esperar que el colonialismo de datos proporcione las condiciones para una nueva etapa del capitalismo que aún no podemos imaginar, pero para la que la apropiación de la vida humana a través de los datos será fundamental. [...] [E]l nuevo colonialismo de datos funciona tanto externamente (a escala global) como internamente en sus propias poblaciones de origen. Las elites del colonialismo de datos [...] se benefician de la colonización en ambas dimensiones, y las divisiones Norte-Sur, Este-Oeste ya no importan de la misma manera.

En el despliegue de esta recolección de información personal, Mejías y Couldry (2019, p. 85) señalan que el colonialismo de datos también recurre a otras lógicas de extracción, empezando por la propia devaluación de dicha información personal. Para ilustrar esta lógica, se apoyan en los postulados críticos de Scholz (2013) o Funchs (2017) que indican que existe una racionalidad social que considera a muchas de las actividades que ayudan a obtener estos datos como actividades sin valor, como un mero intercambio. Igualmente conocida en este sentido es la tesis de Zuboff (2019/2020, p. 129) que apunta a que las empresas extractivistas de datos hacen referencia a “gases de escape digitales” o “migas de pan digitales” como si fuesen deshechos sin valor, concepto al que retornaré a lo largo del marco teórico.

Unido a ello, existe una racionalidad pragmática que sitúa a estas empresas como las únicas con el poder y la habilidad para procesar y, en consecuencia, extraer estos datos. Al mismo tiempo, Mejías y Couldry (2019, p. 85) encuentran una racionalidad política que busca establecer a la sociedad como el objetivo natural de los esfuerzos de extracción de estas corporaciones, de la misma manera que se asumía que la humanidad se beneficiaría del colonialismo histórico como un proyecto de “civilización”.

Asimismo, este extractivismo opera sobre otro plano conectado al de los datos personales, que tiene que ver con las relaciones laborales en el entorno digital. Sobre esto, vale la pena volver al concepto tan

empleado hoy día de Inteligencia Artificial (IA) para desarmarlo, puesto que, tal y como indica Morozov (2023, párr. 4):

En realidad, lo que hoy llamamos “inteligencia artificial” no es ni artificial ni inteligente. Los primeros sistemas de IA estaban muy dominados por reglas y programas, de modo que, por lo menos, la palabra “artificial” estaba justificada. Pero los sistemas actuales, como el ChatGPT que tanto gusta a todos, no se basan en reglas abstractas, sino en el trabajo de seres humanos reales: artistas, músicos, programadores y escritores, de cuya obra creativa y profesional se apropian esos sistemas con la excusa de querer salvar la civilización. En todo caso, es una “inteligencia no artificial”.

Pero no solo toma el trabajo de otros para su construcción sino que, a su vez, precisa del trabajo humano, a menudo mal pagado, para su entendimiento y etiquetado:

Adherirse a la IA tal y como la conocemos implica ahondar en un compromiso con prácticas laborales de las que la mayoría no somos siquiera conscientes, que son sesgadas por género y raza, y que se presentan sin ninguna negociación colectiva sobre condiciones laborales o de remuneración justas (McQuillan, 2022, citado en Cabello, 2024, p. 968).

Por otro lado, en cuanto al término “inteligencia”, también merece la pena recordar aquello que Joseph Weizenbaum (citado en Cabello, 2024, p. 968) vislumbró ya en 1966 al poco de lanzar ELIZA, el primer *chatbot* de la historia, y comprobar cómo su propósito experimental y, en gran medida, (auto)irónico era (mal)interpretado frente a la ilusión de que ELIZA era un ente capaz de comprensión y, más allá, de emisión de juicios fidedignos:

Suele decirse que explicar es explicar por descarte. En ningún lugar se cumple mejor esta máxima que en [...] la inteligencia artificial. [...] Una vez que un programa queda desenmascarado, una vez que su funcionamiento interno se explica en un lenguaje suficientemente sencillo para inducir su comprensión, su magia se desmorona [y] el observador mueve el programa en cuestión de la estantería marcada como “inteligente” a aquella reservada a las curiosidades.

Sobre esta misma idea, Morozov (2023, párr. 5) apunta que la influencia de la Guerra Fría en la creación de este concepto marca claramente el sentido que hoy le otorgamos: «Es el tipo de inteligencia que sería útil en una batalla. Por ejemplo, lo mejor de la IA actual es su capacidad de buscar patrones» (Morozov,

2023, párr. 5). Sin embargo, continúa argumentando que este tipo de algoritmos no serían capaces de, por ejemplo, generalizar:

Cuando generalizamos, la emoción anula las clasificaciones arraigadas y aparentemente “racionales” de las ideas y los objetos cotidianos. [...] No es algo que convenga hacer en medio de una guerra. [...] El peligro de seguir manejando un término tan inexacto y obsoleto como “inteligencia artificial” es que corremos el riesgo de convencernos de que el mundo funciona con arreglo a una lógica singular: la del racionalismo profundamente cognitivo y sin sentimientos (Morozov, 2023, párr. 7).

En razón de todo lo anterior, al efecto contaminante de la obsesiva recopilación y conservación de datos personales debemos sumarle una intoxicación en el plano de la información, ya que según argumenta la filósofa Carissa Véliz (2020/2021, p. 110):

Los datos personales son peligrosos porque son un material sensible, muy susceptible de un mal uso, difícil de tener a buen recaudo y codiciado por muchos, desde delincuentes hasta empresas aseguradoras y agencias de inteligencia. Cuanto más tiempo tengan otros almacenados nuestros datos y cuanto más los analicen, más probable resultará que alguien acabe usándolos contra nosotros. Los datos son vulnerables y eso hace que, a su vez, los sujetos de datos y cualquiera que los guarde sean vulnerables también.

Y si la sola acumulación de datos personales puede resultar ya tóxica, también debemos alertar de la toxicidad de su manipulación. En este sentido, el experto en derecho de privacidad de la información, Paul M. Schwartz (1989) ya llamaba la atención sobre el peligro de que “el ordenador” pusiese en riesgo la autonomía humana, ya que cuanto más conocimiento se tiene sobre alguien, más fácil resultaría controlarlo. Así, décadas antes del escándalo de Cambridge Analytica, este profesor hablaba incluso del peligro sobre la democracia de no estructurar correctamente el uso social de la información, y que debería permitirse ciertas dosis de ocultación de la misma.

Por ello, considero relevante ubicar el extractivismo de datos personales como una parte de las historias del “Capitaloceno”¹, al que se refiere la historiadora de la conciencia Donna Haraway (2016/2019) dentro de su reflexión sobre los tiempos perturbadores, confusos, turbios y problemáticos que vivimos.

1 Si atendemos al artículo de Raúl García y Nancy Merary (2020), el Capitaloceno es un concepto que pretende sustituir al de Antropoceno. Así mientras que este se refiere a que la actividad humana ha adquirido la potencia de convertirse en una fuerza ambiental destructiva a nivel mundial, aquellos que se decantan por el concepto de Capitaloceno consideran que esta potencia destructiva proviene más de la organización capitalista de los humanos que de su actividad en abstracto.

Ante esta situación, la autora señala que es habitual que surjan dos posibles respuestas: bien que una tecnología futura todavía no pensada (o, lo que podría ser lo mismo, un Dios entendido como un ente superior) nos salvará; o bien creer que ya no hay nada que hacer y que podemos dar el juego por terminado.

Frente a ello, Haraway defiende que, en lugar de imaginar un tiempo futuro o caer en el bucle de autocompasión por un pasado horrible entre cuyas consecuencias nos desarrollamos, debemos aprender a estar presentes de manera entrelazada con el resto de habitantes del planeta en nuestro día a día: «Nuestra tarea es generar problemas, suscitar respuestas potentes a acontecimientos devastadores, aquietar aguas turbulentas y reconstruir lugares tranquilos» (Haraway, 2016/2019, p. 19).

1.1.3. El concepto de dato personal

Partamos de entrada de cómo la Comisión Europea (s.f., párr. 1) define los datos personales:

Cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales.

Pues bien, lejos de esta descripción aséptica, la cuestión de qué son los datos tiene profundas implicaciones filosóficas, socioeconómicas y políticas. De esta manera, en los últimos años han adquirido amplia difusión diferentes propuestas para conceptualizarlos, y cada una de ellas viene acompañada de un conjunto distintivo de metáforas. A este respecto, Antonio Calleja-López (2018) destaca tres modelos: la consideración de los datos como recurso natural; la consideración de los datos como trabajo; y, finalmente, la consideración de los datos como infraestructura. Tal y como apunta el autor (2018, p. 15), los conceptos y metáforas con los que tratamos de entender y enmarcar esta realidad están ligados a nuestras prácticas, y en última instancia, a diferentes formas de vida y las luchas en torno a ellas, por lo que resulta necesario indagar en cómo se entienden los datos personales desde estas visiones para poder estudiar las implicaciones de comprenderlos desde uno u otro prisma.

Datos personales como materia prima

Desde un enfoque pragmático, un aspecto clave tanto de los datos como de la información es su uso, ya sea comunicativo, de control o cualquier otro. Para Mejías y Couldry (2019, p. 84), al igual que se operó dentro de las formas clásicas del colonialismo histórico, el colonialismo de datos también se asienta sobre una base ideológica deliberadamente articulada para su beneficio. Así, se ha extendido ampliamente la metáfora de entender los datos personales como el “nuevo petróleo”, mantra que amplificó el Foro Económico Mundial (2011, pp. 5-7) cuando estableció que: «los datos personales serán el nuevo ‘petróleo’, un recurso valioso del siglo XXI [...] convirtiéndose en un nuevo tipo de materia prima que está a la par con el capital y el trabajo».

La metáfora de los datos como materia prima, tal y como indica Calleja-López (2018, p. 16), los presenta como un bien que se debe extraer de su fuente: la actividad humana. Resulta por tanto un recurso que se debe extraer, procesar y almacenar en grandes cantidades para generar información valiosa, que luego a su vez, puede venderse como una mercancía o como un servicio. Sin embargo, este movimiento discursivo oculta, para Mejías y Couldry (2019, p. 84), los vínculos entre los datos y un proceso previo de recolección y apropiación. Además, este desenfoque se consigue gracias a la metáfora que da a entender que mediante la concepción generalizada de que los datos son un “residuo” remanente de la vida cotidiana, no pueden ser propiedad de nadie y solo las empresas pueden extraerles el valor que realmente tienen.

Datos personales como trabajo

La metáfora que trata de cambiar esta manera de pensar vincula los datos personales con formas de trabajo que también están sujetas a explotación. De esta manera, la idea de entender los datos como trabajo parte de una visión crítica del modelo actual de la economía digital. Investigaciones como las de Arrieta *et al.* (2018, p. 39) confrontan cómo entender los datos como materia prima (*data as commodity*) significa tratarlos como un escape natural del consumo que las empresas deben recopilar, mientras que entender los datos como un trabajo (*data as labor*) sería entenderlos como algo que es propiedad de los usuarios, quienes por ello deberían ser los principales beneficiarios de su extracción.

Para estos autores, al entender los datos como materia prima primaría el beneficio empresarial, el espíritu emprendedor y la innovación. Frente a ello, la comprensión de los datos como trabajo fomentaría una mayor calidad y cantidad de los mismos y entendería los modelos como el de Aprendizaje Automático (*Machine Learning*) como una tecnología de producción que mejoraría la productividad laboral y crearía una nueva clase de “trabajadores de datos”. Por último, al entender los

datos como materia prima, los autores plantean que se establece un contrato social basado en servicios gratuitos a cambio de una vigilancia predominante, mientras que al entenderlos como trabajo, son las instituciones gubernamentales quienes deben verificar la capacidad de las plataformas digitales para explotar su particular poder monopolístico sobre los proveedores de datos y garantizar un mercado justo (entendido como transparente) para el trabajo de datos.

Sobre esta metáfora, Calleja-López (2018, p. 18) reconoce el potencial que tiene su asentamiento para figuras como los sindicatos, dado que, tal y como los autores del artículo sugieren (Arrieta *et al.*, 2018, p. 41), en estas condiciones las huelgas serían más fáciles de llevarse a cabo en las plataformas digitales. Junto a ello, se podría asegurar la calidad de los datos, incrementando de esta manera la rentabilidad de los mismos. Calleja-López (2018, p. 18) ve en el núcleo de esta estrategia la capacidad de convencer a las personas de una visión alternativa de los datos y proyectar mecanismos potenciales para medir y hacer cumplir, a través del pago, el valor de los datos.

Datos personales como infraestructura

El tercer conjunto de metáforas que destaca Calleja-López (2018, p. 18) se basa en la consideración de los datos como un bien público, como en el caso de los modelos de datos abiertos, haciendo el símil con la infraestructura. El supuesto implícito es que el Estado tiene que desempeñar un papel clave en la provisión de datos en condiciones concretas. Es decir, los datos provenientes de servicios públicos y procesos e infraestructuras de, por ejemplo, una ciudad tendrían que ponerse a disposición de todas las personas como datos abiertos. Aquí las condiciones para el tratamiento y uso de estos datos serían las mismas tanto para corporaciones (independientemente de su tamaño) como para la ciudadanía, y el fin de su disponibilidad estaría vinculado a prácticas como la innovación, la transparencia o la eficiencia.

La metáfora pasa, según el autor citado, por entender los datos como los caminos y los puentes de la economía digital. Esto puede implicar también una política de datos no tan disponibles para la ciudadanía pero orientados a garantizar la calidad de los mismos y el interés público. Aquí los datos se explotarían a través de paneles de control de las ciudades para la operatividad del «gobierno como un sistema inteligente» y las «ciudades inteligentes» (Calleja-López, 2018, p. 18).

Si bien las primeras dos metáforas harían referencia al uso y empleo de los datos personales definidos al comienzo, esta última implicaría la decisión de tomar o no algunos datos de carácter personal y combinarlos con otros tipos de datos. Así, el volumen de afluencia de personas en el transporte público se puede basar en los datos de geolocalización de los teléfonos de los pasajeros o en mecanismos de conteo instalados en los vehículos.

1.1.4. Prácticas de resistencia

En este punto, Mejías y Couldry (2019) retoman la visión del sociólogo Aníbal Quijano, el cual promulgaba que «el objetivo no era simplemente pasar de lo colonial a lo ‘poscolonial’, sino cuestionar la legitimidad fundamental del colonialismo a través de formas de pensamiento ‘decoloniales’» (Mejías y Couldry, 2019, p. 93). Si bien Quijano estudió el legado del colonialismo histórico, su diagnóstico resulta de óptima translación al colonialismo de datos que Mejías y Couldry investigan:

Quijano pide una “descolonización epistemológica para dar paso luego a una nueva comunicación intercultural, a un intercambio de experiencias y significaciones como la base de otra racionalidad que pueda pretender, con legitimidad, a alguna universalidad” (2007, p.177). El objetivo no es abandonar la racionalidad, ni siquiera la pretensión de “alguna universalidad”. Lo que debe abandonarse es la pretensión de universalidad absoluta que Quijano considera característica de la modernidad europea, y que encontramos reproducida en el colonialismo de datos y sus lógicas de extracción universal y administración de seres humanos a través de datos (Mejías y Couldry, 2019, p. 93).

La resistencia decolonial a la extracción de datos personales resulta un aspecto crucial de la lucha en curso por la autonomía y la autodeterminación en la era digital. A medida que las personas y las comunidades siguen lidiando con las implicaciones de la minería de datos y la vigilancia, la necesidad de resistencia a estas prácticas coloniales se hace cada vez más evidente. La resistencia decolonial implica desafiar la dinámica de poder en juego en la extracción de datos, redefinir las nociones de autoridad y propiedad en el ámbito digital y abogar por una mayor transparencia y rendición de cuentas en la forma en que se recopila y utiliza esta información.

Una de las cuestiones clave de la resistencia decolonial a la extracción de datos personales es el reconocimiento de que la minería de datos y la vigilancia no son procesos neutrales en cuanto a valores, sino que están insertos en sistemas más amplios de poder y control. Al cuestionarnos las historias y los legados coloniales que sustentan estas prácticas, las personas y las comunidades podemos comenzar a redefinirlos. Esta forma de resistencia implica recuperar la autonomía sobre los propios datos, afirmar el derecho a determinar cómo y dónde se comparte la información personal y defender políticas que prioricen la protección de la privacidad.

Para resistir eficazmente la extracción de datos personales, es esencial participar en esfuerzos colaborativos que centren las voces y experiencias de las comunidades marginadas. La resistencia decolonial requiere solidaridad y apoyo mutuo en diferentes contextos sociales, políticos y culturales, así

como un compromiso para desafiar las formas interrelacionadas de opresión que informan las prácticas de extracción de datos. Al trabajar juntos para construir modelos alternativos de gobernanza y propiedad de datos que prioricen el bienestar colectivo y la justicia social, las personas y las comunidades podremos comenzar a generar cambios significativos en la esfera digital. En última instancia, la resistencia decolonial a la extracción de datos personales no solo tiene que ver con la protección de la privacidad individual, sino con desafiar las estructuras subyacentes de poder y control que perpetúan los legados coloniales en la era digital.

De esta manera, tal y como apunta Ana Valdivia (2024, p. 4), recientes proyectos de centros de datos se han enfrentado a la resistencia de comunidades locales, como en el caso de la comunidad rural e indígena de Querétaro en el que se basa su investigación. Otras resistencias a la instalación de centros de datos la encontramos también en territorio español, como el colectivo Tu Nube Seca Mi Río², que se opone a la construcción de un centro de datos de Meta cerca del río Tajo en España por el alto coste ambiental que supondría. Profundizando en el auge de la construcción de centros de datos en España, cabe enfatizar que, por más que sus promotores afirmen que están pensados para tener un consumo de agua mucho más eficiente y funcionar con energías renovables, la falta de información al respecto cuando se les solicita, tanto a ellos como a las administraciones públicas (Castillo, 2024) no apacigua las sospechas de que finalmente operen como en otros territorios.

En este sentido, para intentar dar una respuesta a la problemática derivada del extractivismo de datos personales, estimo singularmente inspirador recoger el esquema de cuatro reguladores sociales —ley, norma social, mercado y arquitectura— propuesto por Lawrence Lessig (2006/2009), quien lo presenta de esta forma:

Ahora bien, por más que difieran las restricciones, todas son claramente interdependientes. Cada una puede respaldar u oponerse a otra. [...] Las restricciones operan conjuntamente, aunque cada una funcione de forma diferente y provoque un efecto distinto. Las normas restringen por la estigmatización que impone una comunidad; el mercado, por medio del precio que exige; las arquitecturas, a través de las constricciones físicas que imponen; y la ley, mediante el castigo con que amenaza (p. 207).

Siguiendo este esquema, nos encontramos en primer lugar con la “ley”, y cómo la muy diferente economía política del *copyright* y la privacidad ha desembocado en que la proliferación y contundencia de las leyes que apuntalan los monopolios intelectuales haya convivido con una notable escasez y

2 Véase: <https://tunubesecamirio.com/>

permisividad de las que deberían proteger la privacidad.

Con todo, es oportuno recordar que las revelaciones de Snowden y la victoria judicial de Max Schrems contra los acuerdos de transferencia recíproca de datos entre la UE y EEUU (Peirano, 2019, p. 105–110), y que propiciaron que en 2016 se aprobara en la Unión Europea un Reglamento General de Protección de Datos (RGPD), que desde su entrada en vigor el 25 de mayo de 2018 (así como su transposición a España a finales del mismo año mediante la Ley Orgánica de Protección de Datos Personal y Garantía de Derechos Digitales, LOPD-GDD) sitúa a la UE como referencia en esta materia.

En palabras de Cathy O'Neil (2016/2017), estas leyes constituyen la “artillería pesada” en materia de privacidad al pedir el consentimiento previo del uso de nuestros datos así como consagrar una cláusula de “no reutilización” que ilegaliza su venta: «Esto evita que los datos acaben en manos de las agencias de datos cuyos expedientes alimentan las calificaciones electrónicas tóxicas y las campañas de microsegmentación» (O'Neil, 2016/2017, p. 264).

Sobre las “normas sociales” y el “mercado”, es importante el empeño por concienciar a la ciudadanía sobre el derecho a la privacidad (sin ellos el RGPD no habría tenido cabida) y también por crear fundaciones o empresas focalizadas en el respeto a la privacidad. Sin embargo, hemos siempre de atender a que estas acciones no acaben en la consabida doble trampa derivada, por un lado, de que se nos haga únicos responsables de proteger la privacidad, dando por hecho que nosotros difundimos la información sin que nadie nos obligue a ello (cuando ya hemos visto que no es siempre así); y por el otro, de que se incurra en violaciones de derechos amparadas en la impunidad implícita bajo “la falacia de la autorregulación mercantil”.

Y por último nos encontramos con la “arquitectura”, entendida en un sentido tecnológico, donde la máxima ciberespacial «el código es ley» (Lessig, 2006/2009, p. 31–41) se da la mano con aquella clásica “*Privilegia ne inrogatur*” para evidenciar que «las asimetrías de poder y saber» (Brunton y Nissenbaum, 2011, párr. 12-16) contenidas en las cajas negras algorítmicas nos devuelven a una resistencia contra privilegios, esto es, contra leyes privadas. De ahí el fracaso de protocolos voluntarios de exclusión del seguimiento como el P3P (Lessig, 2006/2009, pp. 363–364) o el *Do Not Track* que, siendo técnicamente impecables, requerían de su adopción por unas corporaciones poco dispuestas a renunciar a su extractivista modelo de negocio.

1.1.5. Ofuscación³

He aquí donde emergen los diferentes instrumentos de ofuscación, definidos por Brunton y Nissenbaun (2015, p. 1) como herramientas de producción, inclusión, suma o comunicación de datos engañosos, ambiguos o falsos en un esfuerzo por evadir, distraer o confundir a los recopiladores de datos o devaluar la confianza (y el valor) de las bases de datos que generan.

La ofuscación persigue tres metas relacionadas entre sí: en primer lugar encontramos la protección, quizá la más obvia de las acciones, la cual alude a la acción directa para conseguir un efecto de minimizar un perjuicio. En segundo lugar la expresión, ya que la ofuscación existe no solo para cumplir una función meramente instrumental, sino también para amplificar las perspectivas sociales, culturales o políticas (Howe, 2015, p. 93). Y en tercer lugar, la subversión, referida al grado en que la herramienta intenta quebrantar el sistema contra el que actúa.

Estimo que la ofuscación puede entenderse mejor si se la enmarca en el concepto de «táctica», que recupero de las claves que Michel de Certeau ofrece con su caracterización de los «modos de hacer». Si bien en el Capítulo 2 desarrollaré más ampliamente esta teoría, en este momento es relevante reseñar que el filósofo francés basa sus estudios en las prácticas cotidianas que articulan aquellos desposeídos de un lugar propio para desarrollar sus actividades. A dichas prácticas, Certeau las denomina “tácticas”, en contraposición a las “estrategias” de los que se encuentran en una posición de poder. Las tácticas aprovechan el privilegio que tienen sobre el tiempo sobre una composición de lugar que les resulta desfavorable. De este modo, Michel de Certeau llega a una síntesis de los modos de hacer como:

[U]n estilo de intercambios sociales, un estilo de invenciones técnicas y un estilo de resistencia moral, es decir, una economía del ‘don’ (generosidades *à charge de revanche*), una estética de ‘golpes’ (operaciones de artistas) y una ética de la tenacidad (mil maneras de negarle al orden establecido el estatuto de ley, de sentido o de fatalidad) (Certeau, 1990, p. 46).

Esta caracterización táctica de la ofuscación concuerda con la explicación de los potenciales beneficiarios de la misma que plantean Brunton y Nissenbaum (2015, p. 79):

[A] la gente que no es rica o políticamente influyente y que no está en posición de rechazar las condiciones de participación [...] la ofuscación le ofrece cierto grado de resistencia,

³ Este apartado forma parte de un artículo que publiqué en *Teknokultura* bajo el título: “Ofuscación. Tácticas de resistencia frente al capitalismo de vigilancia” (Solera, 2024).

oscuridad y dignidad, cuando no una reconfiguración permanente del control o una inversión de la jerarquía arraigada.

Es este cariz táctico de la ofuscación el que acaba marcando la diferencia de esta «resistencia vernácula» (Brunton y Nissenbaum, 2011) frente a otras formas de protección de la privacidad.

Junto a ello, Brunton y Nissenbaum (2015) explicitan diversos motivos por los que se puede hacer uso de estas tácticas, entre los que citan el deseo de defenderse de los “peligros” de la recopilación de datos, la acción contra las citadas asimetrías de poder y saber, la ocultación de actividades legítimas o ilegítimas o para hacer que el sistema de recopilación de datos sea inservible.

Las tácticas de resistencia, entre la que se encuentra la ofuscación, que presento en este trabajo buscan agitar las aguas, encarar colectivamente el problema, proteger(nos) mediante la sobreexposición y en muchos casos, simplemente ganar tiempo mientras la reivindicación legislativa llega a buen puerto. Tienen, además una función expresiva, al enfrentarse a los investigadores que creen que las cosas, como apunta Haraway, «realmente importan solo si funcionan. O, peor, que algo importa solo si lo que yo y mis colegas expertos hacemos funciona para arreglar las cosas» (Haraway, 2016/2019, p. 23).

1.2. Preguntas de partida y objetivos

Una vez explicado esto debo añadir que parto de la humilde creencia de que la ofuscación no es la opción determinante que debe reemplazar otros modos de defensa de la privacidad, sino un complemento a ellos. Por lo que esta investigación, al igual que la ofuscación, tiene una finalidad expresiva, cuyo fin primordial es poner en valor la defensa activa y colectiva de la privacidad frente a las herramientas del extractivismo de datos personales.

Resulta importante señalar también que este estudio está enmarcado bajo el marco conceptual que aporta Certeau (1990), el cual indica que resulta un error suponer que los usuarios somos cuerpos pasivos que se guían voluntariamente por reglas establecidas. Es por ello que considero oportuno centrarme en las prácticas cotidianas para descubrir cómo operan realmente las personas, cómo se comportan frente a las estrategias del poder en lugar de poner el foco en la tecnología como un ente abstracto, despolitizado y descorporeizado.

Con la intención de abordar este dilema desde un punto de vista lo más global posible, parto del esquema, descrito más arriba, de los cuatro reguladores (las leyes, las normas sociales, los mercados y las arquitecturas tecnológicas) a los que alude Lawrence Lessig (2006/2009) en sus estudios sobre la privacidad. Junto a él, me guío siempre por la epistemología del conocimiento situado de Haraway (1991/1995), donde la objetividad feminista trata de la localización limitada y del conocimiento situado, no de la trascendencia y el desdoblamiento del sujeto y el objeto.

A partir de todo lo anterior, el objetivo general que se marca esta investigación es analizar las tácticas de resistencia al extractivismo de datos que surgen desde la ciudadanía, esto es, aquella que debe moverse en un espacio que no le es propio, pero que aun así inventa diferentes respuestas desde diferentes perspectivas como la legal, la tecnológica o la política.

Pero para llegar a este objetivo debemos atravesar una serie de objetivos más específicos como el de profundizar sobre las concepciones históricas y teóricas sobre los conceptos de vigilancia y privacidad y examinar cómo el advenimiento de la digitalización ha afectado a dichos conceptos y, por extensión, también a nosotros. Con tal fin resulta necesario reconocer los posibles riesgos que las intersecciones entre normas y tecnología generan, así como indagar sobre cómo respondemos a este extractivismo de datos personales, sin desatender nunca la reflexión que los propios actores —desarrolladores y colaboradores— de estas respuestas efectúan y las consecuencias que su uso les implican.

1.3. Posicionamiento de la investigación

El enfoque que adopto a lo largo de esta investigación es disciplinariamente pluralista, ya que incorpora conocimientos e ideas de diferentes campos tales como la sociología, la informática, la ciencia política, el derecho y la filosofía. Sin embargo, en lugar de resultar en una cacofonía discordante de perspectivas divergentes, este camino ha sido teóricamente fructífero y analíticamente complementario ya que me ha otorgado una comprensión desde distintos planos que, si bien no siempre se encuentran conectados, a lo largo de estas líneas he podido ir entretejiendo gracias a una serie de hilos conductores que han articulado este estudio y que presento a continuación.

Una primera fuente de inspiración epistemológica y metodológica para mi posicionamiento como investigadora ha sido la «*feminist standpoint theory*», originalmente propuesta por Nancy Hartsock (1983a; 1983b), la cual traducimos (Solera y Cabello, 2024, p. 7) como “Teoría del Posicionamiento Feminista” (TPF) y que Tracy Bowell (s.f., párr. 1) resume sobre tres afirmaciones principales: (1) El conocimiento está situado socialmente; (2) los grupos marginados están situados socialmente de maneras que les permiten ser más conscientes de las cosas y hacer más preguntas que los no marginados y que (3) la investigación, en particular la centrada en las relaciones de poder, debe comenzar con las vidas de aquellos que habitan un espacio que no les es propio. La concepción de la TPF de Harstsock entronca con un proyecto intelectual y político de crítica al patriarcado que ya delineó décadas atrás en la revista feminista *Quest* (Hartsock, 1975, p. 76):

El método del feminismo supone también que hemos de examinar los modos en que el patriarcado y el supremacismo blanco se entrelazan con el capitalismo. [...] El feminismo como un modo de análisis nos lleva a respetar la experiencia y las diferencias, a respetar a la gente lo bastante como para creer que ellos están en la mejor posición para realizar su propia revolución.

Esto resuena con una insistencia que recorre todo el análisis del historiador Michel de Certeau (1990, p. 255) sobre los «modos de hacer» como prácticas de invención y resistencia cotidianas:

[E]n el momento en que el aparato científico (el nuestro) es llevado a compartir la ilusión de aquellos poderes de los que es necesariamente solidario, es decir, a suponer a la muchedumbre transformada por las conquistas y las victorias de una producción expansionista, siempre es bueno recordar que no hay que tomar a la gente por idiota.

En relación a lo anterior y en su afán por «integrar cambio personal y político» (1975, p. 71), Hartsock rescata su experiencia de ver rechazado un artículo con el argumento de que «todo lo que hacía era apropiarme de una metodología de Marx y renombrarla como feminista» para sintetizar así su apuesta por «reocupar el marxismo como feminismo» (2019, p. 73). Dicha apropiación empieza por el propio concepto de «*standpoint*», que toma del original «posicionamiento proletario» marxiano para profundizar en sus implicaciones epistemológicas a la luz de la división sexual del trabajo en el marco de la vida cotidiana:

1. La vida material (la posición de clase en la teoría marxista) no solo estructura sino que pone límites a la comprensión de las relaciones sociales.
2. Si la vida material se estructura de modos fundamentalmente opuestos para dos grupos diferentes, puede esperarse que la visión de uno represente una inversión de la del otro, y que la visión de la clase dominante sea tanto parcial como perversa.
3. La visión de la clase (o género) dominante estructura las relaciones materiales en las que todas las partes están obligadas a participar, y por tanto no puede ser descartada como simplemente falsa.
4. En consecuencia, la visión disponible para el grupo oprimido ha de surgir de la lucha, y representa un logro que requiere tanto ciencia para ver bajo la superficie de las relaciones sociales en las que todos están obligados a participar, como la educación que solo puede nacer de la lucha para cambiar dichas relaciones.
5. En cuanto visión comprometida, la comprensión de los oprimidos, la adopción de un posicionamiento [*standpoint*] expone las relaciones reales entre seres humanos como inhumanas, apunta más allá del presente y comporta un papel históricamente liberador (Hartsock, 1983a, p. 285).

Años después, Fredric Jameson (2009/2013, p. 247) enfatizó la audacia de esta apropiación feminista vinculándola con la relectura de Lukács del *standpoint* como una cuestión de «prioridad epistemológica», si bien ya no del proletariado, sino de la experiencia de opresión y explotación de las mujeres. Más adelante, Sandra Harding vinculará esta teoría con la reivindicación de una «objetividad fuerte» cuya «reflexividad» fundamental resuena para Donna Haraway con su metáfora de la «difracción» como esfuerzo por marcar diferencias en el mundo (citadas en Hartsock, 2019, p. 81).

En suma, esta teoría del posicionamiento feminista posibilita para Jameson (2009/2013, p. 247) «un relativismo con principios, en el que las pretensiones epistemológicas de los distintos grupos pueden ser

inspeccionadas (y respetadas) por su “contenido de verdad” [...] o por sus respectivos “momentos de verdad”».

Jameson (2009/2013, pp. 249-250) es también el autor de una acotación clave para verter al castellano el concepto de «*standpoint*» sin recurrir al consabido «punto de vista»: «Es preferible, en nuestro propio clima lingüístico e intelectual, retraducir la figura perspectivista y orientada al sujeto del “punto de vista” a la noción estructural del posicionamiento de una determinada clase o fracción de clase en la totalidad social». De no hacerlo así, el célebre parafraseo de Hartsock por parte de Sandra Harding (1998, p. 150) que podemos considerar la síntesis más condensada de esta teoría se volvería indescifrable por tautológica: «*A standpoint is not the same as a viewpoint or perspective, for it requires both science and political struggle...*» («Un posicionamiento no es lo mismo que un punto de vista o una perspectiva, pues requiere tanto ciencia como lucha política...»). Íntimamente enlazada a esta teoría, como ya apuntaba Bowell en su síntesis de la TPF, se encuentra la teoría de Donna Haraway (1991/1995) del conocimiento situado, en la cual perfila que:

La objetividad feminista trata de la localización limitada y del conocimiento situado, no de la trascendencia y el desdoblamiento del sujeto y el objeto. Caso de lograrlo, podremos responder de lo que aprendemos y de cómo miramos. [...] Muchas corrientes en el feminismo tratan de teorizar motivos para confiar por encima de todo en las posiciones ventajosas de los subyugados. Existe una buena razón para creer que la visión es mejor desde abajo que desde las brillantes plataformas de los poderosos (Hartsock, 1983a; Sandoval, n.d.; Harding, 1986; Anzaldúa, 1987). [...] Pero la alternativa al relativismo no es totalización y visión única, que es siempre finalmente la categoría no marcada cuyo poder depende de una estrechez y oscurecimiento sistemáticos. La alternativa al relativismo son los conocimientos parciales, localizables y críticos, que admiten la posibilidad de conexiones llamadas solidaridad en la política y conversaciones compartidas en la epistemología (Haraway, 1991/1995, pp. 327-328).

Fruto de todas estas reflexiones, en esta tesis he decidido abordar el foco de estudio incorporando diferentes casos de resistencias cotidianas al extractivismo de datos, de manera similar a como resume de manera muy elocuente la investigadora Tina Sikka (2019) sus estudios sobre tecnología climática desde el posicionamiento feminista:

Para las teóricas del posicionamiento feminista, esto incluye prestar atención «a las actividades cotidianas, rutinarias y a menudo mundanas que brindan diferentes

oportunidades para ‘ver’ cómo las relaciones sociales están moldeadas por el poder y cómo la responsabilidad y la acción recaen sobre cuerpos situados de manera diferente y desigual» (Bee *et al.*, 2015, p. 5).

El otro hilo argumental que atraviesa y articula la investigación se basa en los postulados de Langdon Winner (1985) sobre las controversias acerca de la tecnología y la sociedad, más concretamente, sobre si los artefactos técnicos tienen cualidades políticas, esto es, si:

las máquinas, estructuras y sistemas de nuestra moderna cultura material pueden ser correctamente juzgados no sólo por sus contribuciones a la eficacia y la productividad, ni simplemente por sus efectos ambientales colaterales, sino también por el modo en que pueden encarnar ciertas formas de poder y autoridad específicas (Winner, 1985, p. 121).

Para profundizar en este planteamiento clásico de la filosofía de la tecnología de Winner estimo fundamental complementarlo con la tesis de Judy Wajcman (2004/2006) de que dentro de las cualidades políticas de los artefactos hemos de prestar atención específicamente a su política de género:

[L]os enfoques de los estudios sociales de la ciencia y la tecnología [...] se han mostrado ciegos antes el género, la raza, la religión, la clase, la sexualidad y otros ejes de diferencia social. El paso de los enfoques más macroestructurales a los etnográficos ha servido de contundente crítica del concepto estático de intereses sociales, pero raras veces se tiene en cuenta el «hacer» del género, ni por parte de los académicos masculinos ni por la de las personas a quienes éstos estudian. Como investigadores, muchos de ellos no son capaces de reconocer que la ausencia de las mujeres de las redes sociotécnicas no significa que dichas redes sean una zona libre de género. No cabe duda de que la red tiene política de género (Wajcman, 2004/2006, p. 157).

De esta manera, para Winner (1985, p. 125) es habitual concebir las tecnologías como instrumentos imparciales que pueden emplearse de manera positiva o negativa, para realizar el bien, el mal o algo intermedio entre los dos. Sin embargo, a menudo ignoramos si un invento específico pudo haber sido diseñado y construido de tal manera que generara un conjunto de efectos lógicos y temporales anteriores a sus usos habituales. Para este autor, si el lenguaje político y moral que utilizamos para valorar las tecnologías solo comprende categorías vinculadas a las herramientas y sus aplicaciones, esto es, si ignoramos el significado de los diseños y planes de nuestros artefactos, entonces nos volveremos ciegos frente a gran parte de lo que es relevante desde una perspectiva intelectual y práctica.

Por su parte, Wajcman (2004/2006, p. 61) añade que las tecnologías no se limitan a la etapa de innovación, sino que progresan mediante su empleo. Para ello, alude al concepto de “flexibilidad interpretativa” para subrayar la naturaleza moldeable de las tecnologías, sin llegar a afirmar que se las pueda manipular como si fueran infinitamente plásticas. Así, la presencia material de los artefactos establece restricciones a las oportunidades de reinterpretación, de lo que se deriva que el cambio tecnológico es un proceso fluctuante y diverso, en el que diferentes colectivos pueden interpretar las tecnologías de maneras muy diferentes, modificando drásticamente su significado. Además, para Wajcman (2004/2006, p. 65) no resulta sorprendente que se haya ignorado el impacto que los objetos tienen, dado que los sistemas técnicos se “naturalizan” y se descomponen en el entorno. Algo similar apunta Winner (1985, pp. 127-128) cuando explica que:

Debido a que las elecciones respecto al equipamiento material, la inversión de capital y los hábitos sociales tienden muy pronto a estabilizarse, la primitiva flexibilidad respecto a los propósitos prácticos desaparece una vez que se adoptan ciertos compromisos iniciales. En este sentido, las innovaciones tecnológicas se asemejan a los decretos legislativos o las fundamentaciones políticas que establecen un marco para el orden público que se perpetuará a través de las generaciones.

En esta misma línea, si bien en el contexto específico de Internet, Wajcman (2004/2006, p. 65) añade que las interacciones en línea no están exentas de corporeidad: a pesar de que la comunicación por ordenador modifique la interacción al suprimir las señales físicas, los cuerpos siguen desempeñando un rol crucial en lo que implica ser parte de la especie humana. Si la sociedad colabora con la tecnología, es necesario analizar las repercusiones de las relaciones de poder en el diseño de la misma:

La tecnología debe entenderse como parte del tejido social que asegura la cohesión de la sociedad; nunca es meramente técnica ni social. Antes bien, la tecnología siempre es un producto sociomaterial —una telaraña o red sin costuras que combina artefactos, personas, organizaciones, significados culturales y conocimientos. Por consiguiente, el cambio tecnológico es un proceso contingente y heterogéneo en el que tecnología y sociedad se constituyen mutuamente. De hecho, el modelo lineal de innovación, difusión y utilización ha suscitado la idea de que la tecnología no es nunca un producto acabado. Mucho después de que los artefactos abandonen el laboratorio de investigación, siguen evolucionando en las prácticas diarias de uso. La flexibilidad interpretativa de la tecnología significa que siempre existe la posibilidad de que una tecnología y sus efectos sean otros (Wajcman, 2004/2006, p. 161).

1.4. Diseño metodológico

En coherencia con el posicionamiento de la investigación descrito, surge el siguiente diseño para acceder a la información necesaria con el fin de responder a los objetivos propuestos en esta investigación.

De esta manera, he optado por partir de un relato sobre cómo la determinación por poner el cuerpo en esferas geográficas donde se desarrollaban una serie de actividades relacionadas con mi foco de estudio, me ha llevado a abordar la investigación desde una perspectiva eminentemente cualitativa, inviable de no haber tenido la posibilidad de realizar ese estudio de manera tan presencial. Es por ello que, a mi juicio, resulta ineludible atender a las condiciones materiales en que he desarrollado dicho estudio, desde el entendimiento de que ellas han tenido un considerable impacto en mi labor.

Otra de las consideraciones para la elaboración de la estrategia metodológica ha tenido que ver con la combinación de la teoría —principalmente crítica— y las prácticas —de resistencia— escogidas, con las que establezco un diálogo continuo. Es la suma de todo ello lo que me ha llevado a dar un paso más hacia la práctica con la incorporación de lo estudiado a un proyecto en marcha al que aludiré en el punto 1.4.4.

1.4.1. Situaciones de conocimiento

A lo largo de estos años mi investigación me ha llevado a ocupar y habitar diferentes espacios que han promovido que emergiesen ciertas cuestiones que no había planteado al comienzo de este estudio y que, sin embargo, no hacen sino enriquecerlo. A continuación voy a relatar en un sentido más o menos cronológico algunos hitos y motivos que me han conducido a presentar este escrito tal y como es.

Si bien me resulta difícil determinar una fecha concreta para el inicio de esta investigación, puesto que ha coincidido con otras pesquisas y proyectos que he ido realizando a lo largo del tiempo desde mis primeros años de formación universitaria, quizá podría enmarcar su inicio en el año 2018 por la concatenación de una serie de sucesos: el primero es que el 25 de mayo de ese año vencía el plazo fijado por la UE para la implantación del Régimen General de Protección de Datos aprobado el 14 de abril de 2016. En aquel tiempo yo trabajaba para un *e-commerce* y fui la encargada de implementar las modificaciones pertinentes que la nueva normativa exigía, por lo que estaba bastante familiarizada con el tema en sus niveles más prácticos. Por otro lado, el estallido del caso Cambridge Analytica en marzo nos demostró hasta qué punto las técnicas de perfilado y publicidad personalizada podían afectar a los resultados electorales.

En ese mismo tiempo durante las conversaciones que mantenía con el profesor Florencio Cabello en el Centro Social y Cultural de Gestión Ciudadana *La Casa Invisible*, sobre estas y otras cuestiones, me puso en conocimiento de una serie de prácticas críticas en Internet conocidas como «ofuscación». Según me contó entonces, quien le había puesto tras la pista de ellas fue el investigador y activista de la plataforma de democracia digital X.net Sergio Salgado, con ocasión de su invitación como ponente (junto a Simona Levi) a la materia Tecnologías Aplicadas a la Publicidad y las Relaciones Públicas en la UMA en noviembre de 2014. Tirando de ese hilo, Florencio llegó a la publicación del libro *Obfuscation: A User's Guide for Privacy and Protest* (2015), en el que Finn Brunton y Helen Nissenbaum presentaban este original concepto de resistencia cotidiana que llevaban años estudiando y promoviendo activamente y que he definido anteriormente. La ofuscación me pareció una idea tan potente que durante un tiempo me dediqué a profundizar en ella y encontrar otros ejemplos ajenos a los que presentaban los autores y que implicaban los propios cuerpos para ofuscar. Fruto de ello, el 18 de diciembre de 2018 Florencio me invitó a presentar mis primeros progresos en una conferencia para su alumnado de Tecnología de la Comunicación Audiovisual del Grado de Publicidad y Relaciones Públicas de la Facultad de Ciencias de la Comunicación de la UMA.

Estas indagaciones no se detuvieron aquí, puesto que durante los meses de confinamiento por la Covid-19, Florencio y yo estuvimos (tele)trabajando en lo que se materializó más tarde en un capítulo encargado por Jesús Sabariego para el libro *Algoritmos* (2020) que coeditaba en la editorial Tirant lo Blanch. Esta publicación, que titulamos *Ofuscación algorítmica: Obnubilación táctica para una privacidad por las nubes*, sería la base sobre la que, ya parcialmente desconfinados, preparé a finales de 2020 mi proyecto de tesis para el acceso al Programa de Doctorado en Educación y Comunicación Social de la Universidad de Málaga, en el que fui aceptada en febrero de 2021.

Si continuamos la línea cronológica he de incluir en este punto que en abril de ese mismo año me sumé al equipo de trabajo del Proyecto de Investigación denominado *Narrativas emergentes sobre la escuela inclusiva desde el modelo social de la discapacidad. Resistencia, resiliencia y cambio social*, financiado por el Ministerio de Ciencia e Innovación (con referencia RTI2018-099218-A-I00), el cual puede parecer de entrada desconectado de la temática de esta tesis, si bien más tarde se revelará como muy importante para la misma.

Volviendo al concepto de “ofuscación”, mi primera oportunidad de presentarlo a la comunidad académica fue en noviembre de 2021 en el IV Congreso Internacional *Move.net* sobre Movimientos Sociales y Tecnologías de la Información y la Comunicación celebrado en la Facultad de Comunicación de la Universidad de Sevilla. En ese marco, y con la inestimable actuación como moderadora de la mesa

de comunicaciones de Guiomar Rovira, expuse una comunicación titulada *Ofuscación: Generar ruido para vencer a la vigilancia*. De la grata acogida que me fue dispensada durante la presentación y el coloquio da buena muestra el hecho de que en febrero de 2022 fuera seleccionada por los organizadores para enviar un manuscrito basado en mi comunicación para el monográfico titulado *Deliberación democrática en la Red: del diálogo al ruido digital* que tenían concertado con la revista sobre Cultura Digital y Movimientos Sociales: *Teknokultura*. De este modo, en el número 20 de dicha revista apareció mi primer artículo en solitario, que lleva por título: *Ofuscación. Tácticas de resistencia frente al capitalismo de vigilancia*.

Apoyada en estos avances, a lo largo de 2022 fui acotando el foco de estudio, ampliando algunos conceptos clave y comenzado las revisiones históricas y teóricas sobre los conceptos de vigilancia, privacidad, específicamente con los problemas relacionados con la privacidad en público, la vigilancia digital y la influencia que los nuevos dispositivos pueden tener en las relaciones sociales y en nuestros cuerpos. Junto a ello, profundicé en cómo desde la ciudadanía habían surgido algunas iniciativas para subvertir esto. Lo cierto es que para entonces ya había delimitado algunos casos de estudio sobre el área legal y tecnológica, pero me encontraba en la búsqueda de casos que trascendiesen estas resistencias. En concreto, me interesaba especialmente estudiar el papel que herramientas de código libre podían desempeñar para realizar una privacidad por defecto o desde el origen en la tecnología con vistas a la construcción de sistemas alternativos de comunicación y participación democráticas.

Motivada por ello y por la apuesta por poner el cuerpo allí donde podía acercarme mejor a mi foco de estudio, al que ya por entonces tenía decidido incorporar el concepto de “procomún” (Cabello, 2019, pp. 37-46), entre los meses de noviembre del 2022 y febrero de 2023 realicé una estancia de investigación con el grupo Digital Commons Research Group (DIMMONS) que dirige Mayo Fuster en el Internet Interdisciplinary Institute (IN3) de la Universitat Oberta de Catalunya (UOC). Más concretamente, mi estancia en Barcelona giró en gran medida en torno al espacio de trabajo de DIMMONS en el *Canòdrom, Ateneo de Innovación Digital y Democrática*, perteneciente al Ayuntamiento de Barcelona y dirigido por Arnau Monterde, a quien Florencio Cabello y yo habíamos ido a visitar el 12 de julio anterior aprovechando nuestro viaje con motivo del *I Curso Internacional de Educación Digital Democrática y Open EdTech* organizado por Simona Levi en Barcelona en esas mismas fechas. Con esta doble acogida, pude comenzar mi investigación sobre la defensa de la privacidad en la plataforma Decidim, una plataforma digital de participación política construida por el Ayuntamiento de Barcelona y basada en código libre (con una licencia *GNU Affero General Public License v3.0*), que puede leerse, comentarse, mejorarse y copiarse en la plataforma de programación colaborativa Github.

Si bien a mi llegada era vagamente conocedora de la plataforma, fueron los compañeros del grupo de investigación Ricard Espelt y Enric Senabre quienes me pusieron tras la pista del proyecto piloto *Democracia digital y procomún de datos (DDDC)*. Como averigüé, este DDDC era una iniciativa impulsada unos años atrás por el proyecto DECODE (DEcentralised Citizens Owned Data Ecosystem⁴) que junto con Decidim, tenían el propósito de tratar en profundidad la cuestión de los procomunes de datos.

Aprovechando mi vuelta por Navidad a Málaga, reelaboré la ponencia que había preparado para mi primera clase de 2018 y el 19 de diciembre de 2022 la presenté ante el alumnado de Tecnología de la Comunicación Audiovisual de ese curso. Esta labor, muy enriquecida por la investigación y los contactos realizados en Barcelona, me ayudó a recapitular y visualizar los cambios que habían sucedido a lo largo de este tiempo en mi proyecto de tesis.

Finalizando mi estancia en Barcelona se me presentó la oportunidad de poder materializar una segunda que venía planeando desde hacía tiempo con mi director. Y es que a comienzos de 2023 la UMA convocó en el marco de su *II Plan Propio de Investigación y Transferencia* sus ayudas para la realización de tesis con mención de doctorado internacional, y yo presenté una solicitud para disfrutar de una estancia de investigación en Viena junto al grupo de de investigación *Políticas y Género (Gender and Politics)* coordinado por la Dra. Birgit Sauer, perteneciente al Departamento de Ciencias Políticas de la Universidad de Viena (Austria). Tras recibir una de las valoraciones más elevadas, pude conseguir la ayuda y durante los meses de septiembre, octubre y noviembre de 2023 tuve la oportunidad de trasladarme a la capital de Austria para mejorar mis conocimientos sobre metodologías de investigación en ciencias sociales con perspectiva de género, gracias principalmente a la ayuda de la investigadora Alev Cakir, perteneciente a este grupo. Las pautas, consejos y métodos, que me ofreció tanto a la hora de preparar mis entrevistas, como de abordar la posterior transcripción y tratamiento de los datos, me resultaron de gran utilidad de cara afrontar aquellas que tenía previstas durante mi estancia.

En este sentido, también quisiera destacar que durante los meses que estuve en Viena tuve la oportunidad de conversar en profundidad con uno de los abogados pertenecientes al grupo de investigación y activismo jurídico del Centro Europeo de Derechos Digitales NOYB (acrónimo de “None Of Your Business”). Conocer y contar con su testimonio de primera mano me ha permitido enriquecer mi investigación de modo singular, ya que el asunto de la defensa de la privacidad y la regulación de la vigilancia digital son temas de tal actualidad que su investigación conlleva una constante actualización de la información con respecto a ella, y para ello la labor de NOYB resulta única a escala

⁴ Véase: <https://decodeproject.eu/>

europea, si no mundial (no en vano de sus reivindicaciones y litigios en la UE han partido los grandes hitos en este campo de la última década larga).

Finalmente, dentro de mi proyecto para esta estancia tenía igualmente previsto profundizar en el estudio de caso de *Fango*, un dispositivo desarrollado por Martín Nadal dentro del programa European Media Artist in Residence Exchange de la European Media Art Platform (EMAP/EMARE)⁵. Y ello era posible dado que este artista y programador creativo —en teoría— residía en Linz (Austria) y trabajaba en el programa Interface Cultures programme de la Universidad de Arte y Diseño de esta ciudad situada a menos de dos horas de distancia en tren de Viena. Digo en teoría porque he de confesar aquí que, pese a la información de la que disponía en ese sentido, cuando por fin contacté con Martín Nadal éste me comunicó que había cambiado su residencia a la ciudad de Berlín.

Este giro de los acontecimientos, en lugar de anular mis planes, me hizo intentar llegar un poco más lejos en mi investigación, pues en la ciudad de Berlín también reside uno de los investigadores clave para mi estudio, Adam Harvey. El trabajo de este artista e ingeniero de *software* se centra en tecnologías de visión por computación, privacidad y vigilancia. De este modo, mientras preparaba mi encuentro con Martín Nadal, tuve la suerte de obtener una respuesta positiva de Harvey a la posibilidad de realizarle una entrevista en persona en el mes de noviembre de 2023, por lo que se tornó muy viable poder desplazarme a Berlín y reunirme con ambos.

Al margen de mis actividades y reuniones tanto en Viena como en Berlín, durante los meses de mi estancia también me trasladé a la ciudad de Barcelona, dado que los días 18, 19 y 20 de octubre de 2023 se celebró el *Decidim Fest 2023*, congreso anual entorno a la herramienta y que llevaba por significativo título *Democracia, Tecnología e Inteligencia Artificial Colectiva*. Asistir a este congreso no solo me permitía permanecer informada de las novedades sobre la plataforma sino también mantener vivo el contacto con aquellos compañeros y compañeras del *Canòdrom* con los que compartía mis dudas y avances sobre el estudio de caso de Decidim.

De vuelta de la estancia el 17 de diciembre de 2023 tuve la oportunidad de repetir la ponencia para el alumnado de Tecnología de la Comunicación Audiovisual de la UMA, en la que incluí los avances en la investigación que había ido realizando a lo largo de estos últimos meses, con especial incidencia en las últimas iniciativas de NOYB, sobre el que varias alumnas del Grado estaban ya indagando.

En torno a esta fecha concluía también el proyecto de investigación *Narrativas emergentes sobre la escuela inclusiva desde el modelo social de la discapacidad. Resistencia, resiliencia y cambio social* (RTI2018-099218-A-I00),

⁵ Véase: <https://www.martinnadal.eu/fango>

pero los investigadores principales del mismo, Ignacio Calderón y Teresa Rascón, ya estaban sentando las bases del que sería el próximo, para cuyo equipo de trabajo volvieron a contar conmigo: el Proyecto de Investigación *Narrativas emergentes para la construcción de escuelas inclusivas*, que también recibía financiación del Ministerio de Ciencia e Innovación (con referencia PID2022-140193OB-I00).

A comienzos de 2024 recibí otra noticia que venía esperando desde otoño de 2023 (pues ese verano me lo anunció Xabier Barandiaran, uno de los coordinadores de Decidim) y que sería clave para el cierre de mi tesis: por fin se había publicado en la editorial Springer el libro blanco elaborado por el grupo promotor de Decidim, titulado *Decidim, a Technopolitical Network for Participatory Democracy Philosophy, Practice and Autonomy of a Collective Platform in the Age of Digital Intelligence* (2024). Ello supuso una singular oportunidad para dar a conocer este proyecto a la comunidad universitaria y a la ciudadanía malagueña en general. De esta manera, gracias al apoyo de la sección UMA del Sindicato de Apoyo Mutuo (SiAM), Florencio y yo pudimos organizar una charla-coloquio sobre el libro en *La Casa Invisible* y una charla-taller sobre Decidim en la Facultad de Ciencias de la Comunicación de la Universidad de Málaga los días 18 y 19 de abril, respectivamente, contando para ello con dos de los coautores e integrantes del grupo motor de Decidim: Carol Romero y Antonio Calleja-López.

Tras este fructífero encuentro, mi director de tesis y yo llegamos a una conclusión: si el proyecto de investigación por la educación inclusiva antes citado —y del que ambos formamos parte— quería obtener el alcance internacional que se había propuesto para llevar a cabo su trabajo con las escuelas, instalar nuestro propio Decidim, con las modificaciones pertinentes, podría ser la herramienta que necesitábamos, al permitirnos contar con la mayor autonomía posible de plataformas externas y cambiantes para llevar a cabo el mencionado propósito de internacionalización (especialmente con iniciativas de América Latina). Es en este punto donde intersecciona mi investigación doctoral con mi colaboración con el citado proyecto de investigación, todo ello en el marco de la investigación-acción participativa (IAP) que caracteriza a este último y que, en nuestro caso, se ha materializado en la instalación, configuración y formación inicial de una instancia de Decidim para el colectivo Quererla es Crearla impulsado por nuestro proyecto de investigación.

1.4.2. Revisión bibliográfica

Uno de los retos iniciales que hallé durante las primeras etapas de mi investigación fue la escasez de literatura en castellano que abordara temas como la vigilancia en la era digital o la evolución del derecho a la privacidad. A su vez, estos temas tan cruciales para mi estudio a menudo se encontraban desarrollados de manera específica en una disciplina concreta, lo que dificultaba la existencia de un

diálogo interdisciplinario. Además, en reiteradas ocasiones se presentaban problemáticas como la vigilancia masiva como cuestiones novedosas sin atender a su contexto histórico, por lo que podían quedar desvirtuadas. Es por estas razones que encontré necesario establecer un marco integral que aglutinase varios estudios y puntos de vista que permitieran una comprensión holística de esta cuestión compleja aunando los enfoques histórico y conceptual. De este propósito nace la voluntad de emplear la revisión bibliográfica narrativa como herramienta metodológica para este estudio, la cual, para Baumeister y Leary (1997, p. 312) resulta valiosa cuando uno intenta vincular muchos estudios sobre diferentes temas, ya sea con fines de reinterpretación o interconexión.

Para la selección de los textos tuve en cuenta que éstos hubiesen sido escritos por personas reconocidas en sus ámbitos, y en muchos casos también prioricé que aportasen una visión crítica del foco de estudio. En esta línea, destaco las obras de renombrados sociólogos como David Lyon (1994, 2001, 2003a, 2003b, 2006, 2007, 2015, 2018, 2022), quien fue director del Centro de Estudios de Vigilancia de la Queen's University en Kingston; Armand Mattelart (1995/2005, 2001/2007, 2007/2009, 2014/2015), autor imprescindible en los estudios de comunicación, o el propio Anthony Giddens (1985, 1987, 1990). Junto a ellos, me he valido ampliamente de los trabajos del profesor emérito del Instituto Tecnológico de Massachusetts (MIT), Gary T. Marx (1988, 2002, 2007), y de la profesora emérita en la Harvard Business School, Shoshana Zuboff (2004, 2014, 2019/2020).

Por otro lado, me ha resulta inspirador confrontar estas visiones provenientes del campo de la sociología con aquéllas otras propias de, por ejemplo, la antropología, como es el caso de los escritos de David Graeber (2015, 2022), o de la perspectiva feminista, con obras de la filósofa e historiadora Silvia Federici (2004/2010, 2020/2022), a través de cuya mirada he podido revisitar escritos clásicos de Karl Marx. Finalmente, he encontrado fructífero combinar estas lecturas con las aportaciones también críticas de Evgeny Morozov (2019, 2022) y de John Bellamy Foster y Robert W. McChesney (2014).

En el campo de la filosofía, destaco en primer lugar a una serie de autores franceses: Michel Foucault (1975/2002, 1978, 2003/2007, 2004/2006), por la importancia de sus estudios sobre el control y la disciplina; Gilles Deleuze (1977/1983, 1980/1988, 1990/1995), por su teoría de las sociedades de control, y Michel De Certeau (1974/1993, 1990), por su estudio sobre las resistencias cotidianas al poder. Por su mayor cercanía (no solo temática o cronológica, sino también por la posibilidad que he tenido de conocerles en Málaga en torno a la Librería Suburbia inaugurada el de 23 de abril de 2021) también he acudido a otros filósofos como Maurizio Lazzarato (2008) y Gerald Raunig (2015/2023) para completar los pensamientos de aquellos clásicos franceses. Y sin duda otra filósofa de referencia en las páginas que siguen será la profesora de filosofía y ética en la Universidad de Oxford, Carissa

Véliz, quien ha realizado recientemente extensas investigaciones sobre las consecuencias éticas de vulnerar el derecho a la privacidad (2021, 2022a, 2022b, 2023, 2024).

Sobre Certeau, he de aclarar aquí que me he valido de las traducciones realizadas por Florencio Cabello, tanto para su tesis doctoral defendida en el año 2006, como para el prólogo de la versión en castellano de la obra colaborativamente traducida de *Two Bits* de Christopher Kelty (2019) —en cuya traducción yo también participé— en lugar de la obra traducida por Alejandro Pescador en el año 2000. El motivo de esta elección no ha sido otro que mi familiaridad en el estudio a lo largo del tiempo de este autor a través de las traducciones de mi director de tesis. Sin embargo, a lo largo de este trabajo he optado por simplificar el citado de la obra remitiendo a la original en francés.

Las lecturas sobre derecho —y filosofía del derecho— que resalto aquí son las del profesor de Washington Daniel J. Solove (2001, 2003, 2006, 2009, 2011), el catedrático de Harvard especializado en “ciberderecho” Lawrence Lessig (2006/2009) y la experta en *copyright* y privacidad en Internet Julie E. Cohen (1996, 2000, 2012, 2013, 2019). Sobre estos temas, quisiera destacar también las imprescindibles aportaciones teóricas de la profesora de ciencias de la información Helen Nissenbaum (2004, 2015), cuya teoría sobre la integridad contextual resulta clave para esta investigación.

Otros autores que me han aportado conceptos clave para el estudio han sido Didier Bigo (2006), creador del concepto de “*banóptico*”, Roger Clarke (1988, 1994b), quien definió términos como “*dataveillance*” o el de “persona digital”; al igual que Kevin Haggerty y Richard Ericson (2000), quienes propusieron el original término de “doble de datos”.

Por último, quisiera reseñar la utilidad de estudios más recientes como los de Markus Kienscherf (2022) y Paola Ricaurte Quijano (2023) para comprender cómo opera el extractivismo de datos personales, así como los de Tiziano Bonini y Emiliano Treré (2024) sobre la resistencia a este extractivismo.

A esta combinación de obras de los autores y autoras citados se suman otros libros, artículos e informes de temáticas relacionadas, pero también el uso de artículos periodísticos que reflejan el salto de estos temas de la academia a los medios de comunicación (o viceversa) como reflejo de la contemporaneidad y la notoriedad que entrañan. La agregación, análisis, síntesis y contraposición de todo ello es lo que conforma la revisión bibliográfica y la construcción del marco teórico de esta investigación, el cual conforma un bagaje común de cara a la revisión de los estudios de caso seleccionados.

1.4.3. Estudios de caso

En una segunda fase de la investigación he seleccionado para su estudio diferentes ejemplos de tácticas de resistencia al extractivismo de datos que surgen desde la ciudadanía, basándome en los anteriormente citados cuatro reguladores —ley, norma social, mercado y arquitectura— a los que apela Lessig (2006/2009, p. 207).

Dicho estudio ha sido desarrollado a través del método de estudio de caso que, tal y como explica Stake (1995), tiene como característica básica abordar de forma intensiva una unidad, la cual puede referirse a una persona, una familia, un grupo, una organización o una institución. El empleo de los estudios de casos desempeña un papel fundamental en este estudio, ya que ayuda a cerrar la brecha entre la teoría y la práctica al proporcionar ejemplos concretos e ilustraciones de conceptos teóricos que se suceden en la cotidianidad.

Selección de los casos de estudio

Después de leer el apartado 1.4.1. quizá se vislumbre ya cuáles han sido los escogidos, pero estimo importante recalcar que, lejos de guiarme por la aleatoriedad a la hora de elegir los ejemplos que presento en esta investigación, éstos han sido seleccionados basándome en tres criterios principales.

El primero ha sido ajustarme a la ya citada distinción clásica de cuatro reguladores sociales con la intención de aportar una visión diferente que ponga en valor la capacidad de la ciudadanía de reapropiarse de espacios que les han sido tradicionalmente desposeídos, como pueden ser la jurisprudencia o el conocimiento en programación informática.

El segundo se encuentra íntimamente ligado al primero, puesto que al posicionarme desde una perspectiva de la protección de la privacidad de manera colectiva, he buscado casos cuyos resultados se encuentren ampliamente disponibles para —y en algunos ejemplos incluso sean replicables por— el público en general, empezando por el criterio de que apuesten por el *software* libre y hagan accesible su información a través de licencias abiertas.

El tercer criterio responde a un posicionamiento metodológico en el que he primado, dentro de lo posible, el encuentro presencial con mis sujetos de estudio, es decir, la oportunidad de poner el cuerpo allí donde se encontrase el foco de mi investigación. Y es que en una tesis que critica radicalmente el «extractivismo» me parecía importante contraponerle una apuesta epistemológica por la «relacionalidad» tal y como la recoge Dan McQuillan (2022, p. 116) del pensamiento feminista:

El cuidado parte de una preocupación por las fronteras y exclusiones que operan en una sociedad estratificada [...], promueve enfocarse en el modo en que los seres se vuelven cosificados [*objectified*] y reemplaza la reductividad aplanadora por una perspectiva que asume como fundamental la relacionalidad.

Este último criterio me ha llevado, por cuestiones logísticas, materiales y comunicativas, a seleccionar casos que se encuentran ubicados en Europa y que tienen la capacidad de comunicarse en inglés o en castellano. A partir de este enfoque inicial, los casos de estudio seleccionados han sido los siguientes:

- **Tácticas de litigación colectiva por la privacidad en la UE: NOYB y el marco de regulación de la privacidad en la UE.**

El mencionado Centro Europeo de Derechos Digitales NOYB, acrónimo de *None Of Your Business* (que podríamos traducir como “No es asunto tuyo”), es una organización sin ánimo de lucro con sede en Viena (Austria), establecida en 2017 con un enfoque paneuropeo. Co-fundada por el abogado austriaco y activista de la privacidad Max Schrems, NOYB tiene como misión promover tanto una «litigación colectiva táctica» (Cabello, 2024, p. 968) como iniciativas mediáticas en apoyo del Reglamento General de Protección de Datos (RGPD). Si bien muchas organizaciones protectoras de la privacidad centran su atención en los gobiernos, NOYB pone su atención en los problemas de privacidad y sus posibles violaciones por parte del sector privado.

El grupo NOYB representa un ejemplo único tanto en el plano legal como en el comunicativo en materia de defensa de la privacidad desde el marco regulatorio europeo, del cual he considerado oportuno realizar, previamente a la presentación del caso, un repaso por su legislación más relevante. En gran parte le atribuyo esta singularidad a NOYB debido a que la organización cuenta con una completísima plataforma *wiki* gratuita y abierta denominada GDPRhub⁶ donde, con el propósito del conocimiento compartido y procomún creativo, opta por divulgar (la mayoría de) su investigación sobre la aplicación del RGPD en la UE y el Espacio Económico Europeo (EEE) de manera pública y sin coste.

- **Tácticas de resistencia expresiva frente al extractivismo de datos personales: Ofuscación, generar ruido para vencer a la vigilancia digital.**

Mi inclinación por el estudio de la ofuscación (previamente definida en el punto 1.1.5.) parte de mi convencimiento de la ineficacia y la imposibilidad de una abstinencia digital, dado que resulta cada vez

⁶ Véase: <https://gdprhub.eu/>

más complicado eludir los espacios pertenecientes a organizaciones extractivistas de datos mientras desarrollamos nuestras tareas educativas, laborales o sociales. Ante ello estimo cada vez más urgente explorar y poner en conocimiento las posibles alternativas con las que podemos contar para proteger nuestra privacidad de manera colectiva, así como expresar nuestra disconformidad o presencia crítica.

A lo largo de su investigación, los citados Brunton y Nissenbaum (2011, párr. 29–50) han realizado una clarificadora diferenciación entre distintos tipos de ofuscación —por más que luego pueden llegar a combinarse— y presentado ejemplos de ello. Mi particular aportación en esta línea consiste en el estudio en profundidad de los trabajos de dos investigadores y activistas residentes en territorio europeo, los mencionados Adam Harvey y Martín Nadal. No en vano, pese a que presentan trayectorias diferentes, ambos coinciden en una representación de la problemática de la vigilancia digital a través del arte, especialmente mediante soluciones tecnológicas que emplean *software* libre para ilustrarla y desafiarla. De esta forma, tal y como comentaba Harvey en una entrevista realizada en 2017:

En cuanto al papel del arte en mi obra, suelo considerar que el arte funciona como un espacio donde las cosas pueden existir pero que aún no tienen cabida. El arte puede funcionar como un lugar para ideas tan imposibles como la zona desmilitarizada entre Corea del Norte y Corea del Sur, donde la paz y la neutralidad intentan existir pero aún no tienen cabida (Harvey, citado en Herrmann, 2017, párr. 22).

- **Tácticas recursivas para una democracia participativa: El caso de Decidim.**

Los impulsores de Decidim (Barandiaran *et al.*, 2024, pp. 1–3) definen esta pionera plataforma como una infraestructura digital para la democracia participativa. Se trata de una iniciativa construida íntegra y colaborativamente con *software* libre y configurable para ser utilizada como una red política para la participación democrática. Sin embargo, la característica que hace aún más estimulante el estudio de la plataforma Decidim es que su gobernanza se organiza alrededor de MetaDecidim: un espacio de encuentro, un proceso y una comunidad participativa, orientada a decidir, diseñar y producir de manera colaborativa y democrática múltiples aspectos del devenir del propio proyecto.

Como he comentado anteriormente, durante mi estancia en Barcelona, pude conocer los distintos procesos en los que esta plataforma y su comunidad se vieron embarcados hacia una defensa de la privacidad de sus usuarios. En particular, me centré en la vinculación de Decidim con el mencionado DECODE, un proyecto europeo H2020 que perseguía construir herramientas legales, tecnológicas y socioeconómicas con las que la ciudadanía pudiera recuperar el control de sus datos y generar un mayor

beneficio común de los mismos, es decir, una iniciativa que trata de contribuir a los procomunes de datos. Por todo lo expuesto estoy cada vez más convencida que Decidim constituye (en el amplio sentido de la palabra) un ejemplo clave para comprender cómo podemos transitar de las resistencias a las organizaciones extractivistas de datos hacia modelos autogobernados cuya preservación de la privacidad es eje principal de su construcción.

Técnicas de investigación empleadas y análisis de la información obtenida

Si bien algunas de las técnicas de investigación empleadas en estos estudios (como la recopilación de la información) son comunes a todos, las características propias de cada uno de los casos han propiciado que haya empleado una u otra técnica o variables de las mismas para su correcto desempeño.

De esta manera, en el caso de NOYB, la persona entrevistada (a la que tan solo puedo citar de esta elusiva forma) me requirió que nuestra conversación no fuera registrada, por lo que la información que se refleja en esta investigación procede de técnicas de información secundarias seleccionadas a partir de esta charla. En contraste, en los dos casos que involucraban ejemplos artísticos prácticos de ofuscación, pude documentarlos mediante el empleo de entrevistas en profundidad registradas, a Martín Nadal y Adam Harvey, aunque ésta última no aparece transcrita en este trabajo a petición del entrevistado.

El caso de estudio de Decidim ha resultado más complejo y lo he abordado con un enfoque que quizá podría describir como inmersivo. Así, desde las primeras tomas de contacto a través de la recopilación de la información hasta la implantación de nuestro propio Decidim para el desarrollo de las tareas de nuestro grupo de investigación, ha existido un camino mediado por muy diversas técnicas y recursos que englobo bajo la rúbrica metodológica de la “observación participante”: entrevistas y charlas informales, asistencia a cursos, talleres y congresos sobre el tema, e incluso la organización de nuestros propios seminarios (presenciales en Málaga pero también virtuales) donde aprovechamos la toma de información de primera mano necesaria para esta investigación con el fin de ofrecerla a otros públicos.

A partir de esta diferenciación, a continuación paso a desglosar las técnicas de investigación empleadas en sí mismas, sin referencia concretas a los casos:

- **Recopilación de información**

Como primera toma de contacto con el foco de estudio acudí a diferentes fuentes secundarias de información, como pueden ser la literatura científica, artículos periodísticos, entrevistas, asistencia y/o posterior visionado de charlas en las que participaban los protagonistas de los casos de estudio o sus propias páginas *web*.

Debo señalar aquí que esta última ha resultado la fuente de información más fructífera, dado que todos los casos estudiados se caracterizan por la minuciosa recopilación y difusión de información que realizan, lo cual resulta por lo demás plenamente lógico teniendo en cuenta que uno de los criterios de selección de los casos ha sido su compromiso con el *software* libre y, por extensión, el conocimiento libre.

- **Entrevistas en profundidad**

Las entrevistas en profundidad realizadas, como técnicas generadoras de información primaria, presentan ventajas como la riqueza informativa de primera mano. El hecho adicional de haber podido realizarlas todas en persona, intentando minimizar las tecnologías que mediaban en ellas, ha supuesto una ruptura del distanciamiento entre investigadora e investigado que estimo muy propicia. Asimismo, dichas entrevistas han favorecido la comprensión de los temas tratados debido al contacto directo con expertos en la materia capaces de enriquecer, corroborar o refutar posibles argumentos planteados durante el análisis documental.

Para establecer un orden o secuencia utilicé un guión predeterminado, integrado por preguntas abiertas, y diseñado a partir de la información recabada en la fase documental e incluyendo los principales temas y subtemas como puntos a tratar a lo largo de la conversación. Sin embargo, de cara a realizar una conversación fluida y cómoda para el entrevistado, se primaron las cuestiones que él indicaba como más relevantes para su correcta explicación. Por tanto, se comenzó por un breve recorrido por su trayectoria profesional para después abordar temas como las tensiones entre privacidad y vigilancia digital y su visión sobre diferentes aspectos relacionados con su ámbito de trabajo, así como prospectivas que podían tener sobre el tema.

He de mencionar aquí que, en el caso de las entrevistas no registradas, éstas me sirvieron como guía para detectar cuáles eran los temas de interés sobre los que trabajaban mis interlocutores para luego buscar y hacer uso de la información que la organización había publicado o difundido al respecto en charlas y conferencias.

En cuanto al procedimiento de recogida de información, en aquellos casos que la persona entrevistada me ha dado su consentimiento, éste ha consistido en la grabación de las entrevistas en soporte digital. Una vez recogida así la información, he procedido en todos los casos a transcribirla y remitirla a los entrevistados para su revisión a través de un documento compartido de la plataforma CryptPad⁷, la cual ofrece una suite ofimática de *software* libre que permite realizar documentos colaborativos y sincronizar

⁷ Véase: <https://cryptpad.fr/>

los cambios en los mismos en tiempo real de forma segura. Esto es debido a que todos los datos están cifrados de extremo a extremo, por lo que ni el servidor ni sus administradores tienen forma de ver el contenido que se está editando y almacenando.

Tras este proceso realicé un análisis de discurso y de contenido con objeto de identificar unidades de sentido, detallando los argumentos que respondían a los objetivos de la investigación, así como aquéllos que confirmaban, avalaban y enriquecían los resultados de mis pesquisas. En este sentido, el análisis de las entrevistas en profundidad ha perseguido un fin específico y concreto: la comprensión del mundo tal y como el propio entrevistado la construye (Vargas Jiménez, 2012).

Dichas tareas de análisis han comenzado siempre, pues, con la escucha activa de las entrevistas grabadas y la lectura detenida del contenido transcrito. En el análisis del discurso he contemplado dos dimensiones, el texto y el contexto. Por ello, la contextualización de los argumentos expresados por el entrevistado ha sido de orden transversal, esto es, ha acompañado todo el proceso de estudio. El objetivo fundamental era la búsqueda y sistematización de las categorías utilizadas por el entrevistado. Este recurso a las categorías ha permitido codificar toda la conversación a través de conceptos. Una vez fijados los núcleos centrales a través de las categorías globales (conceptos-eventos), elaboré el plan específico de análisis y seguidamente inicié el proceso deductivo. Dicho proceso consistió, por un lado, en segmentar la información sujeta a las categorías de interés para el estudio, y por otro, en realizar la codificación de cada división realizada.

- **Observación participante**

La observación participante es un método de investigación que se utiliza habitualmente en los campos de la antropología, la sociología y la psicología, y que Octavio Cruz (2007, p. 47) define así: «La técnica de la observación participante se realiza a través del contacto del investigador con el fenómeno observado para obtener informaciones sobre la realidad de los actores sociales en sus propios contextos». El objetivo principal de esta técnica es obtener una comprensión profunda de la cultura, las normas y las prácticas del grupo que se está estudiando. Al participar activamente en las actividades de dicho grupo, quien investiga puede obtener información privilegiada que no sería accesible a través de otros métodos de investigación.

Una de las prácticas clave de la observación participante es establecer una relación y generar confianza con los individuos a (y con) quienes se está estudiando, lo cual resulta esencial para obtener acceso al grupo y garantizar que las observaciones sean más precisas. En este sentido, mi presencia en el *Canòdrom, Ateneo de Innovación Digital y Democrática* me brindó la posibilidad de observar y documentar

desde un punto de vista privilegiado cómo llevan a cabo sus actividades algunos integrantes del grupo que conforma *Metadecidim*. Así, gracias al contacto que mantuve con ellos durante mi estancia de investigación (y que sigo manteniendo tras ella) he podido recibir su invitación para asistir —sin ser miembro— a las asambleas que *Metadecidim* ha organizado durante las ediciones de 2023 y 2024 del mencionado *Decidim Fest*.

En esta misma línea, he participado en otras actividades como la *Masterclass Ruby on Rails en Decidim* organizada por Pokecode, empresa especializada en la instalación de Decidim, el 16 de febrero de 2023, o como el encuentro (al que me invitó Enric Senabre) del grupo motor para la “mejora de los mecanismos de participación de la comunidad de Goteo.org” a través de Decidim, que tuvo lugar durante los meses de enero a mayo de 2024. Finalmente, de todos estos vínculos surgió la facilidad para organizar en apenas unas semanas las jornadas de presentación y taller de Decidim en Málaga citadas en el punto 1.4.1.

Con todo, como fruto de esta técnica no cabe encontrar un trabajo etnográfico al uso sobre las personas que componen el proyecto, sino que ésta, como comentaba al principio, me ha servido para adquirir una comprensión más profunda de las motivaciones que se encuentran detrás de algunas decisiones que han llevado a que la plataforma opere de una u otra manera. Dado que muchas de estas respuestas emanan de conversaciones informales los lectores no encontrarán en esta investigación un registro de ello, si bien recalco que la información así obtenida ha sido sistemáticamente cotejada y citada con fuentes oficiales, entrevistas y charlas grabadas.

1.4.4. Investigación-Acción Participativa. IAP

Como he comentado anteriormente, a renglón seguido del trabajo de observación participante en torno a Decidim, emergió la posibilidad de extrapolar mi conocimiento adquirido para el desarrollo de las acciones previstas en el proyecto de Investigación *Narrativas emergentes para la construcción de escuelas inclusivas* (PID2022-140193OB-I00) del que formo parte.

Estimo que, dado mi nivel de implicación con la concepción, instalación y despliegue de esta instancia de Decidim con respecto a las anteriormente nombradas, de la técnica de observación participante he transitado aquí hacia una investigación-acción participativa (en adelante IAP), en línea con lo que enuncian Fals y Brandão (1987, p. 18): «Una de las características propias de este método, que lo diferencia de todos los demás, es la forma colectiva en que se produce el conocimiento, y la colectivización de ese conocimiento».

La IAP es, por tanto, un enfoque de investigación que implica la participación de lo que se entendía como el “sujeto de estudio” en el proceso de investigación. No en vano, su objetivo principal es empoderar a estas personas involucrándolas en todos los aspectos del proceso de investigación, desde la identificación de preguntas hasta el diseño e implementación de intervenciones. Al implicar activamente a miembros de la comunidad o partes interesadas en el proceso de investigación, la IAP aspira a crear conocimiento que sea relevante y útil para abordar problemas o desafíos que enfrenta la comunidad. Sus antecedentes se encuentran en la idea de “investigación-acción” formulada por Kurt Lewin en 1944 —y retomada en su artículo *Action research and minority problems* (Lewin, 1946)— y que se define como un proceso participativo y democrático de recolección de datos, análisis, conceptualización, organización, implementación y evaluación, todo ello realizado en colaboración con la población local.

Como veremos a lo largo del Capítulo 6 de esta tesis, titulado *Decidimos Educación Inclusiva*, las citadas tareas de instalación, configuración y sus posteriores aprendizajes de la plataforma, lejos de haber sido individualizadas y propias de una persona investigadora alejada de su sujeto de estudio, bien al contrario, el desarrollo de dichas tareas ha implicado en mayor o menor medida a diferentes agentes, en una suerte de meta-investigación de la propia plataforma similar a las características que marcan la trayectoria de Metadecidim y, más allá, a las palabras de Fals (1991, p. 34) al respecto: «Los investigadores entran así en un proceso en que la objetivación de sí mismos, en una suerte de inagotable sociología del conocimiento, se convierte en testigo de la calidad emancipatoria de su actuación».

Sin embargo, debo añadir que el proceso cíclico de reflexión y acción que ha marcado la implementación de esta IAP no aparecerá aquí redactado como finalizado, puesto que la investigación en la que se enmarca tiene una vigencia mayor que la escritura mi tesis. Por tanto, lo que espero aportar en estas páginas es un conjunto de reflexiones aún incipientes sobre un proyecto que pusimos en marcha a mediados de junio de 2024 pero que merecía tener un capítulo propio en esta tesis (como cierre provisional de la investigación en ella desplegada), pero cuyas conclusiones finales deberán esperar a ser leídas en futuras producciones.

1.5. Estructura de la investigación

El presente estudio se divide en seis capítulos a lo que se deben añadir los apartados de introducción y conclusiones. El primer capítulo —que este mismo punto concluye— corresponde al posicionamiento y diseño de la investigación, y en él he incluido lo siguiente: una delimitación del foco de estudio, en la que se abordan estudios recientes vinculados al extractivismo (material y de datos) así como a su contraparte vinculada a diversas tácticas de resistencia, para culminar explicando qué es la ofuscación, concepto por el que comencé a abordar este trabajo. Tras esta acotación procedo a desarrollar las preguntas de partida y objetivos propuestos, el posicionamiento en el que baso mi investigación, su diseño metodológico y el análisis de los datos obtenidos a partir del mencionado posicionamiento.

El segundo capítulo corresponde al marco teórico de la investigación, el cual comienza situando histórica y teóricamente los conceptos de vigilancia y privacidad para después avanzar hacia las relaciones entre las personas y la tecnologías mediadas por la vigilancia digital dentro de las sociedades de control, hasta el desarrollo teórico del denominado extractivismo de datos personales. Tras estas indagaciones incluyo un apartado denominado 2.4. *Desimplantar Matrix de la matrix* a modo de digresión para ilustrar de manera encarnada cómo a través de la intersección entre acecho legal y tecnológico a los cuerpos gestantes, podemos abordar el conflicto al que nos enfrentamos día a día en relación a la salvaguarda tanto de nuestros datos personales como de nuestras interacciones. Dicha digresión sirve además de enlace hacia el estudio teórico de cómo respondemos al extractivismo de datos personales que culmina este capítulo y da pie a los siguientes de carácter más exploratorio sobre casos prácticos.

De esta manera, los capítulos tres, cuatro y cinco, corresponden a los estudios de caso anteriormente explicados, a saber: el capítulo 3 se dedica a la respuesta legal y al estudio de NOYB y el marco de la regulación de la protección de datos personales en la UE; por su parte, en el capítulo 4 abordo la respuesta tecnológica y de las tácticas de ofuscación que buscan generar ruido para vencer al extractivismo de datos; y en tercer lugar, el capítulo 5 lo dedico al estudio de Decidim como herramienta para trascender las prácticas extractivistas a través de una herramienta basada en *software* libre para las prácticas democráticas participativas.

Ligada a esta última propuesta emerge el capítulo seis, titulado *Decidimos Educación Inclusiva*, como acción propositiva de cómo es posible integrar la herramienta anteriormente citada en un proyecto de investigación al que vertebra la Investigación-Acción Participativa.

2. Marco teórico: Extractivismo de datos personales

2.1. Situando la vigilancia

En primer lugar, a nivel etimológico, en el caso del término vigilancia en castellano, su vocablo original latino *vigilare* genera dos términos diferentes: vigilar y velar, aunque ambos hacen referencia a hacer guardia en la noche, el primero guarda relación con la defensa de un territorio y el segundo con actividades relacionadas con algún ritual. En cambio, el término en inglés *surveillance* proviene a su vez del francés *surveiller*, conceptos que implican la “mirada sobre algo o alguien” o la “super-visión”.

Al margen de la etimología del término, la coyuntura actual no podría entenderse sin hacer referencia al contexto histórico en torno a la vigilancia. Desde que, por un lado, los gobiernos modernos comenzaron a registrar nacimientos, matrimonios y defunciones y, por otro, desde que las empresas modernas comenzaron a monitorear el trabajo y a mantener registros precisos de los salarios y el progreso de los empleados, la vigilancia se ha ido ampliando. Dicha vigilancia denota lo que sucede cuando diferentes organizaciones burocráticas intentan realizar un seguimiento de la información de diversas poblaciones y grupos de una manera cada vez más compleja. Sin embargo, es más que simplemente “burocracia”, la vigilancia está fuertemente ligada a nuestro cumplimiento del orden social y puede llegar a ser un medio de control de la población.

Al mismo tiempo, estos sistemas de vigilancia están destinados a garantizar también el pago de diferentes prestaciones sociales, así como a ayudar a que actividades como el terrorismo y el tráfico de drogas estén contenidas. Funciona tanto para que se nos informe sobre los últimos artículos de consumo disponibles como para que se nos pueda advertir de los riesgos para nuestra salud de un producto u otro. También sirve para que podamos votar en las elecciones, o para que podamos pagar bienes y servicios con tarjetas bancarias, entre otras actividades. La mayoría podríamos considerar que estos logros contribuyen positivamente a nuestra calidad de vida. Así pues, la vigilancia no es inequívocamente buena o mala; y de ahí los dilemas que rodean el uso de bases de datos informáticas para almacenar y procesar nuestros datos personales.

Lo que sí es cierto es que la vigilancia se ha ido expandiendo de manera sutil, a menudo como resultado de decisiones y procesos destinados a alcanzar objetivos relacionados con la eficiencia o la productividad. Además, dicha sutileza se ha visto aumentada por su carácter digital, lo que provoca que la mayor parte de la vigilancia actual se produzca fuera de nuestra percepción. Y esto sucede, como ya hemos visto, no de manera clandestina y conspirativa, sino en las transacciones más comunes como comprar, votar, llamar por teléfono, conducir y trabajar. Esto significa que las personas rara vez sabemos que somos sujetos de vigilancia o, si lo sabemos, no somos conscientes de cuán completo es

en realidad el conocimiento que otros tienen sobre nosotros. Aunque la vigilancia moderna se originase en instituciones específicas como el ejército, las corporaciones y las instituciones gubernamentales, actualmente se encuentra presente en otras muchas áreas de nuestra vida. Sin embargo, esto no debe hacer subestimar la importancia de la violencia circunscrita a este control, pues como explica Graeber (2015, p. 84):

Las burocracias [...] no son tanto por sí mismas formas de estupidez como formas de organizar la estupidez: de gestionar relaciones que ya están caracterizadas por estructuras de imaginación extraordinariamente desiguales, que existen por la existencia misma de las formas de violencia estructural.

2.1.1. Breve historia del origen de la vigilancia

Los primeros censos

Debemos tener claro que la vigilancia no se originó con el surgimiento de las sociedades modernas, sino que, como explica David Lyon (1994, pp. 22-27), desde tiempos inmemoriales las personas nos hemos vigilado para comprobar lo que estábamos haciendo, seguir los diferentes progresos de los demás, organizarnos o cuidarnos. En paralelo, ya los gobernantes de civilizaciones antiguas, como en Sumeria, Egipto o la China imperial, mantenían registros de población para la recaudación de impuestos, reclutamiento militar e inmigración. Así, por ejemplo, en *El Libro de los Números* del siglo XV a.C. vemos un registro de cómo el pueblo nómada israelí llevó a cabo más de un censo con el objetivo de registrar detalles de su población (Lyon, 1994, p. 22).

Estos censos israelitas resultaron una forma de reagruparse después de la huida de la esclavitud en Egipto y de cara a asegurar cierta apariencia de orden militar entre individuos que poco antes habían sido una clase baja y una minoría étnica explotada. Más tarde, el censo, aunque todavía mantenía connotaciones militares, también sirvió como una forma de repartir la tierra a medida que estos nómadas se fueron asentando. La división de un pueblo en tribus y clanes, y el registro de nombres y edades de cada uno de ellos, permitía la supervisión y el orden. Una vez completada la numeración, los líderes podían calcular cuántos de ellos eran adecuados para luchar y qué tierras se necesitarían y dónde.

Conviene destacar aquí que, tal y como apunta Max Weber (1946, p. 245), las estructuras burocráticas tienen la peculiaridad de resultar permanentes, lo vemos a través del ejemplo de estas primeras formas de registro de la población, donde en los citados lugares de Mesopotamia y Egipto, continuaron

existiendo durante miles de años según se sucedían las diferentes dinastías o élites gubernamentales. Tal es también el caso del funcionariado chino, que permaneció constante pese a los diferentes cambios de poder que se sucedían en el territorio (Graeber, 2015, p. 151). Este hecho se justifica bajo la idea de que los invasores precisaban incluso más la información registrada por los burócratas que los propios gobernantes locales:

La única manera real de librarse de una burocracia establecida, según Weber, es matarlos a todos, como hicieron Alarico el godo en la Roma imperial o Gengis Kan en ciertas partes de Oriente Medio. Deja a un número significativo de funcionarios vivos y en pocos años acabarán gestionado tu reino (Graeber, 2015, p. 151).

El libro de Domesday

Avanzando un poco más en la historia Lyon (1994, p. 22) nos remite hacia otro ejemplo en el libro de *Domesday*, un registro de la propiedad de las tierras inglesa iniciado en 1086 que contenía una enorme colección de datos sobre personas y propiedades. Este documento permitió a la administración normanda, una vez establecida militarmente, consolidar su poder. Guillermo I inauguró entonces un plan masivo de transferencias de tierras, redistribuyendo la propiedad e imponiendo nuevos sistemas impositivos. El efecto, como señala Vivian Galbraith (1974, p. 172), fue «aprovechar la riqueza de Inglaterra para un nuevo sistema de baronías feudales». Se trataba de un «registro escrito del nuevo orden, visto a través de los ojos normandos» (Galbraith, 1974, p. 172).

El recuento contenido en el *Domesday* intentaba llevar a cabo un exhaustivo estudio de todos los arrendamientos y herencias, en contraste con lo que se había hecho anteriormente. Era inevitable pues que surgieran disputas, especialmente con las transferencias de tierras, y la administración normanda tuvo que contrarrestarlas. Para ello, resultaba esencial saber y establecer por escrito quién era el responsable de qué. El *Domesday*, por tanto, buscaba el conocimiento completo, como medio para lograr el control total.

Conviene destacar que esta encuesta no fue para nada popular entre quienes debían dar cuenta de ella. La *Anglo-Saxon Chronicle*, una colección de anales en inglés antiguo que narra la historia de los anglosajones, registró el malestar con el que el estudio fue recibido «realizado tan al detalle que no quedó ni un solo escondite o patio, ni – vergüenza que no fuese contada [...] no hubo un buey, vaca o cerdo que no quedase registrado en sus escritos» (Finn, 1963, p. 7).

Aunque no está claro por qué recibió el nombre de *Domesday*, un tesorero inglés, en un escrito de 1179,

explicaba que se refería metafóricamente al *Día del Juicio*, cuando, según el *Apocalipsis*, los muertos serán juzgados por lo que está escrito en el libro (Finn, 1963, p. 3). Tal interpretación resulta de lo más probable y apropiada para este caso.

Las revoluciones campesinas en la Baja Edad Media europea

Entre los siglos XII y XIV, lejos de la idea que se nos ha impuesto sobre la sociedad feudal como un momento histórico estático y de completa aceptación del orden social, encontramos una serie de revueltas del campesinado contra el poder terrateniente, desarrolladas de manera constante y colectiva (Federici, 2004/2010, pp. 41-46). De hecho, según Hilton (1985, citado en Federici, 2004/2010, p. 43), existen pruebas de una “deserción masiva” de los servicios laborales por parte de los siervos que se negaban a trabajar la tierra de sus señores cuando éstos eran convocados. Y cuando sí se presentaban, bien lo hacían demasiado tarde, provocando que muchos de los cultivos se arruinasen, o bien trabajaban de manera descuidada e irregular, provocando que los señores tuvieran que ejercer una constante y firme vigilancia sobre ellos (Bennett, 1967, citado en Federici, 2004/2010, p. 42) sin embargo, aquí todavía hablamos de una vigilancia directa empleada a través de la mirada de un superior sobre el resto.

Otra de las resistencias de las que tenemos registro por parte del campesinado fue la relacionada con la obligación de acudir a filas en tiempos de guerra (Federici, 2004/2010, p. 44). Así, por ejemplo, en algunas aldeas inglesas les fue necesario recurrir a la fuerza para llevar a cabo el reclutamiento de los soldados. Además, existía un gran porcentaje de deserciones que se sucedían en cuanto tenían oportunidad. Todas estas revueltas resultaron según Federici (2004/2010, p. 46) en la concesión de:

“privilegios” y “fueros” que fijaban las cargas y aseguraban “un elemento de autonomía en la administración de la comunidad aldeana”[...] Sin embargo, la resolución más importante del conflicto entre amos y siervos fue la *sustitución* de los servicios laborales por pagos en dinero (arrendamientos en dinero, impuestos en dinero) que ubicaba la relación feudal sobre una base más contractual.

De esta manera, se comenzó a poner fin a la servidumbre como forma de relación, pero este aparente avance también supuso la desintegración de la aldea feudal, al solo lograr parcialmente los objetivos que el campesinado se había propuesto. Ello provocó a su vez una nueva división social, dado que:

La sustitución también hizo posible que los arrendatarios libres emplearan y explotaran a otros trabajadores, de tal manera que, «en un desarrollo posterior», promovió «el

crecimiento independiente de la propiedad campesina», transformando a «los antiguos poseedores campesinos» en arrendatarios capitalistas (Marx, 1867/1975, citado en Federici, 2004/2010, p. 48).

En el caso de las mujeres, si bien antes tampoco gozaban de una gran equidad en materia de derechos, independientemente de su clase social, con este cambio sufrieron un retroceso en este aspecto al quedar aún más restringidos sus derechos de acceso a la propiedad y a los ingresos (Federici, 2004/2010, pp. 48-49).

A lo largo del siglo XIV sucedió otro acontecimiento que tuvo notables consecuencias sobre los sistemas de organización del campesinado europeo: la peste negra. Esta pandemia histórica acabó con la vida de entre un 30% y un 40% de la población europea y constituyó uno de los momentos clave de los conflictos de esta época (Ziegler, 1969, p. 230), dado que la alta y transversal tasa de mortalidad provocó el cambio en las formas de vida social y política europeas. De esta manera, la disciplina social quedó debilitada, y es que tras haber experimentado la muerte tan de cerca, la población dejó de preocuparse por el trabajo y las regulaciones tanto sociales como sexuales y abrazó un estilo de vida más centrado en el goce y el festejo.

Sin embargo, una de las consecuencias más relevantes de la peste fue la crisis del trabajo. Al haber quedado tan reducida la mano de obra, se revalorizó el coste de los trabajadores exponencialmente y ello brindó a campesinos y artesanos la oportunidad de acabar con el dominio feudal imperante. Signo de ello fue la proliferación de huelgas de inquilinos, fortalecidas por la facilidad de cambiar de tierras o de ciudad que esta proliferación de terrenos abandonados por la falta de trabajadores ofrecía (Dyer, 1968, citado en Federici, 2004/2010, p. 74).

Si bien es cierto que, como respuesta al aumento del coste de la mano de obra, en diversos lugares se intentó aumentar la explotación del trabajo mediante la restauración de los servicios laborales anteriormente citados, y en algunos casos incluso de la esclavitud, estas medidas solo aumentaron el conflicto entre clases (Federici, 2004/2010, p. 75). Por tanto, podemos pensar que el periodo posterior a la peste resultó una época de poder para ciertos campesinos de Europa occidental, ya que la falta de mano de obra les otorgó un poder de decisión que antes no poseían, pero además, ver a sus posibles empleadores por primera vez competir por sus servicios, aumentó su autoestima y corrigió siglos de degradación y sumisión (Federici, 2004/2010, p. 78).

Sin embargo, a finales del siglo XV las autoridades políticas contrarrestaron estos movimientos a través de una perversa política sexual que incluyó la legalización de la violación y la institucionalización de la

prostitución a través del establecimiento de burdeles municipales. Estas medidas provocaron la disolución de la protesta de los trabajadores y el cambio del antagonismo de clase a la animadversión hacia la mujer proletaria. Como resultado, tal y como relata Federici (2004/2010, p. 78) la solidaridad de clase de la lucha antifeudal quedó debilitada y la permisividad ante tales prácticas estableció una mentalidad misógina que relegó de nuevo a las mujeres de cualquier clase social, y les insensibilizó frente a la violencia contra ellas, sentando así las bases para las cazas de brujas que tuvieron lugar en el mismo periodo:

Resulta difícil discernir, de forma retrospectiva, hasta qué punto esta “carta sexual” ayudó al Estado a disciplinar y dividir al proletariado medieval. Lo que es cierto es que este *new deal* fue parte de un proceso más amplio que, en respuesta a la intensificación del conflicto social, condujo a la centralización del Estado como el único agente capaz de afrontar la generalización de la lucha y la preservación de las relaciones de clase (Federici, 2004/2010, p. 82).

A través de este proceso el Estado se impuso como el encargado de gestionar las relaciones de clase y como supervisor de la reproducción de la fuerza de trabajo, a través de la creación de leyes que imponían límites al coste del trabajo, castigaban la vagancia y fomentaban la reproducción de la fuerza laboral (Federici, 2004/2010, p. 82).

A lo largo del siglo XVI las rebeliones campesinas europeas contra el sistema feudal fueron aplastadas. Dichas derrotas, sumadas a las cazas de brujas desplegadas por el centro y el norte europeos y a las consecuencias que supuso la expansión colonial para la libertad de los trabajadores, fueron algunas de las causas que provocaron el fin del proceso revolucionario en este continente.

Sobre el cambio del sistema feudal al capitalista Federici (2004/2010, pp. 73-178) hace un uso entrecomillado del término “transición” para referirse a esta etapa. Y es que, aunque describirlo así resulta útil para nombrar el periodo entre 1450 y 1650 en que el feudalismo estaba llegando a su fin mientras aún no estaba claro qué otro sistema le sucedería, dicho término denota un proceso gradual que nunca fue tal. He aquí, en contraste, el modo en que Federici (2004/2010, p. 88) se refiere a estos años:

una época que fue testigo de transformaciones apocalípticas, que los historiadores solo pueden describir en los términos más duros: la Era de Hierro (Kamen), la Era del Saqueo (Hoskins) y la Era del látigo (Stone). “Transición”, entonces, no puede evocar los cambios que allanaron el camino para la llegada del capitalismo y las fuerzas que lo conformaron.

Sobre la relación entre la “reacción feudal” y el desarrollo de las relaciones capitalistas, la autora hace un uso crítico del concepto marxiano de «acumulación primitiva» (Marx, 1867/1975). Este término describe la reforma social y económica por parte de la clase dominante europea en relación a su crisis acumulativa y determina que el capitalismo se desarrolló a partir de una concentración previa de capital y trabajo, y que es la separación de los trabajadores de los medios de producción la fuente final de su riqueza.

Sin embargo, Federici critica que Marx relacionara casi en exclusividad este proceso con el del varón proletario industrial europeo, sin hacer apenas mención a la expropiación de los medios de subsistencia y la esclavización de los pueblos originarios de otros lugares como América, África y Asia. Igualmente señala que el filósofo alemán tampoco tuvo en cuenta la desfiguración del cuerpo en máquina de trabajo a través, y sobre todo, del sometimiento de las mujeres para la reproducción de la fuerza laboral. Dicho proceso realmente se produjo a través de la destrucción del poder de las mujeres mediante el exterminio de las “brujas” (Federici, 2004/2010, p. 87-90). En suma, para Federici (2004/2010, p. 90), este proceso originario supuso, por tanto, no solo una dinámica de acaparamiento de riqueza y fuerza de trabajo, sino:

también una acumulación de diferencias y divisiones dentro de la clase trabajadora, en la cual las jerarquías construidas a partir del género, así como las de «raza» y edad, se hicieron constitutivas de la dominación de clase y de la formación del proletariado moderno.

Algunas conclusiones sobre los orígenes de la vigilancia

¿Qué vemos a través de estos ejemplos históricos? En primer lugar, destacaría cómo se mantiene el poder a través de tales actividades de vigilancia, y cómo aquellos llamados a rendir cuentas, como en el caso registrado tanto de la Inglaterra normanda, como del campesinado de la Edad Media, experimentaron negativamente el escrutinio de sus vidas por parte de las instancias de poder. En el caso de los campesinos, también desarrollaron toda una serie de resistencias activas y pasivas contra el pago de impuestos, trabajo y reclutamiento militar. Vale la pena aquí mencionar que todas estas indagaciones dependían en gran medida del desarrollo de la escritura. Se podría decir, por tanto, que el cambio de técnica facilitó alteraciones en la capacidad de vigilancia de los gobernantes y también por qué Graeber (2012/2021, p. 16) afirma que:

Por la misma razón, durante los últimos cinco mil años, y con una regularidad notable, las insurrecciones populares han comenzado de la misma manera: con la destrucción ritual de

los registros de deudas (tablillas, papiros, libros, cualquier forma que tomaran en las diferentes épocas y lugares). Tras ello, los rebeldes solían ir a por los registros de posesión de tierras y los cálculos tributarios.

Tal y como apuntan Harold Innis (1951) o James Carey (1989), todas las formas de tecnología de la comunicación tienen un «sesgo» (Carey, 1989, p. 98). En los estados antiguos, los ciudadanos estaban unidos mediante el uso de la escritura, ya sea en piedra, pergamino o arcilla. Los detalles registrados de transacciones y reglas pasadas se consideraban más seguros que la memoria humana. En efecto, sólo cuando el papiro estuvo ampliamente disponible para los romanos, a través de su conquista de Egipto, pudieron mantener unidos administrativamente los vastos espacios que se conocerían como el Imperio Romano. Pero al caer el papiro en desuso tras la decadencia de Roma, tuvimos que esperar hasta el desarrollo de la imprenta para poder ver otro cambio relevante en el poder administrativo. Tras este invento, la esfera política pudo expandirse ampliamente, dada la novedosa disponibilidad de textos escritos. Por supuesto, esto es muy pertinente para el desarrollo de la vigilancia como dimensión en la modernidad, dado que la imprenta facilitó el desarrollo de la gobernanza moderna.

Por otro lado, observamos ya el empleo por parte de Estados con formas organizativas más centralizadas de los cuerpos de las mujeres como forma de adoctrinamiento y control social, convirtiendo a estos en los únicos agentes capaces de gestionar las relaciones y luchas de clase. Como relata Federici (2004/2010, pp. 138-139):

El resultado de estas políticas que duraron dos siglos [...] fue la esclavización de las mujeres a la procreación. Si en la Edad Media las mujeres habían podido usar distintos métodos anticonceptivos y habían ejercido un control indiscutible sobre el proceso del parto, a partir de ahora sus úteros se transformaron en territorio político, controlados por los hombres y el Estado: la procreación fue directamente puesta al servicio de la acumulación capitalista.

Sin embargo, la vigilancia entendida como algo centralizado y omnipresente no surgió hasta los tiempos modernos. Si bien sus formas originarias pueden verse, por ejemplo, en el siglo XI con el libro de *Domesday*, su expansión a partir del siglo XIX fue dramática. La vigilancia sistemática y a amplia escala llegó con el crecimiento de la organización militar, la industrialización de las ciudades, la administración gubernamental y las empresas capitalistas dentro de los Estados-nación europeos.

Si la vigilancia no es un fenómeno nuevo, ¿qué ha cambiado entonces? En los ejemplos vistos se dan ciertas características. La vigilancia se conecta con el poder de ayudar a organizar y controlar poblaciones; pero además, las técnicas mejoradas de registro (escritura o impresión) facilitaron nuevos niveles de vigilancia. Al examinar los sistemas de vigilancia actuales, vale la pena tener en cuenta estas cuestiones: ¿qué tipo de poder está involucrado? ¿Cómo se experimenta la vigilancia (si es que se hace) y con qué efectos? Y ¿de qué manera las mejores técnicas contribuyen a una mayor capacidad de vigilancia?

2.1.2. Vigilancia en la época moderna

Como comentaba en líneas anteriores, la vigilancia ha resultado ser una característica central de la modernidad. Las prácticas rudimentarias de las sociedades tradicionales y feudales se fueron intensificando y se hicieron más sistemáticas en la era moderna. Resulta, sin embargo, complicado aislar un punto de partida simbólico para la vigilancia moderna. Algunos pensadores como Marx (1867/1975) vinculan su auge como parte de la economía política del capitalismo, otros autores como Max Weber (1904/1930, 1946) la asocian como un producto de la organización burocrática y otros, entre los que destaca Michel Foucault (1975/2002), como un paso del castigo como espectáculo (o el espectáculo del castigo) a la autodisciplina. En cada caso se tiene en cuenta un tipo específico de sistema y un concepto específico de vigilancia.

Es importante, por tanto, recordar que las diferentes dimensiones de la modernidad vinculadas al desarrollo de la vigilancia que presento a continuación son en realidad distinciones analíticas un tanto artificiales, pues en realidad cada una está entrelazada con las demás de maneras complejas. Junto a ello, cabe recalcar que en muchos casos se han ignorado por parte de la academia clásica los procesos de reproducción, tratando como indiferenciadas las historias femenina y masculina y, por consiguiente, no prestando la atención que se merece al “disciplinamiento” específico al que se somete a las mujeres (Federici, 2004/2010).

La creación del ejército moderno

En un primer momento, Lyon (1994, p. 27) apunta a que las prácticas modernas de vigilancia son claramente visibles en el surgimiento de los ejércitos modernos de los siglos XVI y XVII. En este periodo, Mauricio I de Nassau-Orange, capitán general de Holanda y Zelanda, en su labor ante el desafío de los españoles en los Países Bajos, desarrolló una sistematizada armada dividida en pequeñas unidades tácticas, en las que se enseñaba a los soldados a cargar y disparar sus armas permitiendo así

constantes ráfagas de fuego. Estos ejercicios, supervisados a su vez por un nuevo grupo de oficiales, hicieron que la acción armada fuera semiautomática (McNeill, 1984, pp. 125-143).

Desde la perspectiva francesa Armand Mattelart (2001/2007, pp. 23-25), introduce conceptos como el de la «revolución militar» (Mattelart, 2001/2007, p. 24) iniciada entre 1670 y 1680 por el marqués de Louvois, secretario de Estado para la Guerra en el reinado de Luis XIV, consistente en la:

aplicación sistemática de la ciencia a la guerra (y creación corolaria de un cuerpo de ingenieros), establecimiento de una administración civil de la guerra en torno a un ministerio *ad hoc*, fin del mercenarismo, profesionalización y organización de la disciplina, estabilización de los efectivos militares en los cuarteles, establecimiento de un «escalafón», ordenación de la carrera en la que los militares ascienden por antigüedad, perfeccionamiento del arma de fuego y del arma blanca (abandono del mosquete y de la pica en beneficio del fusil de chispa armado con bayoneta de cubo) (Guerlac, 1986).

Otro concepto que introduce el autor es el de «sistema de fortificación» (Mattelart, 2001/2007, p. 25) del ingeniero militar francés Sébastien Le Prestre, señor de Vauban:

Por un lado, [...] una monografía estadística que describe la población y sus condiciones de vida, las actividades y los recursos de la ciudad fortificada y del país circundante. Por otro, [...] un plano gráfico o “plano-relieve” [...] sino también su entorno, con especial atención a las vías de comunicación y a los puentes sobre una considerable extensión que en ocasiones puede alcanzar hasta veinte veces la superficie de la ciudad.

Los citados cambios en la táctica bélica tuvieron como resultado la aparición del ejército moderno, en el que se observaba una burocracia embrionaria, una clase separada de funcionarios y oficiales, uniformes y un entrenamiento disciplinado. Todo ello con el objetivo de lograr la mayor eficiencia junto con la necesidad de reducir costes. Sin duda, resulta llamativo cómo todas estas características reaparecerán luego hasta cierto punto en otras organizaciones modernas: la fábrica, la oficina, la prisión o la escuela (Lyon, 1994, p. 28).

Otros estudiosos como Christopher Dandeker (1990) parten también de este desarrollo militar como un destacado punto de partida de la vigilancia moderna. En este sentido, este autor sostiene que las fuerzas armadas representaron el componente más significativo del Estado moderno temprano, al indicar que los militares fueron abriendo el camino, al menos en Europa, al proporcionar un modelo burocrático de organización para que otras organizaciones, como las empresas, lo siguiesen.

Más allá de esto, la guerra también fomenta la extensión de la supervisión estatal de la sociedad para objetivos militares y, a partir del siglo XX, las conexiones entre el Estado de guerra y el Estado de bienestar se tornaron más fuertes y significativas (Marwick, 1988), dado que involucraban a sociedades enteras gradualmente en el proceso bélico. Aunque esto ocurrió de diferentes maneras y a diferentes ritmos dependiendo de cada sociedad, esta movilización masiva encontró su mayor expresión en las guerras mundiales del siglo XX. La lealtad al Estado nación para ese supuesto esfuerzo bélico se aseguró en parte mediante la consiguiente extensión de los derechos de la ciudadanía.

Conviene citar aquí el caso de Gran Bretaña, donde a partir de 1916 se desplegó una vigilancia burocrática a gran escala para reclutar a soldados, tanto mediante el registro de hombres aptos para la guerra, como en los modos de tratar con grupos disidentes, como los objetores de conciencia. Asimismo, la producción y distribución de información fueron reguladas como nunca antes, siempre bajo la premisa de asegurar que en condiciones de guerra total fuera posible lograr la victoria. Los servicios de seguridad intensificaron sus actividades de vigilancia, informando sobre personas sospechosas, interceptando cartas y mensajes por cable y recopilando datos sobre varias categorías de personas potencialmente peligrosas (Lyon, 1994, pp. 28-29).

Durante este período de conflictos bélicos se establecieron nuevas formas de control y registro de la población, tales como la tarjeta de identidad nacional, que permanecieron después del fin de la guerra. También en nombre de la protección de la ciudadanía contra amenazas externas, algunas libertades civiles, tales como el derecho de reunión, movimiento e información quedaron erosionadas. Clara mención merece la *Espionage Act* estadounidense de 1917, con la que se viene persiguiendo a Julian Assange, Chelsea Manning y Edward Snowden, entre otros muchos, más de un siglo después (Snowden, 2019, pp. 394, 396).

Por lo tanto, se pueden encontrar varios aspectos de la vigilancia integradas en la historia de las actividades militares y relacionadas con las guerras modernas. Véanse desde la observación y el cálculo de los movimientos de los soldados para una preparación eficaz para la batalla hasta la organización burocrática de los ejércitos y sus oficiales. Y desde la movilización de poblaciones civiles enteras para una guerra total hasta el crecimiento de los servicios de seguridad como departamentos de Estado. Cada uno implica, bien la supervisión directa de grupos subordinados, bien la recopilación y documentación de datos personales con el propósito de coordinación o control de la población. Además, dicha vigilancia a menudo se intentaba presentar desde una perspectiva positiva, dado que el objetivo general de tales esfuerzos era lograr la seguridad nacional, la supremacía militar o la derrota del enemigo.

Aunque es cierto que el trasfondo militar de la vigilancia moderna es una influencia clave para la misma, debemos observar otras que también están interrelacionadas de maneras complejas. Más si tenemos en cuenta que las sociedades modernas tienen varias dimensiones institucionales importantes, ninguna de las cuales puede reducirse a otra. En este sentido, Anthony Giddens (1985, 1987, 1990) sugiere que la vigilancia es fundamental para todos los tipos de organización asociados con la modernidad: capitalismo, industrialismo, poder militar y cultura. Es visible, por ejemplo, en la supervisión capitalista del lugar de trabajo, la administración gubernamental y el monopolio por parte del Estado nación de los medios para ejercer la violencia.

El disciplinamiento de los cuerpos

Durante los siglos XVII y XVIII fue surgiendo un nuevo concepto de Estado, siempre en el marco europeo, que se diferenciaba de sus formas anteriores en al menos un aspecto crucial: en ellos se fueron buscando cada vez más medios distintos de la violencia directa para contener a la población.

Dicho surgimiento derivaba, entre otros motivos, de la culminación de los cercamientos de tierras agrícolas para su uso a mayor escala durante el cambio del régimen feudal al capitalista, el cual provocó que los nuevos trabajadores sin tierra buscaran empleo en las ciudades, aumentando el constante temor por parte de las instancia de poder al estallido de nuevos disturbios.

Para garantizar dicho orden, los medios utilizados implicaron un uso cada vez mayor de la separación de las poblaciones que se desviaban de las normas deseadas de la “sociedad”. En diversos lugares de Europa, los asilos, los hospitales y las prisiones sirvieron como lugares donde los desobedientes o los desviados podían ser “encarcelados” o “reformados” para convertirlos en ciudadanos productivos. De esta manera, instituciones como las cárceles se convirtieron no sólo en lugares de castigo, sino también en sitios donde defender y realizar los ideales de la época. Así, la visión del orden frente al caos potencial pudo mantenerse e incluso ejemplificarse a través de las prisiones.

Sin embargo, a partir del siglo XIX, estas formas no quedaron enmarcadas solo dentro del territorio penal, ya que los urbanistas comenzaron a tomar nota de la función de control social interno que podían ejercer las ciudades. La vigilancia se llevó entonces a cabo en las calles de la ciudad, lugar de posible criminalidad y disturbios. La ley y el orden se perseguían al mismo tiempo arquitectónicamente y mediante una planificación racional y estratégica. Y es que, las formas embrionarias de vigilancia callejera dentro de la metrópoli comenzaron mucho antes de la era de las cámaras de vídeo colocadas en las fachadas de los edificios.

De esta manera, toda esta extensión progresiva de los dispositivos de la disciplina se fue expandiendo a través de todo el cuerpo social, dando forma a la «sociedad disciplinaria» (Foucault, 1975/2002). Si bien, como hemos visto anteriormente, el disciplinamiento de los cuerpos de las mujeres llevaba ya siglos experimentándose, en esta sociedad sobre la que teoriza el autor, los muros, cerrojos y celdas conformaron toda una serie de «ortopedia social» (p. 135) cuyo fin último era el de sojuzgar el cuerpo, tanto masculino como femenino, para corregir el alma. Estos mecanismos de coerción se materializaron a través de una arquitectura espacial: el Panóptico.

Pero antes de adentrarnos en este concepto, debemos entender que este modo de vigilancia bebe de otro momento histórico de nuevo vinculado a otra enfermedad de carácter pandémica. A este respecto, Foucault (1975/2002, pp. 199-232), alude a los episodios de epidemias y en concreto el de la peste de finales del siglo XVIII en paralelo al surgimiento de gobiernos más disciplinarios.

En este sentido, el filósofo francés recoge algunas de las medidas que se adoptaban cuando se declaraba la peste en una ciudad: la estricta división espacial y cierre de la urbe, la prohibición de salir de las zonas acotadas y el establecimiento del poder de un intendente. Bajo estas circunstancias la inspección funcionaba sin cesar mediante un registro permanente, con guardias en cada esquina y el recuento de los habitantes de cada hogar, así como de su estado de salud. Todo ello se anotaba en informes que se trasladaban a través de una jerarquía de puestos de control (síndico, intendente, regidores y alcaldes). De esta manera, la relación de cada uno con su enfermedad y posible muerte pasaban siempre por el arbitrio del poder:

Este espacio cerrado, recortado, vigilado, en todos sus puntos, en el que los individuos están insertos en un lugar fijo, en el que los menores movimientos se hallan controlados, en el que todos los acontecimientos están registrados, en el que un trabajo ininterrumpido de escritura une el centro y la periferia, en el que el poder se ejerce por entero, de acuerdo con una figura jerárquica continua, en el que cada individuo está constantemente localizado, examinado y distribuido entre los vivos, los enfermos y los muertos —todo esto constituye un modelo compacto del dispositivo disciplinario (Foucault, 1975/2002, p. 201).

Si la Peste Negra acontecida durante el siglo XIV alentó aún más la revolución del campesinado por el aumento de su poder de decisión frente a las fuerzas de trabajo, esta nueva epidemia representa para Foucault la estandarización de la disciplina de los cuerpos a través del control del espacio que ocupan y donde se mezclan y entrecruzan con otros cuerpos. Para ello, se efectuaba la instauración de una jerarquía que garantizaba el funcionamiento del poder, gracias a un control y registro estricto de a quién

pertenecía ese cuerpo sano, enfermo o muerto, el control de esta nueva peste apelaba así a la distribución individualizante.

Sin embargo, este modelo se entrecruzaba con ese otro modelo excluyente del que hablábamos al principio, de tal modo que desde comienzos del siglo XIX todas las instancias de control individual comenzaron a funcionar de manera dual: de un lado se impuso a los excluidos una disciplina individualizante y de otro la universalidad de los controles disciplinarios posibilitó señalar al diferente para su posterior exclusión.

La figura arquitectónica que representa esta composición es para Foucault el Panóptico, idea del filósofo utilitarista Jeremy Bentham, que consistía en una construcción de forma de anillo con una torre con anchas ventanas en el centro de la edificación desde la que se podía controlar de manera total la circunferencia del edificio que se disponía a su alrededor. Dicho edificio quedaba dividido a su vez en alvéolos en los que las personas vigiladas se encontraban alojadas en celdas individuales y separadas las unas de las otras. Cada celda constaba de dos ventanas, una daba al exterior del edificio y la otra al interior, por lo que la luz atravesaba el habitáculo, y gracias a ese efecto de contraluz que se generaba se podían discernir las siluetas que en ellas habitaban sin darles a éstas la posibilidad de saber si estaban siendo o no fruto de escrutinio. Toda esta disposición permitía por un lado dejar al encarcelado individualizado y permanentemente visible y por otro dar al guardián el privilegio de ver sin ser visto:

La Antigüedad había sido una civilización del espectáculo. “Hacer accesible a una multitud de hombres la inspección de un pequeño número de objetos”: a este problema respondía la arquitectura de los templos, de los teatros y de los circos. [...] La edad moderna plantea el problema inverso: “Procurar a un pequeño número, o incluso a uno solo la visión instantánea de una gran multitud”. En una sociedad donde los elementos principales no son ya la comunidad y la vida pública, sino los individuos privados de una parte, y el Estado de la otra, las relaciones no pueden regularse sino en una forma exactamente inversa del espectáculo: Nuestra sociedad no es la del espectáculo, sino de la vigilancia; bajo la superficie de las imágenes, se llega a los cuerpos en profundidad; detrás de la gran abstracción del cambio, se persigue el adiestramiento minucioso y concreto de las fuerzas útiles; los circuitos de la comunicación son los soportes de una acumulación y de una centralización del saber; el juego de los signos define los anclajes del poder; la hermosa totalidad del individuo no está amputada, reprimida, alterada por nuestro orden social, sino que el individuo se halla en él cuidadosamente fabricado, de acuerdo con toda una táctica de las fuerzas y de los cuerpos. Somos mucho menos griegos de lo que creemos. No

estamos ni sobre las gradas ni sobre la escena, sino en la máquina panóptica, dominados por sus efectos de poder que prolongamos nosotros mismos, ya que somos uno de sus engranajes (Foucault, 1975/2002, pp. 219-220).

Esta arquitectura garantizaba pues la asimetría, el desequilibrio y la diferencia de poder. De hecho, poco importaba quién ejercía el poder, cualquier individuo podía hacer funcionar la máquina de vigilancia. Esto era así porque es realmente el que está sometido al campo de visibilidad quien, bajo el temor de estar bajo constante escrutinio, reproduce sobre sí mismo las relaciones de poder y sometimiento. El Panóptico permite también establecer diferencias, evitar contagios y registrar las capacidades de los observados para desempeñar diferentes tareas, así como experimentar con ellos. Sin embargo, esta idea, lejos de quedar acotada a recintos cerrados o a ciudades en estado de peste, para Bentham era la oportunidad de establecer un sistema global de vigilancia, sintetizado por Foucault (1975/2002, p. 212) de esta manera: «El panoptismo es el principio general de una nueva “anatomía política” cuyo objeto y fin no son la relación de soberanía sino las relaciones de disciplina».

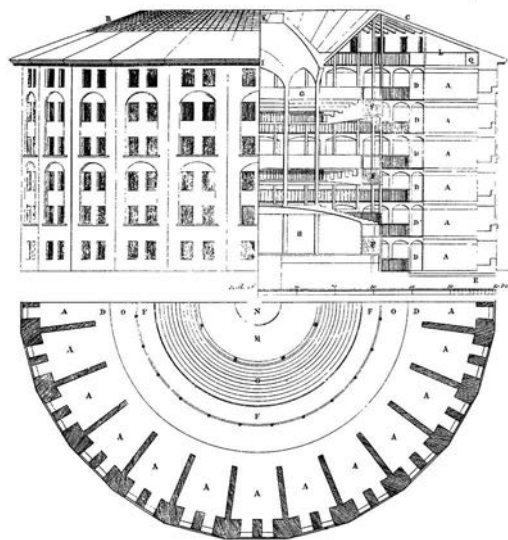


Figura 6. Diseño del panópticón de Bentham. Fuente: Bentham, (1843, pp. 172-173)

Las disciplinas son vistas, por tanto, como técnicas que garantizan la ordenación de multiplicidades humanas a través de una táctica de poder que busca tres objetivos distintos: en primer lugar, hacer este ejercicio lo menos costoso posible, tanto en términos económicos como en términos políticos, esto es, que resulten lo más discretos, invisibles y susciten la menor resistencia posible. En segundo lugar, busca que el poder se extienda lo máximo posible y adquiera la mayor intensidad que pueda. Y en tercer lugar, vincula el ejercicio del poder al rendimiento de los aparatos en los que se ejerce (pedagógicos, militares,

industriales, médicos, etc.). En definitiva, busca aumentar la productividad y docilidad de todo el sistema.

Esta serie de finalidades de la disciplina corresponden a una coyuntura histórica concreta: por un lado, nos encontramos en el siglo XVIII ante un gran crecimiento de la población en Europa, junto con un aumento del nomadismo y el consiguiente aumento del número de personas pertenecientes a los grupos susceptibles de este control. Y por otro, asistimos de igual manera al crecimiento, extensión y complejidad del aparato de producción y la búsqueda de la mayor rentabilidad del mismo:

El desarrollo de las disciplinas marca la aparición de técnicas elementales del poder que corresponden a una economía completamente distinta: unos mecanismos de poder que, en lugar de venir “en descuento”, se integran desde el interior a la eficacia productiva de los aparatos, al crecimiento de esta eficacia, y a la utilización de lo que produce. Las disciplinas sustituyen el viejo principio “exacción-violencia” que regía la economía del poder, por el principio “suavidad-producción-provecho”. Se utilizan como técnicas que permiten ajustar, según este principio, la multiplicidad de los hombres y la multiplicación de los aparatos de producción (Foucault, 1975/2002, p. 216).

Toda la transformación histórica de la disciplina a lo largo de los siglos XVII y XVIII encuentra su paradigma en la física benthamiana, donde lo que era una medida circunstancial pasa a generalizarse; lo vemos en las reglamentaciones de los citados ejércitos holandeses, cuyas normas se extienden a todos los ejércitos de Europa, así como en los diferentes centros escolares o en la ordenación de los hospitales. Las disciplinas, pues, funcionan como técnicas para confeccionar individuos útiles para el sistema. Es por ello que Foucault (1975/2022, pp. 218-219) la identifica como un tipo de poder y una forma de ejercerlo, y es así como explica que se extendiese por instituciones como el ejército, las casas de educación, los hospitales, los Estados e incluso las propias relaciones intra-familiares. Esta modalidad disciplinaria queda además ligada a otras formas como la exclusión, extendiendo sus efectos hasta los elementos más ínfimos de la vida cotidiana.

El nacimiento del Estado nación: la burocracia

Podemos estar de acuerdo en que un elemento esencial de la vigilancia es la generación y cotejo de documentación e información sobre otras personas. Si bien esto se da ampliamente en entornos militares, especialmente en el campo de la seguridad estatal, la actividad de mantener archivos sobre individuos es también una característica clave de la administración civil y, más allá, de todas las organizaciones burocráticas. En este sentido, y tal y como sostiene Weber (1946), el expediente escrito

resulta ser la base documental de toda gestión moderna dentro de una organización, dado que los ficheros tienen como objetivo garantizar la eficiencia técnica y la previsibilidad.

Es por ello que, además de la función organizativa de la burocracia, también encontramos que estos archivos cumplen una función de vigilancia, ya que sus actividades pueden ser supervisadas y, por tanto, coordinadas o controladas por una organización en la medida en que conserve un registro de la conducta pasada de quienes pertenecen a la misma. En este sentido, Weber temía que las formas burocráticas de organización se viesan como la cúspide de la razón en cuanto a asuntos humanos se refieren, resultando tan superiores a otras formas de organización que terminasen por «encasillar el espíritu» (citado en Beetham, 1974, p. 81). A medida que el ideal burocrático ganase dominio, quedaría la humanidad encerrada en una “jaula de hierro”⁸ (Weber, 1904/1930). En este sentido Federici (2019/2020, p. 267), confronta las ideas de Weber de la siguiente manera:

Casi ha pasado un siglo desde que Max Weber afirmara en “La ciencia como vocación” que el sino de nuestro tiempo se caracteriza sobre todo por el desencantamiento del mundo, [...] Weber se refería a la desaparición de lo religioso y lo sagrado, pero podemos interpretar su advertencia en un sentido más político, como una referencia al surgimiento de un mundo nuevo en el que nuestra capacidad para reconocer la existencia de otras lógicas distintas a la lógica del desarrollo capitalista se pone cada día más en duda. Este “bloqueo” tiene orígenes diversos y evita que la desdicha en la que vivimos nuestro día a día se convierta en acción transformadora.

En palabras de David Graeber (2015, p. 58), el otro gran teórico del siglo XX que, junto a Max Weber, parecía creer realmente que el poder de la burocracia residía en su eficacia es el mencionado Michel Foucault. En efecto, para el antropólogo estadounidense Foucault adoptaba un enfoque más subversivo que desembocaba en una afirmación de que las burocracias estatales delineaban los límites de la humanidad de una manera mucho más profunda que nada que pudiese haber imaginado Weber. Según Foucault, «toda forma de conocimiento se convertía en una forma de poder, moldeando nuestras mentes y cuerpos a través de medios en gran medida administrativos» (Graeber, 2015, p. 59).

La idea de Foucault radicaba en que el «poder disciplinario» reside en el expediente:

El suplicio da fin lógicamente a un procedimiento impuesto por la Inquisición. El sometimiento a “observación” prolonga naturalmente una justicia invadida por los

8 Sobre este concepto, David Graeber (2015) alude en una nota al final a que «esta expresión parece ser una mala traducción de una frase que significaba más bien algo así como “marco de metal brillante”: no una prisión desnuda, sino un envoltorio de alta tecnología, superficialmente atractivo por derecho propio» (pp. 235-236).

métodos disciplinarios y los procedimientos de examen. ¿Puede extrañar que la prisión celular con sus cronologías ritmadas, su trabajo obligatorio, sus instancias de vigilancia y de notación, con sus maestros de normalidad, que relevan y multiplican las funciones del juez, se haya convertido en el instrumento moderno de la penalidad? ¿Puede extrañar que la prisión se asemeje a las fábricas, a las escuelas, a los cuarteles, a los hospitales, todos los cuales se asemejan a las prisiones? (Foucault, 1975/2022, p. 230).

Como indica también Giddens (1987, p. 156): éste «permite mantener al individuo bajo una observación minuciosa y escrupulosa». Esto, por tanto, va más allá de las preocupaciones primarias de Weber y nos conduce a cuestiones centrales sobre la «sociedad *dossier*», término acuñado por Kenneth Laudon (1986) basado en la creencia de que cada vez más los gobiernos modernos basan su desempeño sobre las bases de datos personales informatizadas de sus ciudadanos.

¿Qué pasó entonces entre el libro de *Domesday* del siglo XI y las redes entrelazadas de bancos de datos gubernamentales y administrativos del siglo XX occidental? El nacimiento de la sociedad moderna, con sus componentes constitutivos del capitalismo industrial, el Estado nación y el nuevo ejército, nos ayuda a dar respuesta a cómo se ha ido desarrollando el sistema actual.

Tanto el crecimiento cualitativo como cuantitativo de las tareas administrativas dentro de estas sociedades exigió algún sistema adecuado para mantenerlo todo unido. Para Weber (1946), la solución fue el desarrollo de la burocracia que, a medida que evolucionaba, se iba recomendando a sí misma como el medio superior para lograr los objetivos de la organización. Según Graeber (2015, p. 150), el sociólogo alemán sostenía que, una vez creado un sistema burocrático, éste se las ingeniaría para resultar indispensable para mantener el poder, a través de la monopolización del acceso a ciertos tipos de información clave.

¿Y cuáles fueron las tareas administrativas que proliferaron en los Estados nación del siglo XIX? Éstas eran la continuación de los tipos de actividad a los que ya se alude en la Inglaterra posterior a la conquista de Guillermo I: la recaudación de impuestos y otras cargas, el registro de la propiedad y, más tarde, algunos detalles estadísticos tales como nacimientos, matrimonios y defunciones, recopilados de una manera uniforme y constante. Posteriormente, y a medida que se amplió el derecho al voto, fue necesario crear registros de votantes potenciales; cuando se declaraba una guerra, había que llamar a filas a reclutas o voluntarios, etc.:

si uno crea una estructura burocrática para lidiar con un problema, esa estructura acabará, invariablemente, creando nuevos problemas que parecerá que sólo se pueden resolver, a su

vez, por medios burocráticos. En las universidades, a esto se lo llama el problema de «crear un comité para lidiar con el problema del exceso de comités» (Graeber, 2015, p. 150).

Los tipos de tareas administrativas emprendidas por el floreciente Estado nación durante el siglo XIX estaban, por tanto, cada vez más organizados sobre una base burocrática, a lo que había que sumar que la mayoría de ellos involucraban documentación personal y, por lo tanto, también pueden verse como contribuciones al surgimiento de la «sociedad de la vigilancia» (Lyon, 1994, p. 31).

El control de la movilidad de la población

Otra de las circunstancias que tienen lugar durante el siglo XIX es el desarrollo de los medios de transporte como el ferrocarril, el cual favoreció el incremento de la movilidad de la población. Este cambio viene acompañado, en palabras de Foucault (2004/2008, p. 93) de una nueva racionalidad que subyace en el gobierno de las poblaciones, a la que designa a través del concepto de gubernamentalidad.

Sin embargo, en esta forma nueva de gobernar, la libertad de circulación se encuentra con una paradoja: mientras el nuevo sistema económico y social proclama el fin del aislamiento entre diferentes regiones y por ende la posibilidad de la población de sustraerse de los enclaves mentales y físicos propios de la sociedad disciplinaria, esta expansión de los flujos migratorios no se puede llevar a cabo sin la equiparación del principio de seguridad (Mattelart y Vitalis, 2014/2015, p. 25). Dicho de otro modo, cuanto mayor es la movilidad, tanto mayor es la urgencia de intensificar el control por parte de los Estados, cuya la razón gubernamental buscará la domesticación del movimiento y ello condicionará los dispositivos dedicados a la identificación, seguimiento y vigilancia de las personas.

De esta manera, «[l]a sociedad disciplinaria es un sedimento de la sociedad de la circulación, de la misma manera que la sociedad de la soberanía había sido un sedimento de la sociedad disciplinaria que le había sucedido» (Mattelart y Vitalis, 2014/2015, p. 27). Las estrategias de soberanía, disciplina y gubernamentalidad funcionan como un triángulo al combinarse en lugar de sustituirse las unas de las otras. Por tanto, el principio de libertad económica propio de esta época resituía las tecnologías del poder a través de una nueva forma de gobernar, dejando el derecho a circular libremente sujeto también a otro nuevo privilegio de una parte de la población frente a otra. Buena prueba de ello la encontramos en este pasaje del código penal napoleónico de 1810 recogido por Bonneville de Marsangry (1844, citado en Mattelart y Vitalis, 2014/2015, p. 30):

En un Estado pequeño, dice el texto que recoge los motivos de la nueva legislación, todo el mundo es vigilado; nadie puede sustraerse al ojo vigilante de sus conciudadanos. Por el

contrario, en un imperio inmenso, es necesario que una institución tan inteligente como activa reemplace esta vigilancia de los unos hacia los otros.

Los medios preventivos y represivos de la vigilancia de la población general en democracia se ensayan, como hemos ido viendo anteriormente, a través del control del universo de la delincuencia, incluyendo el de aquellas personas que se estima que se desvían de la norma social. De esta manera, primero se realiza el control de aquellas consideradas como sensibles o de alto riesgo para culminar con la vigilancia de toda la población, siempre bajo el pretexto de la garantía de la seguridad nacional.

En el caso concreto de Francia, se creó un aparato estadístico estatal de medición de la criminalidad. Esta sistematización armonizó un sistema de recogida de datos y de construcción de series estadísticas periódicas de diversas áreas de la vida cotidiana, especialmente en los ámbitos industrial y agrícola, que ya habían comenzado a elaborarse tras la Revolución francesa y el Imperio napoleónico. Esta forma de descripción cuantitativa de la realidad social dotó a la administración francesa de una originalidad que la hizo establecerse como modelo para otros países (Mattelart y Vitalis, 2014/2015, p. 31).

Así, en 1827 se publicó por parte de la administración de la justicia penal un conjunto de mapas sinópticos, con datos de dos años antes, que reflejaba el estado de la criminalidad de los diferentes departamentos que componían el país galo. Esta cuenta general incluía, además de crímenes contra la propiedad y contra las personas, otras penas como las de nacimientos ilegítimos, desertiones militares, suicidios, el número de vagabundos y la mendicidad (Mattelart y Vitalis, 2014/2015, p. 31). En definitiva, se trataba de una estadística de base moral que instigaba a las autoridades a poner fin a estos fenómenos.

Estas estadísticas fueron posibles gracias a que el código de instrucción penal de 1808 obligaba a los diferentes tribunales a llevar a cabo un registro minucioso de todas las personas condenadas que incluía: nombre, apellidos, profesión, edad y lugar de residencia. De esta forma, Francia contaba con grandes bases de datos sobre sus criminales, si bien su consulta y actualización resultaban tediosas. Con el fin de subsanar este problema, la Dirección General de la Policía puso en funcionamiento un sistema conocido como “tabla móvil perpetua”, un método ampliamente utilizado por naturalistas, bibliotecarios y negociantes de la época. Este método consistía en un sistema de fichas dispuestas en orden alfabético en casilleros que remitían a sumarios sobre las condenas, lo que facilitaba en gran medida esta tarea.

Durante el siglo XIX, la moral industrial, reflejada en el código de Napoleón de 1804, asume el nomadismo como el paso previo a la criminalidad, e implanta medidas para penarlo, bajo la creencia de

que estas personas sin residencia «desconocen la ley suprema, que es el trabajo» (Frégier, 1840, citado en Mattelart y Vitalis, 2014/2015, p. 34). Siguiendo estas creencias, ya en 1781 el Antiguo Régimen impuso a los trabajadores de los diferentes gremios la obligatoriedad de portar un documento de identificación, en el que debían quedar registrados los certificados de trabajo, bien emitidos por sus empleadores o bien por la policía judicial.

Este documento quedó invalidado bajo la revolución al considerarse que era incompatible con la libertad de trabajo, pero en 1803 fue de nuevo restituido por Napoleón. El propósito de dicho carnet no era otro que facilitar el control y circunscripción de los obreros a la región administrativa de su lugar de trabajo. En él debían registrarse el nombre, apellidos, fecha y lugar de nacimiento, una breve descripción, su profesión y el nombre de su empleador.

De esta manera, los trabajadores solo podían moverse del territorio en el que estaban inscritos previa gestión de un visado por parte del alcalde o adjunto y siempre con el visto bueno de su patrón. Este método vinculaba la libertad del trabajador a los deseos de su jefe, dado que era este último quien custodiaba el documento durante el periodo laboral. Y es que todo aquel que se trasladase sin estar en posesión de la documentación reglada sería considerado vagabundo y correría el riesgo de ser detenido y castigado. Este carnet, aunque cayó en desuso entre 1860 y 1870, no fue abolido hasta 1890.

El registro: de la descripción a la biometría

La Dirección General de la Policía francesa introdujo en 1833 una ficha cuyo objetivo era el controlar a los condenados, pero con ella se enfrentaban a un crucial problema: la inexactitud de la descripción que la acompañaba la hacía una parca solución al dilema del correcto registro de la criminalidad.

Uno de los primeros intentos de solventarlo fue la implantación en los informes de los detenidos de los retratos de frente y perfil derecho — la fotografía de identidad judicial — que se había comenzado a utilizar durante la represión de los militares insurrectos de la Comuna de París de 1871. Durante este tiempo, el criminalista Alphonse Bertillon, inspirado en las teorías del estadista moral y pionero de los censos Adolphe Quételet, comenzó a combinar estas fotografías con medidas antropométricas, es decir, medidas del cuerpo, de la cabeza y de los miembros, para la identificación de delincuentes.

Pero no es hasta 1882 que la Dirección General de Policía decide implantar estos procedimientos y, a finales de esa misma década se instauró por primera vez el servicio de antropometría judicial. El proceso de identificación que se llevaba a cabo, conocido como “ficha parisiense”, constaba de cinco métodos diferentes: el antropométrico, la fotografía, la descripción física mediante signos abreviados y

fácilmente reconocibles a distancia, el color del iris y finalmente otros signos más particulares como deformidades, tatuajes o cicatrices.

Con la llegada de la dactiloscopia en la última década del siglo XIX se perfeccionan los métodos de identificación judicial, dado que se trataba de una marca biométrica única, permanente e inmutable. Si bien el pionero en el estudio de las huellas digitales y creador del primer sistema de clasificación de las líneas papilares fue el eugenista inglés Francis Galton, su método fue considerado demasiado complejo para la identificación a gran escala tanto por Scotland Yard como por parte de la comisión gubernamental que se encargaba de evaluarlo. Sobre este personaje, es importante recalcar, tal y como hace McQuillan (2022, p. 86) que:

Galton, que era medio primo de Charles Darwin, [...] quería afirmar la heredabilidad de la inteligencia como un factor explicativo de las jerarquías sociales y raciales. Anticipando los métodos predictivos del aprendizaje automático, Galton quería desarrollar una matemática para la intervención social. Su objetivo era fomentar una mejora general de la sociedad mediante la crianza selectiva, fomentando la producción de descendencia por parte de padres de alta inteligencia y desalentando a aquellos con menor inteligencia de tener hijos. Galton llamó a su programa «eugenesia», que significa «bien nacido» (Allen, 2001). Fundó el primer departamento científico para la promoción de la eugenesia en el University College de Londres, y fue sucedido allí por su protegido Karl Pearson.

Con todo, la primera persona que elaboró un sistema de clasificación manejable fue el responsable de estadística de la policía de la ciudad argentina de La Plata, Juan Vucetich, al reducir las huellas a cuatro grandes grupos y crear un sistema de archivo más sencillo, junto con un sistema de registro de control para saber si una huella se encontraba en el casillero donde se custodiaban. Este método fue el que acabó constituyéndose como referencia, junto con el del inglés Edward R. Henry.

El perfeccionamiento de las técnicas de reconocimiento atrajo el interés de ampliar el registro a la ciudadanía general. Esta fantasía alrededor de la matriculación universal se realizaría bajo la promesa de la garantía de la seguridad nacional. Sin embargo, estos deseos chocaron contra una opinión pública que ya venía objetando el uso de la fotografía para la identificación ciudadana, entendida como una afrenta a las libertades civiles (Noiriel, 1998, p. 100).

Mientras tanto, en los países de América Latina a finales del siglo XIX, las huellas digitales usadas en un principio para la identificación de criminales fueron rápidamente adoptadas para el seguimiento y fichaje de los inmigrantes que iban llegando en masa a sus costas. Al mismo tiempo, se acordó un plan

conjunto de unificación y centralización de intercambios de las fichas de los individuos considerados peligrosos entre las policías de los diferentes países entre los que se encontraban: Argentina, Brasil, Chile, Uruguay, Paraguay, Bolivia, Perú y Ecuador (Mattelart y Vitalis, 2014/2015, p. 41). Esta cooperación dio lugar a un ambicioso plan de generalización del carnet de identidad, que incluía fotografía y toma de huellas dactilares.

Al tiempo que la población de las capitales imperiales se resistía a la instauración de los documentos de identidad, en las colonias la situación era muy distinta, de hecho, estas regiones constituyeron un vasto campo de ensayo a escala real para la identificación. De esta manera, el Imperio británico decretó en 1897 la obligatoriedad del registro de las huellas digitales en todas las Indias británicas. Y en ese mismo año, la administración colonial francesa lo implantó en Indochina para el control migratorio de los trabajadores chinos en su región.

Considero muy significativo el hecho de que la realización de los primeros estudios sobre la dactiloscopia del anteriormente citado Francis Galton, se pudieron llevar a cabo gracias al gran banco de datos que supusieron las huellas dactilares de indígenas tomadas durante decenios por William James Herschel, alto funcionario de la administración civil inglesa en la región de Bengala (Mattelart y Vitalis, 2014/2015, p. 42). Y cómo, de nuevo, estas medidas de control y registro poblacional en los imperios británico y francés ocasionaron multitud de revueltas entre su población. Por su parte, McQuillan recalca que:

Lombroso utilizó sus datos sobre las geometrías de las caras y las cabezas de las personas para “probar” que algunas personas nacían criminales, justificando convenientemente su prejuicio de que los italianos del sur eran racialmente inferiores a los italianos del norte (Agüera y Arcas *et. al*, 2017). Aproximadamente al mismo tiempo que Lombroso hacía sus mediciones, el científico victoriano Francis Galton [...] perseguía objetivos similares al superponer exposiciones de criminales convictos en la misma placa fotográfica para destilar características esencialmente criminales (Agüera y Arcas *et. al*, 2017). Desafortunadamente para sus defensores, el carácter cientificista de la IA y su inmersión en una economía política racista significan que la fisonomía de la IA no es una anomalía sino un síntoma de algo más profundo (McQuillan, 2022, p. 69).

De vuelta al viejo continente, son las profesiones ambulantes y las personas nómadas quienes resultan objetivos de la vigilancia estatal. Ello se llevó a cabo en Francia mediante la imposición en 1912 del uso del carnet antropométrico individual, el cual debía someterse al control tanto a la entrada como a la

salida de cada región que visitasen. En él figuraban: nombre, apellido y/o apodo; fecha, lugar y país de nacimiento; una descripción antropométrica del sujeto, que en este caso incluía características como el matiz de la piel o el dorso y la base de la nariz; las huellas dactilares y dos fotografías del sujeto.

Para el caso de los niños menores de 13 años, sus huellas debían incluirse en un carnet colectivo de la familia o grupo, donde debían reflejarse también quiénes eran los integrantes de la unidad familiar, sus vínculos, así como fechas de boda, divorcio y fallecimiento. Las personas no eran las únicas que debían someterse a este registro, puesto que sus vehículos también debían contar con una “placa de control especial” dotada de un número de serie y del sello del Ministerio de Interior, la cual debía colocarse de manera visible en la parte trasera de la máquina.

Durante la Primera Guerra Mundial las autoridades extendieron la obligatoriedad de este documento a todos los extranjeros que se encontrasen en su territorio y a principios de los años 40, el régimen de Vichy extendió esta medida a toda la población francesa. El carnet antropométrico para los nómadas no fue abolido hasta 1969 y tras ello fue reemplazado por otro tipo de documentos. Sin embargo, no debemos olvidar que la ideología securitaria que justifica medidas como los documentos de identificación para los nómadas y su uso discriminatorio sigue muy vigente en nuestros días.

La estadística como forma de control social

Más allá de los usos policiales, la ciencia de las mediciones humanas constituyó el comienzo de una nueva forma de regulación social. Uno de los pioneros en la internacionalización de estos nuevos servicios estadísticos fue el ya mencionado sociólogo Adolphe Quételet, que publicó sendas obras sobre la antropometría y desarrolló la teoría del hombre medio. En esta última consideraba que solo a través de los datos de la masa poblacional se conoce realmente al individuo, como explica Caponi (2013, p. 835):

Quételet concluye, a partir de estudios cuantitativos y de la observación de datos empíricos, que cada año se repite, de manera exacta, el mismo número de crímenes, de suicidios, de matrimonios y de nacimientos en una población determinada. [...] Observa que el número de alienados, internados en los asilos, se mantiene asombrosamente constante y que el tipo de crímenes y las penas aplicadas permanecen regulares según los datos suministrados por los registros civiles y los psiquiátricos. El único modo de poder explicar esas constantes que tanto seducían a Quételet era analizar cada uno de estos hechos desde una perspectiva, ya no individual, sino poblacional. No se trataba de entender por qué razón ocurría cierto tipo de crimen y no otro, o por qué motivo un individuo presentaba una altura o peso

determinados. Se trataba de explicar la repetición de fenómenos que, por su constancia, parecían indicar alguna fuerza común a todos ellos, una causa común capaz de mantener ese equilibrio, la acción de leyes tan regulares como las que rigen los astros o la caída de los cuerpos.

Su proyecto de construcción de la física social se basaba, por consiguiente, en la capacidad de efectuar un cálculo lo más correcto posible. Para ello, además de sus propias observaciones, utilizó tanto las del aparato estadístico nacido de la justicia criminal y penal francesa, como los estudios territoriales y regionales de la Inglaterra de entre 1830 y 1860 sobre la ecología del crimen. Con ello quería comprobar que las reglas matemáticas dictaminan tanto las medidas individuales como las patologías sociales, por lo que con su cálculo se podrían predecir y controlar.

Con la expansión de este planteamiento de la estadística social, los métodos de predictibilidad del riesgo propios de las aseguradoras privadas pasan a emplearse para la gestión de toda la sociedad, lo que provocó una doble transformación en la forma de gobernar: por un lado, la tesis del hombre medio «hace que nos sintamos extraños a nosotros mismos» (Ewald, 1986, p. 147), ya que esta nueva identidad del ser humano, si bien nos quiere representar como suma, nunca conseguirá hacerlo de manera individual, de ahí quizá que nadie sienta que encaja por completo dentro de la norma. Y por otro, sienta las bases de la “sociedad actuarial”: «Al reemplazar la lógica de asistencia por la lógica del seguro, es la problemática de la responsabilidad la que cede ante la interdependencia calculada de los individuos» (Mattelart y Vitalis, 2014/2015, p. 48).

Una esquemática explicación de la “justicia actuarial” como base de la idea del “control actuarial” la ofrecen Cabello y Rascón al glosar la entrada que Dominique Robert escribió al respecto para una enciclopedia criminalística:

Para examinar el modo en que el control actuarial define y aborda el riesgo social partimos de las cuatro divisas fundamentales que Robert (2005, p. 11-12) asocia al concepto seminal de justicia actuarial: 1) “La desviación es normal”, por la que se considera la criminalidad un mero “subproducto de las sociedades modernas”; 2) “Perfiles de riesgo más que individuos”, por la que se encasilla a los sujetos desviados mediante variables de medición de riesgo; 3) “La gestión más que la transformación”, por la que se privilegia la administración de la desviación, y no el “diagnóstico y tratamiento” de las personas desviadas; 4) “El futuro más que el pasado”, por la que se explotan las técnicas estadísticas para “incapacitar y regular conductas futuras. (Cabello y Rascón, 2020, p. 278).

Como hemos venido observando, el control del individuo a partir de informaciones recogidas sobre él deriva, en parte, de las bases de datos recolectadas para uso policial, las cuales presenciaron un salto cualitativo en cuanto a organización y explotación en 1833 con el paso del registro a la ficha móvil. Su posterior evolución a formatos más pequeños y con mejores materiales facilitaron las tareas de ordenación, manipulación, clasificación, actualización e incluso destrucción (Mattelart y Vitalis, 2014/2015, p. 115). Con el paso del tiempo, este fichaje se extendió a otros sectores administrativos hasta llegar a la toda la población.

Esta progresión en el número de registros y almacenamientos de la identidad en papel, con formas cada vez más intrusivas sobre los datos que se incluían por parte de algunos Estados, ha traído multitud de tragedias consigo a lo largo de la historia. Una de las más notorias fue la relacionada con las diferentes formas de proceder por parte de Francia y de Países Bajos en relación a las fichas realizadas a sus ciudadanos durante la Segunda Guerra Mundial (Véliz, 2020/2021, pp. 133-136).

En marzo de 1940, Jacobus Lambertus Lentz, un inspector de registros de población holandés con una clara predilección por las estadísticas demográficas, propuso a su gobierno la idea de crear un sistema de identificación personal mediante la obligatoriedad del carnet de identidad. Este inspector había diseñado unos documentos que incluían elementos como tintas translúcidas y marcas de agua que dificultaban en gran medida su falsificación. En un principio, su gobierno rechazó esta idea dado que lo consideraban contrario a sus tradiciones democráticas. Sin embargo, su proyecto fue rescatado solo meses más tarde por las fuerzas de ocupación nazi, por lo que toda la población adulta de Países Bajos comenzó a portar un carnet de identidad en la que se incluía una “J” si la persona era judía, lo que rápidamente se convirtió en una sentencia de muerte en formato de bolsillo.

Como complemento a estos documentos de identidad y para ampliar la información registrada, Lentz utilizó las máquinas Hollerith desarrolladas por IBM, unos aparatos tabuladores para la realización de tarjetas perforadas que mejoraban el grabado y procesamiento de los datos (Black, 2001). Se daba también el caso de que en los Países Bajos, desde hacía décadas, y con la idea de realizar un seguimiento detallado de cada individuo «desde la cuna hasta la tumba» (Véliz, 2020/2021, p. 133), entre otros detalles personales, contaban con un registro sobre la religión que procesaban. El uso de estas máquinas tabuladoras por parte de Lentz y sus colaboradores es lo que facilitó en gran medida la identificación de estos datos que se habían vuelto extremadamente sensibles. Buena prueba de ello la recoge Hondius (1975) a través del relato de un testigo ocular:

Los ataques de la resistencia a las oficinas del censo han constituido actos heroicos para

salvar a personas, lo mismo que el ataque aéreo de precisión efectuado el 11 de abril de 1944 por la 63 escuadrilla de la Royal Air Force [...] que tuvo como resultado la destrucción de 250.000 expedientes individuales (p. 187).

En contraposición, en Francia, a pesar de ser cuna del registro poblacional, no se recogían datos sobre la religión que profesaban sus ciudadanos desde 1872. Además, tampoco habían instaurado el uso de tarjetas perforadas, por lo que la recopilación de estos datos se tornaba complicada. Para solventarlo, René Carmille, auditor general del ejército francés y entusiasta de las tarjetas perforadas, se ofreció para la tarea. De esta manera Carmille, con la creación de un número de identificación personal a escala nacional, se convirtió en el precursor del actual número de seguridad francés. En 1941, este auditor comenzó lo que sería el censo total de la población francesa de entre 14 y 65 años, en el que se enumeraban diferentes datos personales, como podía ser la profesión.

La clave se encontraba en la pregunta número once, donde se debía identificar la religión profesada a través de los abuelos paternos y maternos de cada individuo y donde los nazis esperaban encontrar su cribado entre personas judías y no judías. Sin embargo, estos datos nunca llegaron, sin ellos los nazis solo dependían de que los judíos se entregasen por voluntad propia o fuesen delatados por otras personas. Esto ocurrió porque René Carmille realmente formaba parte de la Resistencia francesa, y con esta supuesta operación censal llegó a generar 20.000 identidades falsas y utilizó estos mecanismos para identificar posibles adeptos a la resistencia:

Las respuestas a la pregunta número 11 sobre si los encuestados eran judíos jamás se tabularon. Los agujeros correspondientes nunca llegaron a perforarse y esos datos se perdieron para siempre. [...] Cientos de miles de personas fueron salvadas por una sola persona que decidió no recopilar sus datos (Véliz, 2020/2021, p. 133).

Lamentablemente, Carmille no corrió la misma suerte, las SS lo arrestaron en 1944 y, tras torturarlo durante días, fue enviado al campo de concentración de Dachau, donde murió en 1945.

Estas dos historias sobre la creación de los censos por parte de Francia y Países Bajos en una época tan convulsa, arrojan unos resultados cuantificables inequívocos: la tasa de mortalidad de habitantes judíos en Países Bajos fue la más alta de Europa, un 73%, mientras que la de Francia se situó en un 25%. Otra cifra que avala esta hipótesis se basa en la diferencia en la tasa de mortalidad entre los judíos residentes y los refugiados en Países Bajos, pues los índices de mortalidad de estos últimos fueron muy inferiores, dado que no figuraban en los registros oficiales (Seltzer y Anderson, 2001).

Además de este ejemplo, el uso indebido de los datos personales de los censos oficiales también se dio en otros lugares, como la expulsión de sus tierras de los Indios Americanos en Estados Unidos en el siglo XIX (Véliz, 2020/2021, p. 136). Aunque también es particular el caso del censo de la Unión Soviética de 1926, donde se preguntaba a sus ciudadanos abiertamente por su nacionalidad. Esta estadística permitió convencer a las élites soviéticas, principalmente rusos étnicos, de que se encontraban en minoría frente al conjunto de otras étnicas que conformaban la unión. «Esos resultados reforzaron significativamente la determinación de Stalin de erradicar dichas culturas, “reeducando” a sus pueblos en la ideología del marxismo-leninismo destinada a extirparles sus raíces» (Snowden, 2019, p. 252). Más recientemente también encontramos el uso del sistema de registro poblacional belga de los años treinta del siglo XX para el asesinato de los tutsis durante el genocidio de Ruanda de 1994 (Seltzer y Anderson, 2001).

Ya en este siglo XXI, con el uso extendido del ordenador surgen los ficheros automatizados y las grandes bases de datos sobre las personas, haciendo resurgir estas historias en nuestras memorias. De esta manera, los países que comienzan a informatizarse también toman conciencia de que una máquina capaz de registrar todo atenta contra la privacidad. Por lo que en los países democráticos se comienzan a establecer ciertas leyes para la protección de dichos datos frente a los Estados.

La vigilancia en el entorno laboral

Sobre el año 1890, Frederick W. Taylor comenzó a contabilizar el tiempo y los movimientos dentro de la fábrica. Para ello facilitó a una serie de controladores un cronómetro insertado dentro de un libro hueco, llamado *match book*, con el objetivo de registrar los gestos de los obreros de una manera más disimulada que a través de la observación directa. El conocimiento de esta experiencia organizativa de la división del trabajo se extendió gracias a la publicación de su libro *The Principles of Scientific Management* [*Los Principios de la Administración Científica*] (1911). La economía política pronto elevó esta obra a la categoría de clásico, ya que enaltecía a la clase gerencial y suponía la conclusión a las investigaciones sobre la naturaleza y la riqueza de las naciones de Adam Smith, así como el estudio de la economía manufacturera de Charles Babbage (Marshall, 1919).

Debo apuntar aquí que la sociedad capitalista no es la única que se rindió ante el taylorismo, ya que a partir de 1918, el poder soviético adoptó esta formulación y dictaminó que solo «la sociedad socialista será capaz de rematar esta conmoción, toda vez que el modo de producción capitalista está enzarzado en la anarquía de la competencia» (Mattelart, 2001/2007, p. 48).

Dicho esto, la aparición y el desarrollo de la empresa capitalista todavía nos ofrece una perspectiva muy

interesante sobre la importancia de la vigilancia en el mundo moderno. De hecho, un conocido punto de partida anterior al taylorismo para el análisis de la misma la encontramos en el trabajo de Karl Marx (1867/1975). Pero otros teóricos posteriores, como es el caso de Foucault (1975/2002), retomaron las tesis de Marx sobre cómo la vigilancia entendida como «pieza interna en el aparato de producción y engranaje especificado del poder disciplinario» (p. 180) pasaba a considerarse una operadora económica decisiva. Según Marx (1867/1975, p. 402): «Esta función directiva, vigilante y mediadora se convierte en función del capital no bien el trabajo que le está sometido se vuelve cooperativo. En cuanto función específica del capital, la función directiva asume características específicas».

El sistema capitalista introdujo en primer lugar nuevas formas de disciplinar a los trabajadores que, en sociedades anteriores, a menudo habían disfrutado de un grado mucho mayor de control sobre su trabajo. Cuando los trabajadores habían estado previamente bajo el dominio de un terrateniente u otro empleador, se disponía de formas físicas de coerción para hacer frente a la obstinación, el feudalismo implicaba fuerza. Pero cuando se aceptó que los trabajadores tenían derecho a disponer de su fuerza de trabajo como quisieran, por muy limitada que pudiera resultar esa elección, se buscaron otros medios para mantener a la gente en su puesto de trabajo.

La más obvia era la mera necesidad de sobrevivir sin ningún otro medio visible de sustento que el que un empleador podría ofrecer al otorgar un salario. Esto fue posible gracias a que en muchos lugares se arrebataron y cercaron los espacios comunes, *commons* en inglés, que ofrecían estos medios alternativos de subsistencia (Federici 2004/2010). La otra forma de coerción se hizo a través del desarrollo de la vigilancia, con la implantación del cronograma, la disposición de los cuerpos en espacios determinados y la observación y control sobre el trabajo.

El contraste entre la vida laboral en las sociedades tradicionales y en las capitalistas-industriales modernas se podría explicar a través de los cambios de concepción tanto del tiempo como de las rutinas diarias. Ya que, mientras que en entornos principalmente agrarios las rutinas diarias están limitadas por la estación, la luz del día y la marea, las rutinas de trabajo modernas están adaptadas al reloj. Tal y como describe Graeber (2018, p. 134):

En el concepto de tiempo tuvo que producirse un cambio. Durante siglos, los seres humanos fueron conscientes del concepto de tiempo absoluto o sidereal observando el firmamento, donde los fenómenos celestiales se producen con una regularidad exacta y predecible. [...] pero siempre se ha considerado que la vida en la Tierra es un poco más desorganizada. [...] Esto es algo extremadamente común: en aquellos lugares que carecen

de relojes, el tiempo se suele medir por acciones, en lugar de medir las acciones por tiempo.

El historiador inglés E. P. Thompson apuntó a una suma de transformaciones éticas y tecnológicas que se retroalimentaron. La introducción de los relojes domésticos y de bolsillo en el inicio de la revolución industrial, a finales del siglo XVII, propició que la misma postura se difundiera entre las clases medias. Todo el mundo empezó a ver el tiempo como los comerciantes de la época medieval: una propiedad limitada que necesitaba ser gestionada y gastada con gran meticulosidad, al igual que el dinero. Para este autor (1967, p. 60): ordeñar vacas, esquila de ovejas, arar campos, pescar, hilar y tejer eran actividades regidas en gran medida por factores “naturales”. Estos viejos ritmos de trabajo fueron reemplazados por las rutinas del “relojismo” de la fábrica y el taller dentro del capitalismo industrial. Para Thompson, por tanto, el énfasis estaba en el tiempo como mercancía.

Desde el momento en el que el tiempo se convirtió en dinero, se empezó a hablar de “gastar el tiempo” en lugar de “pasarlo”, y también de malgastarlo, matarlo, ganarlo, perderlo, ir a contrarreloj, etc. Los predicadores puritanos, metodistas y evangélicos comenzaron a instruir a sus feligreses en el arte de la “economía del tiempo”, advirtiéndoles de que la gestión cuidadosa del mismo era la esencia misma de la moralidad. Las fábricas comenzaron a emplear relojes de fichar; los trabajadores debían pulsar el reloj cuando entraban y cuando salían; las escuelas de caridad, concebidas para enseñar disciplina y puntualidad a los pobres, dieron paso a sistemas de escuelas públicas en las que a los estudiantes de todas las clases sociales se les enseñaba a levantarse y trasladarse a otra clase cada vez que oían el sonido de una campana, un procedimiento diseñado para entrenar a los niños para sus futuras vidas de trabajo asalariado en las fábricas. (Graeber, 2018, p. 136).

Sin embargo, sobre esta idea Giddens (1987) discrepa con Thompson, ya que para él, el reloj tiene un significado más general para la vida en el mundo moderno; sirve para sincronizar las actividades humanas en el “espacio-tiempo” (p. 152). Si bien admite que vender el propio trabajo como unidades abstractas de tiempo —el “de nueve a cinco”— es parte de la alienación que experimentan los trabajadores bajo el capitalismo, también enfatiza la importancia del reloj en la coordinación de todos los aspectos de la vida social en los tiempos modernos. Si bien el reloj se convirtió claramente en una parte vital del mecanismo de vigilancia moderno, especialmente en la fábrica capitalista, veremos más adelante que es el ordenador e incluso cada vez más el *smartphone*, quienes hoy día son los que coordinan nuestras actividades en el espacio-tiempo, incluidas aquellas que van mucho más allá de la

esfera productiva.

Las nuevas rutinas controladas por el reloj y la dependencia de la gestión en lugar de la fuerza fueron contribuciones importantes del capitalismo industrial a la modernidad. El control persistió, por supuesto, pero fue un control mediado de una manera más psicológica que física. Sin embargo, no debemos perder de vista, tal y como apunta Federici (2004/2010, p. 201) que:

También es posible observar que, desde el punto de vista del proceso de abstracción por el que pasa el individuo en la transición al capitalismo, el desarrollo de la «máquina humana» fue el principal salto tecnológico, el paso más importante en el desarrollo de las fuerzas productivas que tuvo lugar en el periodo de la acumulación primitiva. *Podemos observar, en otras palabras, que la primera máquina desarrollada por el capitalismo fue el cuerpo humano y no la máquina de vapor, ni tampoco el reloj.*

Con todo, esta «desmilitarización» de la producción es un componente del proceso más general de «pacificación interna» que tiene lugar en las primeras sociedades modernas (Lyon, 1994, p. 35). Conectan la práctica capitalista con el uso de prisiones en lugar de castigos brutales y públicos, con la vigilancia policial en lugar del uso de milicias para el mantenimiento de la ley y el orden, y con el crecimiento general del Estado administrativo. En cada caso, además, la vigilancia de las actividades se convierte en un aspecto más significativo de las relaciones de poder, pero no simplemente en el sentido de que se realza el poder del capital. Una vigilancia más estrecha también garantiza que los trabajadores están protegidos de acusaciones injustas y recompensados por el trabajo apropiado.

Sea como fuere, los nuevos métodos de producción provocan un cambio en el modo de vida integral, así se produce una unión entre la vida en la fábrica y la vida en sociedad y por consiguiente, una nivelación entre la vida pública y privada. Esta vigilancia gerencial del trabajo en cadena se combina con una dinámica similar en la vida privada. Este cambio del modo de regulación social trae consigo la deslegitimación de los intelectuales no positivistas, los considerados como “intelectuales orgánicos” no son aceptados en una sociedad regulada por el binomio taylorismo-fordismo (Gramsci, 1929). Buena prueba de ello la encontramos en el desarrollo de ciertos temas dentro de la cultura:

Lobotomía tayloriana y ciencia fordiana constituyen el telón de fondo sobre el que se ponen de manifiesto las distopías de Evgueni Zamiatin (1918-1921), y *Un mundo feliz* de Aldous Huxley (1932). *Los Tiempos modernos* de Charles Chaplin no andan lejos. La velocidad ha entrado al servicio de la obsesión productivista, la del hombre-medida sometido a desenfrenadas cadencias. (Mattelart, 2001/2007, p. 50).

Pero, ¿hasta qué punto las relaciones de clase asimétricas entre capital y trabajo definen realmente la vigilancia? En este punto persiste una tensión entre Marx y Weber (Dandeker, 1990, p. 35). Dicha tensión no deja de ser importante, ya que el carácter de la vigilancia tiene connotaciones bastante diferentes desde las ópticas de marxistas y weberianos. La cuestión se reduce a si el poder de vigilancia opera a lo largo del eje de las relaciones de clase o en relación con las divisiones burocráticas, incluidas las relacionadas con la ocupación y el empleo. Otra posibilidad, introducida por Foucault (1975/2002), es que el poder sea ubicuo y opere tanto en los dos niveles recién mencionados como en todos los demás niveles micro y macro de la sociedad.

Sin duda, la vigilancia capitalista moderna provocó una crisis de control. Como concluyó acertadamente Marx, la lucha está integrada en el contrato laboral capitalista (Lyon, 1994, p. 35). Los trabajadores siempre se han resistido en mayor o menor medida a la imposición de nuevas disciplinas y regímenes que eliminen su autonomía y responsabilidad dentro del entorno laboral. Sin embargo, su lucha por recuperar cierto control se expresa de una manera mucho más amplia dentro del movimiento laboral y los sindicatos surgidos en esta época.

Todo esto constituye un antecedente importante para los debates más recientes sobre la vigilancia. La posición teórica que uno adopta está estrechamente relacionada con las posibilidades políticas de cambio. Mientras que Marx era bastante optimista acerca de las posibilidades de una transformación revolucionaria que restauraría la autonomía y la dignidad de los trabajadores, Weber era todo lo contrario. Advirtió que «la dictadura de los funcionarios está avanzando, y que esto sería cierto incluso cuando las riendas del control estatal pudieran ser tomadas en nombre del socialismo» (citado en Foucault, 1975/2002, p. 36).

La vigilancia dentro del Estado de bienestar

Resulta importante señalar también que esta incipiente sociedad de la vigilancia tiene más de una cara. Puede verse desde la perspectiva del control social o desde la de la participación social. La maquinaria administrativa construida durante el siglo XIX puede entenderse como un fenómeno negativo (la “jaula de hierro” de la racionalidad burocrática de Weber o la “sociedad disciplinaria” de Foucault) o, más positivamente, como un medio para garantizar que se dé un trato equitativo a toda la ciudadanía. Por tanto, la otra cara de la vigilancia tiene que ver con la participación social y la ampliación de derechos de la ciudadanía.

Justo después de la Segunda Guerra Mundial, cuya experiencia estimuló gran parte de la transición del Estado de “guerra” al de “bienestar”, T. H. Marshall publicó *Citizenship and Social Class* (1950). Donde

argumentaba que los sistemas de bienestar “mitigan” los peores efectos de las desigualdades capitalistas y son un resultado de las conquistas tempranas de la ciudadanía, por tanto, son la base sobre la que se construyen los estados de bienestar.

Según Marshall, primero surgieron los derechos civiles, que tenían que ver con la libertad individual y la igualdad ante la ley. Posteriormente, los derechos políticos se desarrollaron en forma de un sufragio cada vez más amplio y el derecho a ser elegido como cargo político. Los que ocupan el tercer lugar, los «derechos sociales», están algo más vagamente definidos, pero comprenden, para Marshall, «un mínimo de bienestar y seguridad económicos» y el «derecho al disfrute del patrimonio propio y de la vida social de acuerdo con las normas prevalecientes en la sociedad» (Marshall, 1950, p. 11).

Desde este punto de vista, los sistemas de vigilancia de los Estados nación burocráticos avanzados no resultarían las máquinas represivas que los pesimistas indican, sino el resultado de aspiraciones y luchas de la ciudadanía. Si los departamentos gubernamentales deben tratar a las personas de manera equitativa, que es el punto de partida del primero de los derechos según Marshall, y del que se derivan otros derechos, entonces estas personas deben ser identificadas individualmente. Para ejercer el derecho al voto es necesario que su nombre figure en el censo electoral; para reclamar prestaciones sociales, los datos personales deben estar documentados, etc. Así, como insisten Nicholas Abercrombie *et. al* (1986), el hecho de tratar a las personas de manera individual, en lugar de simplemente como miembros de familias o comunidades, supone una ampliación de restricciones específicas pero también mayores oportunidades de vigilancia y control por parte de un Estado centralizado.

Sin embargo, la explicación de Marshall sobre los derechos de la ciudadanía ha sido criticada por varios motivos. Para empezar, deberíamos poner el foco en el nacimiento del concepto “Estado de bienestar”. De este modo, lejos de la estandarizada idea de que fue creado por unas benevolentes élites democráticas, Graeber (2015, pp. 153-154) se esfuerza en recordarnos que la mayoría de las instituciones que posteriormente se integrarían en el concepto de Estado de bienestar (como pueden ser la Seguridad Social, las pensiones o servicios públicos como bibliotecas y ambulatorios) fueron creadas por sindicatos, asociaciones de vecinas y vecinos y cooperativas de diversa índole, así como por partidos de los trabajadores. Según el antropólogo estadounidense, toda esa iniciativa institucional tenía la intención de crear una revolución social pacífica en pos de una Europa en paz marcada por un rápido proceso tecnológico.

El país que nos sirve de ejemplo de la absorción de dichos servicios por parte del Estado es la Alemania de Otto von Bismarck. Según Graeber, la preocupación por el auge de los partidos obreros en su

recientemente unido territorio empujó a Bismarck a crear una alternativa verticalizada a las escuelas, bibliotecas, teatros y demás instituciones y sistemas de ayudas creados desde una base social, despojándolos de los elementos participativos y democráticos que los caracterizaban. Para Graeber estas acciones tenían como objetivo que «el Estado del bienestar se creó en gran medida para evitar que las clases trabajadoras se volvieran revolucionarias» (Graeber, 2015, p. 245), para ello se apoya en una cita del propio von Bismarck recogida por Stead (1892, citado en Graeber, 2015, p. 245): «mi idea era sobornar a las clases trabajadoras, o mejor dicho, ganármelas, que vieran al Estado como una institución creada para ellos e interesada en su bienestar». Cuando otros partidos políticos llegaron al poder, continuaron este sistema e incorporaron otras instituciones creadas por y para obreros a la estructura administrativa del Estado.

Por otro lado, debemos tener en cuenta que este proceso de establecimiento de “derechos” tuvo lugar de diferentes maneras en otros países distintos al caso de Inglaterra, sobre el que se enfoca Marshall. Sin tener que alejarnos demasiado del sistema anglosajón, en Estados Unidos, por ejemplo, la participación democrática se extendió sólo lentamente más allá de los confines de una élite terrateniente masculina blanca. Los afrodescendientes en algunos estados del sur del país continuaron siendo excluidos mediante impuestos electorales y requisitos de alfabetización hasta los movimientos por los derechos civiles y las posteriores acciones judiciales en los años 60. Sin embargo, el punto esencial de la discusión sobre Marshall sigue siendo que la vigilancia moderna es simultáneamente un medio de control social y de garantía de derechos de participación social.

Sobre esto, Giddens (1985) afirmaba que Marshall minimizó el papel de los “derechos económicos” en su análisis de cómo la “ciudadanía” ha “mitigado la lucha de clases” en los tiempos modernos (pp. 201 y ss.). Para Giddens, el elemento económico, visible en la existencia de sindicatos y en la legislación en favor de los derechos de los trabajadores resulta un elemento de “doble filo”. Ya que puede resultar una relación con la vigilancia y el control de las clases subordinadas, o bien una palanca de lucha para contrarrestar ese control. En otras palabras, se demuestra una vez más que la vigilancia es más compleja de lo que una lectura puramente marxista (basada en la preponderancia del poder de clase) podría hacernos pensar.

Si bien los comentarios de Giddens son en cierto modo un correctivo oportuno, también vale la pena señalar que los derechos sociales, tan importantes para Marshall, parecen haber sido absorbidos por los derechos económicos de Giddens. Sin embargo, también exhiben el citado carácter de “doble filo” de los sistemas de vigilancia. Se puede afirmar que las prestaciones sociales alivian la pobreza, pero a cambio del escrutinio de estas personas por parte de los trabajadores sociales. Quizás el problema

radique en una definición demasiado estrecha de estas esferas de vigilancia y de los derechos de la ciudadanía.

En resumen, el surgimiento de la sociedad vigilada, está indisolublemente ligado al crecimiento del Estado nación moderno. A medida que se amplió la gama de tareas administrativas necesarias, la organización burocrática evolucionó como medio de coordinación de actividades. Así, la vida cotidiana estuvo cada vez más sujeta a documentación dentro de los archivos omnipresentes del Estado burocrático. Todo esto puede verse desde dos perspectivas; como un intento de imponer nuevas formas de orden, de controlar situaciones que amenazaban con convertirse en caos a medida que nacía el ahora familiar mundo urbano-industrial, o como resultado de la búsqueda de una ciudadanía plena y una participación democrática en el nuevo orden, que exigía, para un trato justo, que las personas fuesen identificadas, registradas y documentadas en expedientes cada vez más numerosos.

Sobre esta visión actuarial de la sociedad, vale la pena que nos detengamos en las prematuras teorías de Émile de Girardin (1852), que desde una visión utopista, fantaseaba con una sociedad que al ver reducidos todos los riesgos y futuribles posibles a la forma matemática, oscilaría en torno al seguro universal. Este autor se adelantó en sus tesis a la creación de la identificación individual, al afirmar que, para que el Estado llevase a cabo acertadamente su labor como una gran empresa colectiva de ahorros y mutua al mismo tiempo, debía implantar un gran registro de toda la población, donde cada habitante contaría con una cuenta de crédito hasta su muerte (Mattelart y Vitalis, 2014/2015, p. 48).

Esta “inscripción de vida” reemplazaría cualquier otro documento oficial, de manera que, al inscribir a una persona y asignarle una cuenta constantemente actualizada y supervisada por el Estado, permitiría una indagación tan fácil y exacta como suponen las direcciones postales hoy día. Se trataba, afirma Girardin, no de destruir la libertad sino despejar la oscuridad. Según él, “el hombre de bien” que no tiene nada que esconder conservaría su libertad, solo la perdería aquél que obrase el mal (Girardin, 1852, pp. 28-29). Esta teoría se adelanta a posteriores alegatos que enfatizan la total transparencia por parte de la ciudadanía en favor del principio de seguridad de los Estados. En este sentido, resulta llamativo ver cómo los ecos sobre las tesis de Girardin de mediados del siglo XIX todavía resuenan en los discursos de ciertos empresarios y políticos de nuestro tiempo.

Algunas conclusiones sobre la vigilancia moderna

Como comentaba al comienzo de este punto, la realidad sobre las diferentes dimensiones de la vigilancia en la época moderna es mucho más compleja que la disección que he ido realizando. La mayoría de las veces ocurrían a la vez y de manera entrelazada y la visión de los teóricos se veía

asimismo influenciada por ello.

La organización militar dio pistas sobre la civil, en parte gracias a la traslación de ciertas empresas militares a este entorno, muy visible en, por ejemplo, el caso del servicio postal alemán del siglo XIX (Graeber, 2015, pp. 152-161). Sobre las teorías de Weber, éste estuvo a su vez muy influenciado por el estudio del ejército prusiano (Beetham, 1987, p. 16). De hecho, «una de las razones por las que Weber pudo describir la burocracia como la encarnación misma de la eficacia racional fue que en la Alemania de su época las instituciones burocráticas realmente trabajaban bien» (Graeber, 2015, p. 152).

La organización burocrática se encontraba en entornos tan diversos como la empresa capitalista, el ejército y el departamento gubernamental. Las explicaciones de Marshall sobre la ampliación de los derechos de la ciudadanía nos lleva de manera similar a través de diferentes esferas sociales, cada una de las cuales conlleva implicaciones para el seguimiento y la documentación sobre los individuos.

¿Qué conclusiones pueden extraerse, por tanto, que puedan arrojar pistas para un análisis más profundo de la vigilancia actual?

En primer lugar, continuamos viendo las cuestiones relativas al poder. Hemos visto cómo la vigilancia reemplaza progresivamente a la coerción física como medio para mantener el orden y coordinar las actividades de grandes poblaciones, especialmente en los contextos del capitalismo y el Estado nación. La vigilancia también sigue estrechamente relacionada con el conocimiento, expresado de diversas formas en las tareas especiales del funcionario burocrático o del administrador de empresas, quienes están cada vez más separados de aquellos a quienes supervisan. Estar “informado” claramente tiene consecuencias para la disciplina y el poder. Pero si la modernidad no puede reducirse a una de sus dimensiones, entonces debemos tener cuidado de no ver el poder de la vigilancia como algo relacionado exclusivamente con un aspecto determinado.

En segundo lugar, nos encontramos ante cómo se experimenta la vigilancia. Si bien las teorías sobre el panóptico pretenden trasladar las mecánicas de la vigilancia al propio cuerpo del individuo, lo cierto es que parte de la respuesta a la cuestión del poder es que éste no es absoluto. El control de los cuerpos pasa en primer lugar por las personas consideradas en los bordes; delincuentes, enfermos, extranjeros, etc. y se va extendiendo hacia toda la sociedad. Esta vigilancia se origina de manera paradójica —siendo el resultado de la búsqueda de seguridad y también de un mayor control estatal centralizado— y se experimenta con ambivalencia. Por un lado, aceptamos la protección o la obtención de derechos que de ella se puede derivar (seguridad, derecho al voto, prestaciones sociales) y al mismo tiempo la sentimos como un ataque a nuestra privacidad cuando traspasa los límites que entendemos como tal o vemos

amenazada nuestra autonomía.

En tercer lugar, la cuestión política; ¿se convierte el control de la información en la cuestión clave en una “sociedad de la vigilancia”? Como hemos visto, la capacidad de vigilar ha crecido sistemáticamente en las sociedades modernas, cada vez los expedientes sobre la población son más mayoritarios, más extensos y se encuentran más centralizados. La velocidad del flujo de la información y el número de contactos entre los sistemas administrativos y las poblaciones sujetas también ha crecido exponencialmente. Los Estados cada vez se asientan más como garantes de la seguridad y cuentan con la legitimidad del uso de la fuerza, pero es a través del control de la población y su capacidad de gestionar los diferentes servicios sociales donde llevan a cabo la mayor parte de su ejercicio del poder.

En cuanto a la vigilancia en el entorno laboral, académicos como Karl Marx observaron que «la supervisión de los trabajadores, la fragmentación de las tareas, la separación entre tareas mentales y manuales y la regimentación del trabajo» (citado en Zureik, 2003, p. 31) resultaban un medio para subordinar el trabajo al capital. Estos temas se entrelazan mediante la aplicación de nuevas tecnologías que afectan a las relaciones de poder. En cierto sentido, dicha vigilancia expresa un tema constante: quienes establecen algún medio para vigilar a los demás están demostrando que no confían en quienes están siendo vigilados. Los estudios de la vigilancia en el entorno laboral a menudo siguen el enfoque de Foucault sobre las microtécnicas de disciplina que apuntan y tratan el cuerpo como algo que debe ser observado y probado (Staples 2000, p. 9).

A finales del siglo XX, las tecnologías microelectrónicas se introdujeron ampliamente para aumentar y sostener las actividades de vigilancia sobre una base aún más amplia que la conocida en la era de los documentos mecanografiados, las regulaciones impresas y las fichas. Aunque el impacto de las tecnologías electrónicas comenzó a sentirse en la esfera de la vigilancia mucho antes de este tiempo, dado que las comunicaciones telefónicas, por ejemplo, fortalecieron considerablemente la vigilancia, la administración gubernamental y las empresas comerciales desde principios del siglo XX. Con todo, en la época actual todavía conviven formas de control y vigilancia propias de la modernidad, como la máquina de fichar o la arquitectura panóptica; estos mecanismos se han ido ampliando y diluyendo hacia otras esferas como la del *marketing* y el consumo hasta inundar nuestra vida cotidiana con objetivos diferentes al de los poderes hegemónicos de épocas anteriores.

2.1.3. Vigilancia digital y Sociedad de la Información

En este punto debemos comenzar a poner el foco en las diferentes tecnologías vinculadas a la información que se han ido desarrollando durante el siglo XX y en cómo afectan a las formas de control que operan. Y esto es debido a que, al percibir la historia social a través del escaneo tecnológico, no es aconsejable continuar imaginándola como una secuencia, ya que diversas consecuencias se entrelazan bajo la hegemonía de la última versión tecnológica que surge. Si bien los ejes sobre los que se vertebra el mundo actual combinan el conocimiento práctico y el “saber hacer” de épocas anteriores, debemos siempre verlos desde la combinación de las lagunas, supervivencias, desviaciones, regresiones y resistencias que estas tecnologías generan. De esta manera, la historia actual queda compuesta de realidades sociales, políticas y económicas que son asimétricas y asincrónicas. Una vez más, se reafirma la idea principal de que los modelos dominantes de regulación social abiertos, transparentes y cambiantes de ninguna manera eliminarán los mecanismos disciplinarios del mapa cognitivo, incluso si los sitios de reclusión están en crisis y comprometidos con su permanente reforma (Mattelart, 2007/2009, p. 234).

Las nuevas tecnologías de la información aportan innovación al tiempo que activan y “modernizan” antiguos procedimientos y protocolos, adaptándolos a lo que hoy se considera una sociedad móvil. Como ejemplo de ello, Mattelard y Vitalis (2014/2015, p. 234) aluden a que con la implantación de las pulseras electrónicas móviles (PSEM, por sus siglas en inglés), «parece que se desvanecen los muros de la prisión y los carceleros, al ser suficiente la virtualidad de límites intangibles y obligaciones interiorizadas». Pero aquellos condenados que no cumplan con sus obligaciones volverán a ser encarcelados. «Detrás del aspecto etéreo de la pena *high-tech* se levantan las torretas de vigilancia y las alambradas de la inerradicable prisión» (Razac, 2007, párr. 3). Además, la dualidad de los componentes militar y civil permiten la transferencia de conocimientos prácticos adquiridos de un campo a otro. Las últimas tecnologías de posicionamiento y navegación combinan de esta manera un control flexible y aspectos propios de las disciplinas.

Sin embargo, existe una destacada diferencia entre las dos modalidades de vigilancia; las disciplinas precisan la implicación del individuo para cambiar su comportamiento, mientras que este nuevo control ubicuo se efectúa indirectamente y a espaldas del sujeto, por lo que no necesita de su participación. «Se trata de vigilarlo y de tomar decisiones sobre él a partir de un doble constituido por sus informaciones, sus huellas o su imagen» (Heilmann y Vitalis, 1996, p. 78). Esto resuena con los apuntes que realiza Lessig (2001/2009) sobre la capacidad de autoejecución de la arquitectura: «en la medida en que podemos dar lugar a efectos a través de las restricciones automáticas del código del espacio real, no

necesitamos depender de la actividad, lealtad o responsabilidad permanente de los individuos» (Lessig, 2001/2009, p. 532). Diferenciándola de esta manera de la regulación legal o normativa:

La ley y las normas son tanto más eficaces cuanto más subjetivas son, pero necesitan de un mínimo de subjetividad para llegar a ser efectivas. [...] Una ley que castigase secretamente a las personas por delitos cuya existencia desconocen no sería efectiva a la hora de regular la conducta que castiga. Pero esto no sucede con la arquitectura. La arquitectura puede restringir sin necesidad de ningún mínimo de subjetividad. [D]el mismo modo que no es necesario que ningún agente imponga la restricción, tampoco lo es que el sujeto la comprenda (Lessig, 2001/2009, p. 536).

A partir del siglo XX, estas formas de vigilancia operan también fuera del control de los Estados, aunque en multitud de ocasiones trabajan de manera conjunta a ellos. Las necesidades de anticipación y predicción formarán parte de los estudios de *marketing* y sobre los gustos del consumidor.

De la vigilancia moderna a la posmoderna

Como hemos visto, las teorías de la vigilancia moderna se relacionan con aquellos tratamientos clásicos que la entienden como consecuencia tanto de las empresas capitalistas, la organización burocrática y el Estado nación, como del desarrollo de nuevos tipos de solidaridad, que implican menos confianza o al menos diferentes tipos de confianza (Lyon, 2001, p. 109ss). Sin embargo, la teoría de la vigilancia de una época que podemos describir como posmoderna, aborda lo que Staples (2000, p. 11) considera nuevas formas de control y visibilidad: tipos de vigilancia basados en la digitalización de la información, que resultan cotidianos y universales.

Los contornos principales de las teorías modernas de la vigilancia se derivan del análisis de los ya citados Marx y Weber. Pero llegados a este punto, debemos realizar dos adiciones que resultan muy interesantes para este tiempo. Uno es el trabajo de inspiración weberiana del sociólogo y jurista francés Jacques Ellul (1954/1967), y el otro es la gran influencia teórica del trabajo del novelista y crítico social George Orwell (1903-1950). Uno legó un fuerte interés en la dinámica tecnológica de la vigilancia, y el otro una idea de sociedad de vigilancia total mediante la cual se puede medir el grado de poder de la misma en un entorno determinado. Ambas figuras también aportaron una seriedad moral y una urgencia política al desarrollo de la teoría de la vigilancia de mediados y finales del siglo XX.

Ellul puso énfasis en “la técnica”, es decir, realizó una orientación cultural hacia los “medios” más que hacia los “fines”, por lo que podemos encontrar en él algunos puntos en común con la obra de Weber.

El trabajo de Ellul, centrado en la crítica del totalitarismo, fue reconocido como una contribución significativa por muchos investigadores y escritores de los primeros estudios de la vigilancia (Lyon, 2007, p. 52). Por ejemplo, se tuvo en cuenta en el trabajo de Gary T. Marx (1988) sobre la vigilancia policial encubierta o en el de Oscar Gandy (2006) sobre la economía de la información personal. La idea de “flujo de vigilancia”, ahora ampliamente utilizada en este campo, también se origina en el trabajo de Ellul. Este término, o más bien la tendencia a la que apunta, se utiliza, por ejemplo, para el establecimiento de sistemas de tarjetas de identificación digitalizadas, que tienden a ampliarse para incluir otras funciones no previstas originalmente por sus promotores (Lyon, 2001, pp. 111-113).

El trabajo de Orwell, por otra parte, ha proporcionado algunos de los conceptos más duraderos, notorios y públicamente accesibles en los estudios de la vigilancia, sobre todo la figura del Gran Hermano, de su obra *1984* (1949). Vale la pena mencionar aquí la ambigüedad de Orwell con respecto a la ubicación real de la sociedad de 1984. Si bien muchos consideraron su trabajo como una crítica al socialismo de Estado, Orwell no dejó que las democracias liberales occidentales se salieran del apuro tan fácilmente. Está claro que su obra apunta a las tendencias totalitarias —entre las cuales la vigilancia estatal ocuparía un lugar destacado— como inmanentes dentro de cualquier Estado nación organizado burocráticamente (Lyon, 2007, p. 53).

Otro teórico destacado que defiende el papel central de la vigilancia en la vida moderna es Anthony Giddens (1985), el cual lamenta el predominio en la sociología de finales del siglo XX de las teorías influenciadas por Marx, por un lado, y de lo que él llama teorías de la sociedad industrial, por el otro. Giddens insiste en que la vigilancia y el militarismo no deben verse simplemente como un producto del capitalismo o la burocracia. Para él, la vigilancia se refiere tanto a la acumulación de información codificada como a la supervisión directa de la vida social (Giddens, 1985, p. 13), y puede convertirse en un medio importante de dominación.

Aunque el trabajo de Giddens supone una ruptura con el relativo descuido de la vigilancia en la teoría social, Lyon (2007, pp. 53-54) hace dos observaciones sobre su contribución. La primera es que la distinción entre “supervisión” e “información codificada” se vuelve cada vez más difícil de mantener en un mundo digital donde dicha información se convierte cada vez más en un medio de supervisión. Y en segundo lugar, la suposición de Giddens de que la vigilancia es principalmente una característica de los Estados nación es difícil de sostener cuando los datos personales, utilizados con fines regulatorios, se procesan promiscuamente en muchos ámbitos no gubernamentales, pero con indudables consecuencias gubernamentales.

De hecho, desde finales del siglo XX se ha hecho cada vez más notorio que la vigilancia está sufriendo algunas alteraciones severas, a medida que el contexto político-económico avanza hacia un capitalismo más centrado en el consumo y se adoptan nuevas tecnologías digitales en las diferentes organizaciones. Esto significa, por ejemplo, que aquellos que pensaban en términos principalmente *orwellianos* han tenido que considerar prácticas de vigilancia mucho más allá del Estado nación —por ejemplo, en publicidad y *marketing*— e involucrar tecnologías que tienen mayor velocidad y capacidad y, por tanto, son mucho más sutilmente interactivas que cualquier máquina anterior. Estas nuevas tecnologías hacen posible la automatización y el mantenimiento de registros permanentes, y como consecuencia, el cuerpo puede ser observado, evaluado y manipulado de nuevas maneras. Podemos decir, por tanto, que la vigilancia cotidiana se vuelve local e inmediata, mientras que los datos de grandes poblaciones se capturan para clasificarlos y examinarlos.

Este último punto resulta especialmente significativo, pero también debe abordarse con sumo cuidado. Cualquier teoría social y política que intente incorporar lo tecnológico es vulnerable a acusaciones de “determinismo” (Lyon, 2007, p. 54). Y es que, sin la habilitación de nuevas tecnologías la extensión de la “visión” queda restringida (Marx, 1988, pp. 217-219), la usabilidad entre sistemas y la integración en red resultan imposibles, y la “clasificación social”, es decir, la discriminación digital generalizada que hace posible un tratamiento diferente de distintas categorías de población (Graham y Wood 2003; Lyon, 2003b), no podría ocurrir en la escala en que ocurre hoy.

Las versiones más “posmodernas” de las teorías de la vigilancia, como dice Staples (2000), subrayan tipos de vigilancia cotidianos, universales, basados en la digitalización de la información. Por su parte, Mark Poster (1996, citado en Lyon, 2007, p. 54) hace algunas observaciones importantes al respecto, sugiriendo cómo la teoría postestructural nos ayuda a ver las bases de datos como “discursos” y los dobles de datos (término sobre el que nos detendremos más adelante) que se generan, como entidades simultáneamente independientes y dependientes. Para él, esto significa que vivimos en la era del “superpanóptico”. Así, lejos de producir los sujetos “interiorizados” de Foucault, conscientes de su autodeterminación, el discurso de las bases de datos produce individuos objetivados con “identidades” de datos dispersas de las que algunos tal vez ni siquiera sean conscientes. El cuerpo ya no es un bastión que debe protegerse como “espacio privado”, ya forma parte del superpanóptico.

Los aspectos de la vigilancia posmoderna también objetivan el cuerpo puesto que pueden apreciarse en la visibilidad de los mismos ante las agencias de vigilancia, que ahora resultará casi constante en algunos contextos, y en la creciente atención al propio cuerpo como fuente de datos (este aspecto tampoco se limita a agencias externas), como veremos de manera más ampliada en el punto 2.4. A medida que

nuevos tipos de vigilancia se filtran en todas las esferas de la vida, algunas personas se involucran en una autovigilancia de manera bastante precisa y sistemática.

Este carácter cotidiano de la vigilancia posmoderna se refiere a las formas en que la regulación de la vida diaria va mucho más allá de la desviación criminal o laboral. Las categorías de vigilancia ahora incluyen grupos geo-demográficos de estilos de vida, clasificaciones psicológicas, diferencias educativas y distinciones de salud. La vigilancia se torna universal en el sentido de que nadie es inmune a su mirada. La vigilancia también resulta universal en el sentido de que siempre que se adoptan nuevos sistemas, tienden a tener un carácter tecnológico similar.

Sin embargo, lo que realmente sucede en el terreno y en la vida diaria probablemente muestre una mezcla de características de vigilancia “modernas” y “posmodernas”. Si bien la gestión de riesgos y los nuevos modos de gobernanza bien pueden verse en la extracción preventiva de datos o en los Circuitos Cerrados de televisión (CCTV) predictivos, que buscan patrones de comportamiento en lugar de delitos reales, en la mayoría de los países el poder del Estado sigue siendo fuerte. Los sistemas de CCTV en espacios públicos, por ejemplo, aunque pueden funcionar con fines comerciales o subcontratarse a empresas operativas, todavía funcionan en conjunto con los departamentos de policía, y las autoridades de espionaje estatales aún pueden exigir imágenes de ellos. Por “posmoderna” que sea la situación, lo “moderno” todavía está presente en la palabra y en la realidad social.

Marketing y Consumo: la clasificación social

Si bien durante mucho tiempo, los Estados habían sido los encargados de perfilar a las poblaciones, es durante el período de entreguerras, con el surgimiento de la industria del *marketing* y de la publicidad contemporánea, donde las cosas comenzaron a cambiar. Esto es debido a que los teóricos de la opinión pública sostenían que las masas, entendidas como espectadoras de la acción y no como participantes, debían ser gobernadas por una minoría inteligente, una especie de especialistas, para su propio beneficio (Mattelart 2001/2007, p. 49).

En los años de posguerra surgió una fase cualitativamente nueva del capitalismo de consumo basada en un nuevo modelo de negocio compuesto por: los clientes, es decir, las compañías que fabrican los productos y pagan para publicitarlos; las agencias de publicidad que preparan y colocan los anuncios y los medios de comunicación; y los periódicos, revistas, estaciones de radiodifusión, cada uno un medio individual para llevar el mensaje al público. Aunque, más allá de la publicidad misma, estaba el ámbito mucho más amplio del *marketing* corporativo, que involucraba áreas como la segmentación, la investigación de la motivación, el diseño de productos, la promoción de ventas y el *marketing* directo.

De esta manera, el consumo se fue configurando progresivamente como un campo inagotable de experimentación para la creación de métodos de seguimiento y de registro sobre el comportamiento del consumidor. El *marketing* evolucionó rápidamente en su período de mayor avance en la década de 1950 hasta convertirse en un sistema altamente organizado de vigilancia del cliente, propaganda dirigida y manipulación psicológica de las poblaciones. Empresas especializadas comenzaron a analizar las preferencias, los deseos, los intereses y los movimientos y gestos de la persona durante este proceso de «taylorización del consumo» (Mattelart y Vitalis, 2014/2015, p. 71). Se trataba de comprender en profundidad su identidad para poder ofrecerles bienes y servicios adaptados a sus demandas, e incluso ayudarles a definirlos. Esta avanzadilla del consumo en el orden mundial no ha dejado de perfeccionar sus métodos de observación y análisis de los comportamientos de los consumidores, con el fin de identificar segmentos y perfiles cada vez más detallados, gracias también a que las tecnologías de la comunicación se han sofisticado.

Los agentes privados, cuyo modelo económico se basa en las lógicas del *marketing*, llegan a ser los mayores fichadores de los consumidores potenciales o reales debido también a la capacidad creciente de memoria de los soportes digitales que se inmiscuyen en nuestra vida diaria. El establecimiento de monopolios basados en la explotación comercial de los datos personales, que a menudo provienen de la provisión de servicios gratuitos y de la participación de las personas, es un acontecimiento destacado que resulta de esta larga evolución. Prueba de ello son los procesos antimonopolio en que están inmersos distintas compañías, en particular la sentencia de 5 de agosto de 2024 que condena a Google como un “monopolio ilegal”, con el posterior pronunciamiento del Departamento de Justicia de EEUU, que ordena su partición en varias empresas separadas, esencialmente la división entre su negocio de buscadores y el de publicidad (Peirano, 2024). Y es que, a través de las herramientas de captación, medida y previsión de actitudes que brindan las tecnologías en red de la economía digital, se ha llegado al punto de considerar a las personas como una fábrica de datos. Mediante la entrega voluntaria de dichos datos a las empresas incluso en algunos casos sin que el individuo lo note, convierten a estos sujetos en co-productores de la información. De esta manera, el valor agregado de un servicio o producto cada vez se ajustará más y de manera más sofisticada a la demanda.

La financierización (o el crecimiento a largo plazo de la especulación sobre activos financieros en relación con el PIB) desarrollada en Estados Unidos durante los años ochenta se vio espectacularmente potenciada por las redes informáticas de alta velocidad, que se convirtieron en mecanismos decisivos para los mercados especulativos recién creados, y por una cantidad no pequeña de «artimañas financieras» (Lewis, 2014). Al igual que la publicidad y la seguridad nacional, la financierización tenía

una necesidad insaciable de datos. De hecho, su rentable expansión dependió en gran medida de la titularidad de las hipotecas de los hogares, de una ampliación del uso de las tarjetas de crédito y del crecimiento de los seguros de salud y los fondos de pensiones, los préstamos a los estudiantes y otros elementos de las finanzas personales. Todos los aspectos relacionados con ingresos, gastos y el crédito de los hogares se incorporaron a enormes bancos de datos y se evaluaron en términos de mercados y riesgos. Para el año 2000 casi todas las grandes corporaciones de los Estados Unidos estaban construyendo enormes bases de datos y estaban vinculadas a empresas de minería de datos (Dawson, p. 51).

Esta financierización significó la intrusión de las finanzas en todos los aspectos de la vida, al igual que en los “sectores tradicionales”, aquellos que suelen identificarse con la “producción-producción”, empezando por la industria automovilística (Moulier Boutang, 2010/2012, pp. 151-152), lo que exigió nuevas extensiones de vigilancia y control de la información como formas de gestión del riesgo financiero. A medida que la economía se volvió más financierizada, se tornó también más vulnerable a las crisis financieras, lo que aumentó la percepción de riesgo por parte de los inversores y la necesidad percibida de gestión de riesgos, cifrado de datos y seguridad (Foster y McChesney, 2014, párr. 54).

Si atendemos a los procesos de “clasificación social” como un medio para comprender cómo las prácticas de vigilancia reales tienen resultados particulares (Lyon, 2003b), una serie de estudios de la vigilancia hacen uso del ya mencionado término gubernamentalidad de Foucault. Sin embargo, van más allá, al indicar cómo se forman los patrones de poder, desigualdad e injusticia en situaciones concretas y cuáles pueden ser sus consecuencias sociales y políticas más amplias. En términos de algunas líneas clásicas de división, se puede explorar cómo, por ejemplo, las divisiones de género, raza y de clase pueden ser mitigadas o reforzadas por regímenes contemporáneos de gobernanza y rutinas de vigilancia asociadas (Lyon, 2007, p. 63).

Para Oscar Gandy (2006), los marcadores de raza y género dentro de los modelos predictivos, como los de atención médica, dan como resultado una “distribución desigual de los daños”. Una buena síntesis de estas características la ofrecen Brandariz y Faraldo (2007, citados en Cabello y Rascón, 2020, p. 278) al afirmar que:

En definitiva, se tiende a adoptar una lógica más de redistribución que de reducción del riesgo, que era el objetivo básico en la etapa anterior, y que hoy se asume como inabordable, aunque solo sea porque se normaliza la existencia de segmentos sociales permanentemente marginalizados, excedentarios.

De este modo, se hace recaer sobre las poblaciones más vulnerables toda suerte de sobrecostes en términos de vigilancia y control con el fin de dotar de cobertura a las poblaciones más acomodadas. Además, como las decisiones pasadas suelen estar vinculadas con opciones futuras, estas dificultades tienden a agruparse dentro de lo que denomina patrones de “desventaja acumulativa”. Otro desafío importante basado en la vigilancia aparece en el trabajo de Roger Burrows y Nicholas Gane (2006), quienes muestran cómo la teoría de clases sociales se enfrenta a las prácticas de *marketing* actuales. Estos autores sostienen que el uso de datos geo-demográficos para clasificar a los grupos de personas según su lugar de residencia es ahora tan significativo que desafía algunas formas convencionales de concebir la clase social.

Para Didier Bigo, el análisis de Agamben (1997) de la “prohibición” que excluye de manera sistemática a algunos grupos invita a considerar otro neologismo post-foucaultiano, el “*banopticon*”, traducido al castellano como “banóptico” (Bigo, 2006). Si bien la mayoría de los ciudadanos del norte global han normalizado a través de su participación en el capitalismo de consumo las formas mencionadas anteriormente, una vigilancia focalizada sigue estando reservada para las personas sin permiso de residencia, los potenciales terroristas, las personas refugiadas y en definitiva aquellas atrapadas en el imperativo de la movilidad. Los policías, militares y otros profesionales combinan sus esfuerzos para convertirse en los nuevos “profesionales de la seguridad”. El banóptico tiene un propósito específico, prohibir la entrada al sistema a ciertas personas, excluirlas.

«Bigo sostiene que hoy día no existe ninguna manifestación centralizada del diseño panóptico y que sí existe el *dispositif* de modo fragmentado y heterogéneo» (Bauman y Lyon, 2013, p. 70). El Estado y otras organizaciones ayudan a fortalecer la informática y los datos biométricos como métodos de vigilancia enfocados en los movimientos de las personas de un país a otro (Bigo, 2006). La normalización de los grupos no excluidos, a través de la creencia en la libre circulación de bienes, capital, información y personas, y la selección, que excluye a ciertos grupos o a categorías enteras de personas por su comportamiento social futuro, son tres elementos que tienen un poder excepcional en las sociedades liberales. Sin embargo, al igual que ocurría en los siglos XVIII y XIX con los métodos de exclusión y disciplina, en nuestra época operan simultáneamente sobre diferentes grupos de población, si bien de manera más imperceptible, unas formas de ordenación social que a la vez que limitan la entrada de ciertas poblaciones a ciertos privilegios, ofrece alternativas mercantiles para ellos que no hacen sino aumentar la brecha entre ambos grupos.

9 El término que introduce Bigo proviene de la combinación en inglés de panóptico con la palabra “ban” que podemos traducir como prohibir o excluir.

Buena prueba de ello la encontramos en el trabajo de Cathy O'Neill (2016/2017) sobre lo que ella denomina las “armas de destrucción matemática” y cómo el *big data* hace aumentar la desigualdad y amenaza a la democracia. Para esta autora, el uso indiscriminado de algoritmos para la toma de decisiones en los métodos de selección de diferentes áreas, en detrimento de la acción humana, en lugar de producir una mayor equidad, está reforzando la discriminación. Ello es debido a que se trata de modelos matemáticos opacos, no regulados ni contrastados y, en la mayoría de las ocasiones, entrenados con datos sesgados. Lo que provoca que en el caso de EEUU que estudia la autora, por ejemplo, el estudiantado de origen humilde no pueda obtener los préstamos necesarios para sus estudios porque el modelo matemático utilizado lo considere demasiado arriesgado, basándose en un dato aparentemente ubicuo como puede ser su código postal. En contraste, este mismo perfil será objeto de asedio de programas de estudios privados que, según otros sistemas de selección opacos, cuentan con un menor prestigio, lo que no hace sino aumentar la distancia en la oportunidad de acceder a una mejor educación. Lo mismo ocurre en otros entornos como el de la salud, los préstamos o incluso la justicia.

La digitalización de la información

La idea de Lewis Mumford (1934/1998) de que a cada civilización le corresponde un medio fue desarrollada por otros teóricos a partir de los años cincuenta. De esta manera, uno de los autores que intentó demostrar cómo la tecnología de la comunicación podía determinar las formas de poder y dominio imperial fue Harold Innis (1950, 1951). Para él, los distintos vectores de comunicación se distinguen en función de su conexión con el tiempo (aquí enmarcaríamos la tradición oral y el manuscrito) o con el espacio (más propias de la tradición mecanizada, representada por la comunicación electrónica y la imprenta). Por tanto, cada una de estas tendencias tiene una configuración social específica. La memoria, el sentido de la historia, las diferentes comunidades y asambleas y las formas dialógicas de poder son descentralizadas y a su vez características de la primera. Y por otro lado, la tradición mecanizada es centralizadora, ya que permite controlar el dominio y la expansión del territorio.

Muy influenciado por el trabajo de Innis, destaca Marshall McLuhan, con su famosa cita «el medio es el mensaje» (1964/1996), donde resume la importancia de la tecnología de la comunicación en la formación de las civilizaciones. De manera similar al anterior, divide la historia de la humanidad en tres etapas: la primera es la época de la comunicación natural, oral y gestual, que interpela a todos los sentidos; la época del pensamiento mágico y del tribalismo; la segunda es la época de la tiranía de la

visión, iniciada por la escritura y la imprenta; la época del racionalismo abstracto y del nacionalismo; y la última es la época de la transmisión electrónica, que «consagra el retorno de todo el teclado sensorial, edad de un nuevo tribalismo, en este caso planetario» (Mattelart, 2001/2007, p. 78). McLuhan se opone de esta manera a la dicotomía significante/significado promulgada por el análisis estructural, al centrarse mayoritariamente en el texto, dado que defiende que el contenido del mensaje es indisoluble de la forma en que se reviste, pues dicha forma terminará acaparando el proceso de comunicación frente al contenido. Esta visión de la comunicación tuvo importantes implicaciones en las décadas posteriores.

Enfocándonos ahora más en el almacenamiento de dicha información en lugar de en su expansión, encontramos la teoría de las diferentes tecnologías de la memoria de André Leroi-Gourhan, el cual en 1964 publicó en dos volúmenes la obra *El gesto y la palabra*. En el primer tomo hablaba de la técnica y del lenguaje, y en el segundo, de la memoria y de los ritmos. Este autor describía la historia de la memoria colectiva, desde la literatura oral hasta las fichas perforadas y la memoria electrónica, y cómo los seres humanos hemos ido delegando en diferentes tipos de artefactos nuestras capacidades de registro, exteriorizando cada vez más nuestra memoria. Dicha historia de la memoria colectiva queda dividida en diferentes períodos: la transmisión oral, la transmisión escrita a través de tablas e índices, la mecanografiada y la electrónica.

Para Leroi-Gourhan, el triángulo en el que gira la historia de la organización de la memoria colectiva y la exteriorización de los órganos de la tecnicidad se compone, desde los inicios de la hominización, de la mano, el lenguaje y el córtex sensoriomotor:

La herramienta, realmente, sólo está en el “gesto que la hace eficaz” y la sinergia operatoria entre una y otro supone la existencia de una memoria en la que se inscribe el programa del comportamiento. La realización de programas automáticos es un hecho culminante en la historia humana, similar en importancia a la aparición del hacha-martillo manual o de la agricultura. Esta paciente evolución de las herramientas-gestos-memoria constituye la aventura humana de la planetización (Leroi-Gourhan, 1964, citado en Mattelart, 2001/2007, p. 80).

Como hemos ido viendo a lo largo de estas páginas, el desarrollo de la tecnología ha permitido un perfeccionamiento de la vigilancia, desde los registros antiguos en tablillas al uso de las tarjetas perforadas y la mecanografía, de nuevo veremos con la expansión de la escritura digital un salto en su desarrollo. No en vano, dicha digitalización se ha instalado con tanta profundidad en nuestra sociedad

que actualmente la concebimos como «sociedades de la información», es decir, nos entendemos como «información» (López-Gabrielidis, 2020, p. 62). Dentro de esta concepción “cibernética” de la humanidad, la memoria externalizada queda cada vez más organizada, de maneras mejor estructuradas y conectadas. Sobre esto, Morozov (2024, p. 27) apunta a que:

En este contexto la interdisciplinariedad dejó de estar a la orden del día. La IA estaba dominada por jóvenes y brillantes matemáticos o informáticos a los que la cibernética les parecía demasiado abstracta, demasiado filosófica y, ante todo, potencialmente subversiva. También hay que decir que, en el ínterin, Norbert Wiener había empezado a respaldar la lucha sindical y a criticar al ejército, lo que no sirvió precisamente para atraer la financiación del Pentágono.

Desde los años 60 en adelante, el objetivo de la cibernética fue transformar todo lo que fuese factible en datos, conectar y hacer interactuar las memorias externalizada y los cuerpos, así como las memorias digitalizadas entre sí. De esta manera, el mundo comenzó a ser asimilado a través de las tecnologías digitales. Sin embargo, dado que estamos hablando de un tiempo enmarcado dentro del período de enfrentamiento entre los bloques capitalista y comunista, los primeros desarrollos de la cibernética se enmarcaron dentro de la carrera armamentística y del territorio de la defensa nacional. Por ello, los primeros objetos de digitalización fueron máquinas tales como armas, satélites o misiles, ya que lo primordial de aquel tiempo era «abstraer a un lenguaje binario capaz de hacer entrar esa información en las redes de telecomunicaciones, datos relativos a las propias máquinas de guerra y a las propias máquinas informáticas que gestionan esos datos» (López-Gabrielidis, 2020, p. 66).

La dimensión supuestamente inmaterial del mundo digital resulta predominante en estos discursos sobre la digitalización. Ello es debido a que se fundamentan en una naturaleza matemática que, como el propio lenguaje matemático de base, interpretamos como exacta y abstracta. De este modo, aunque reconocemos que sus resultados pueden aplicarse a entidades materiales, entendemos que en su mayor parte se ocupan de entidades inmateriales.

Ese culto al número como forma de entender la sociedad sigue muy presente entre los teóricos sociales de este tiempo. Así, ya en 1949, Claude Elwood Shannon formuló una teoría matemática de la comunicación, en la que entendía la información únicamente desde el punto de vista físico, cuantitativo y estadístico. Esta forma mecanicista de entender la información solo se interesa por cómo fluye la misma, creando una separación entre la noción de comunicación y la de cultura, y es que este concepto de tipo estímulo-respuesta de la sociedad se complementaba con la idea anteriormente mencionada del

flujo de información del centro hacia las periferias de Innis.

La forma en cómo se puede medir la información resultará un debate clave en este «advenimiento de la “sociedad de la información”» (Mattelart, 2001/2007, p. 70). De esta manera, en relación a la definición y la medición de la “economía de la información”, Marc Uri Porat (1977) se centró en los sistemas de dicha información, esto es, los ordenadores y las telecomunicaciones, concluyendo en una definición de información como cantidades de datos que han sido organizados y comunicados. Esta tendencia se enfatizará hasta culminar en la idea de entender que no existe información si no hay un dispositivo técnico detrás, y en su asimilación a un término que proviene de la estadística: los datos. De esta manera se estableció una noción únicamente instrumental de esta sociedad de la información.

Todo ello ha colaborado a que se entienda en gran medida la información digital como un ente inmaterial. Pero lo que subyace a esta creencia es un pensamiento estático y dualista operado sobre una «ontología hilemórfica que separa materia y forma, un concepto de información con lastres cartesianos donde la forma (activa y agencial) informa unidireccionalmente la materia (pasiva)» (López-Gabrielidis, 2020, p. 154).

El discurso detrás de la digitalización se ha basado en la fe en el progreso técnico y en la posibilidad de generar duplicados inmateriales, perdurables e inmutables de aquellos objetos y cuerpos pesados y perecederos. Aunque ya hemos visto que esto es solo una ilusión, resulta una idea de tal profundidad que ha calado notoriamente en la sociedad actual. Y es que uno de los principales problemas para entender la dimensión material de la información digital está vinculado al hecho de que dicha información existe a unas escalas simultáneas tan dispares que resulta complicado concebirlas en términos materiales, ya que la información se difunde en intervalos muy cortos de tiempo a grandes distancias a través de los cables subterráneos, como ocurre a través de Internet.

El papel de la vigilancia en la concepción de Internet

La existencia de la vigilancia en Internet es algo que tenemos actualmente bastante asumido, aunque muchos de nosotros no entendimos su magnitud hasta las revelaciones de Snowden de 2013. Este hecho supuso un revés a la ola inicial de optimismo sobre el potencial democrático con el que se entendía Internet (Lyon, 2015, p. 53). Aunque no es mi intención en este epígrafe desarrollar la evolución de Internet desde su origen hasta la actualidad, considero conveniente entender correctamente el papel que ha jugado la vigilancia dentro de su concepción.

Para ello debemos remontarnos de nuevo al transcurso de la Segunda Guerra Mundial, donde se

produjo un gran despliegue de recursos científicos, como por ejemplo los desarrollados por el matemático británico, Alan Turing, cuyo aparato según Mattelart (2001/2007, p. 59), representaba la noción de “máquina universal”, ya que era comparable al de un sistema operativo fundamental, al tener la capacidad de realizar cualquier instrucción computable sobre ella. Se inicia aquí, según este autor, el camino hacia la creación de un “cerebro electrónico”, en sintonía con el descubrimiento de cómo funcionaba el cerebro humano (Mattelart, 2001/2007, p. 59). Las tablas de tiro para el uso de la artillería antiaérea, la bomba atómica y el descifrado de la correspondencia estratégica del enemigo son las tres áreas que contribuyen al avance de las grandes máquinas calculadoras durante este tiempo.

En el caso estadounidense, para Foster y McChesney (2014, párr. 3), tanto en la industria como en el gobierno, en la época posterior a la Segunda Guerra Mundial, se actuó rápidamente para estabilizar un sistema que podía tambalearse después del gran esfuerzo bélico. Esto se llevó a cabo a través del establecimiento de un estado belicista permanente, con sede en el Pentágono y enfocado en el control imperial de los mercados mundiales y en la nueva lucha enmarcada en la Guerra Fría. Durante el primer cuarto de siglo después de la Segunda Guerra Mundial, este «complejo militar-industrial», término acuñado en el discurso de despedida como presidente del ex-general Eisenhower el 17 de enero de 1961, en el cual alertaba que «existe el riesgo de un desastroso desarrollo de un poder usurpador y se mantendrá. No debemos permitir nunca que el peso de esta conjunción ponga en peligro nuestras libertades o los procesos democráticos» (Eisenhower, 1961, párr. 19). Este complejo fue uno de los principales mecanismos para absorber excedentes de la economía estadounidense, además del consumo y la inversión capitalistas.

Sin embargo, décadas antes, concretamente en 1946, el general Eisenhower, cuando ostentaba el cargo de jefe del Estado Mayor del Ejército, publicó un memorando sobre el tema de cómo operar los distintos recursos científicos y tecnológicos como activos militares. En este documento, hizo hincapié en que se estableciera una relación contractual estrecha y continua entre científicos, tecnólogos, la industria y las universidades militares y civiles. «La seguridad futura de la nación exige que todos esos recursos civiles que por conversión o redirección constituyen nuestro principal apoyo en tiempos de emergencia se asocien estrechamente con las actividades del Ejército en tiempos de paz» (citado en Foster y McChesney, 2014, párr. 4). Esto requirió una enorme expansión del sistema de seguridad nacional, incorporando a científicos civiles, industria y contratistas dentro de este brazo creciente y secreto del gobierno.

Este argumento lo comparte Weiss (2014, p. 2) en lo que ella denomina el Estado de Seguridad Nacional (NSS por sus siglas en inglés):

Desde la Segunda Guerra Mundial, el NSS ha dominado en tecnologías de alto riesgo y de vanguardia y en industrias emergentes; esta búsqueda ha establecido, y sigue asegurando, las bases para un sector comercial de alta tecnología. Sin embargo, el NSS busca el liderazgo tecnológico para mantener la primacía político-militar de Estados Unidos, no para lograr una ventaja comercial. Para ello tiene que confiar en el sector privado para avanzar en sus objetivos tecnológicos. [...] Pero a medida que las capacidades de vanguardia fueron residiendo cada vez menos en el grupo de grandes contratistas de defensa (el núcleo de lo que tradicionalmente se describe como el complejo militar-industrial), y cada vez más en empresas de alta tecnología renuentes a trabajar en proyectos relacionados con la seguridad, el NSS se vio obligado a reestructurar su sistema de incentivos. [...] [D]esde los años 1980 el NSS ha tenido que salir cada vez más del grupo tradicional de grandes contratistas para atraer a las empresas más innovadoras, incorporando objetivos comerciales a sus programas. Al poner mayor énfasis en las oportunidades de comercialización, algunos de estos incentivos buscan endulzar la colaboración con el Departamento de Defensa (DoD) y otras agencias relacionadas con la seguridad, y así aumentar la influencia del NSS sobre la dirección de la tecnología. De esta manera, la comercialización se convierte en la condición *sine qua non* de la primacía tecnológica y militar. Lejos de ser mutuamente excluyentes, la seguridad y el comercio se han entrelazado estrechamente en la política y la práctica del NSS.

En 1947 con la aprobación de la Ley de Seguridad Nacional se creó el Consejo de Seguridad Nacional, que también creó la CIA. Juntos, el Consejo de Asesores Económicos y el Consejo de Seguridad Nacional debían construir las bases de dicho estado bélico permanente estadounidense. En esta época, según Mattelart (2001/2007, p. 61), la creencia era que solo a través del desarrollo de la mayor fuerza aérea sería posible manejar la guerra de manera racional y con el menor coste humano, ya que ésta se iba entendiendo cada vez más como una industria. Este concepto de gestión automática del campo de batalla toma forma debido también a un entorno donde la opinión pública se decantaba cada vez más por el pacifismo.

Es en este tiempo cuando los informáticos comienzan a elaborar su propio discurso sobre el control, la comunicación y los sistemas. Según Paul Edwards (1989, citado en Mattelart, 2001/2007, p. 61), se veía el ordenador como un instrumento capaz de «resolver cualquier problema formulado de manera suficientemente precisa, es decir, que puede ser sistematizado, matematizado, modelizado y reducido a

un algoritmo». En el futuro, la incorporación de algoritmos automatizados en los sistemas de armamento será secundada por esta ideología basada en el determinismo técnico.

Años después, el presidente Truman creó la «ultraoscura» (Gearan, 2013) Agencia de Seguridad Nacional (NSA) en 1952 como un brazo del ejército encargado de realizar un monitoreo electrónico clandestino de posibles actividades subversivas extranjeras (y nacionales). Como apuntan (Foster y McChesney, 2014, párr. 32):

Un sistema de dominación militar-imperial y de acumulación de capital como éste crea naturalmente no sólo sus propios enemigos externos, sino también sus “enemigos internos”, que a los ojos de la estructura de poder consisten en todos aquellos que se oponen al capitalismo y al Estado bélico, junto con todas aquellas fuerzas de la sociedad que se consideran potencialmente disruptivas. Así pues, un Estado bélico se convierte naturalmente en un Estado de vigilancia.

Sin embargo, el año que resulta clave para el advenimiento de nuevas tecnologías como Internet es 1957. En este año la Unión Soviética lanzó el primer satélite artificial terrestre, el *Sputnik*, este hito avivó los temores estadounidenses de la Guerra Fría sobre el dominio militar soviético en un nuevo terreno, el espacio. De esta manera, en febrero de 1958, el presidente Eisenhower autorizó la creación de la nueva Agencia de Proyectos de Investigación Avanzada (ARPA por sus siglas en inglés). Esta agencia fijó como objetivo primordial la militarización del espacio, incluidos los satélites de vigilancia global, los de comunicaciones y los sistemas de armas orbitales estratégicas, además de una misión a la Luna (Foster y McChesney, 2014, párr. 26). Sin embargo, tras la creación de la Agencia Nacional de Aeronáutica y del Espacio (NASA por sus siglas en inglés) el 29 de julio de 1958, los programas espaciales civiles fueron desligándose gradualmente de ARPA. Así, en 1959 la mayoría de los programas espaciales militares en ARPA, junto con la mayor parte de sus fondos, también habían desaparecido, por lo que para su supervivencia la reconvirtieron en un:

centro de operaciones en investigaciones básicas [*blue sky*] en tecnologías del Departamento de Defensa, que supervisaba todas las fuerzas armadas. ARPA (rebautizada como Agencia de Proyectos de Investigación Avanzada de Defensa o DARPA en 1972) trabajó en el desarrollo [(en paralelo al MIT y al NPL o *National Physical Laboratory*)] de sistemas de misiles antibalísticos y en *Transit*, el predecesor del Sistema de Posicionamiento Global (GPS). Sin embargo, su labor más destacada en sus primeros años estuvo relacionada con el desarrollo de la tecnología de comunicaciones digitales por conmutación de paquetes [...]

que dio origen a la Internet original y a la red de satélites de paquetes (Foster y McChesney, 2014, párr. 26).

De hecho antes de su rebautización, en 1961 la organización ya se había convertido en una fuerza importante en la investigación informática, estableciendo desde ese momento fuertes relaciones contractuales con destacados científicos informáticos de las universidades de todo el país y se introdujo una cultura interna que se centraba en la idea de la interconexión, basada en ordenadores interconectados. De este modo, a lo largo de la década de 1960, ARPA se convirtió en el centro de trabajo sobre redes informáticas, lo que dio como resultado el 21 de noviembre de 1969, a la red Arpanet, la predecesora de Internet, nacida con el objetivo de facilitar el intercambio de información entre los distintos equipos contratados.

Según Foster y McChesney, (2014, párr. 26), en la década de 1980, DARPA se concentró en la promoción de la iniciativa *Star Wars* de la administración Reagan. Y posteriormente, en la década de 1990 y principios del 2000, se dedicó a desarrollar tecnologías de vigilancia digital en estrecha alianza con la NSA, junto con la tecnología de drones militares.

Otro hecho muy importante que destacan estos autores, (Foster y McChesney, 2014, párr. 32-37) sobre Arpanet es que, debido al aumento de las protestas sociales a finales de los años cincuenta y sesenta, primero por los derechos civiles y después por el movimiento contra la guerra de Vietnam entre otras causas, se produjo un aumento masivo de la vigilancia militar y policial de la población estadounidense. En los años 1970 y 1971 surgió el escándalo de los “Archivos del Ejército” (CONUS en inglés), cuando se reveló que el ejército estadounidense había estado espionando y guardando expedientes sobre más de siete millones de ciudadanos estadounidenses. Si bien dichos expedientes se guardaban originalmente en la Biblioteca de Registros de Investigación de Fort Holabird en Maryland, más tarde, gracias a las investigaciones del Congreso, se descubrió que a pesar de que se había dicho que habían sido destruidos, realmente estos datos habían sido transmitidos —más de dos años después de que se ordenara la destrucción de este material— a la NSA a través de Arpanet. Por lo que, para muchos estadounidenses, esta fue la primera noticia de que existía algo como Arpanet (Foster y McChesney, 2014, párr. 35).

Debido a estas revelaciones, el senador Sam Ervin, conocido por su papel como presidente del Comité del Senado estadounidense sobre el caso *Watergate*, pronunció un discurso en el MIT en abril de 1975 en el que declaró que el peligro para la privacidad se había acelerado debido a la presencia de ordenadores que permitían «el almacenamiento ilimitado de datos y su recuperación a la velocidad del rayo» (citado en Foster y McChesney, 2014, párr. 36).

De hecho el año 1975 fue el llamado “*Year of the Intelligence*”, un período que se extendió hasta abril de 1976 en el que se revelaron ante el mundo los secretos más oscuros de varias agencias de espionaje de EEUU. Las principales revelaciones procedieron de la comisión de investigación del Senado conocida popularmente como el Comité Church, en honor a su presidente, el senador Frank Church de Idaho (Townley, 2021), la cual puso la lupa sobre los abusos de la CIA, el FBI y la NSA. De hecho, esta última era prácticamente desconocida para el público por entonces, hasta el punto de que se aludía a ella como “*No Such Agency*” (Gearan, 2013). Los hallazgos de este comité se han condensado a menudo en la célebre frase que el propio Church (1975, 1m25s) pronunció en una entrevista televisiva en la NBC (y de la que Greenwald tomó el título de su libro sobre Snowden *No Place to Hide*):

Al mismo tiempo, esa capacidad podría volverse contra el pueblo estadounidense en cualquier momento, y no quedaría privacidad alguna para ningún estadounidense: tal es la capacidad de monitorizar todo —conversaciones telefónicas, telegramas, lo que sea. No habría ningún lugar donde esconderse.

Al margen de este hecho, debemos saber que al principio Arpanet estaba conectada únicamente a los departamentos de informática de aquellas universidades que contaban con financiación del Departamento de Defensa y con las autorizaciones de seguridad correspondientes. Con el éxito del sistema, otros departamentos de informática universitarios y la industria privada también querían conectarse a esta red. Esto dio lugar a la creación de la Red de Investigación en Ciencias de la Computación (CSNET por sus siglas en inglés) y de la Red de la Fundación Nacional de la Ciencia (NSFNET por sus siglas en inglés), desarrollada por el gobierno de EEUU para reemplazar Arpanet como base de Internet (Foster y McChesney, 2014, párr. 56).

La alternativa a ella sería construida como una serie de redes dedicadas a la comunicación educativa y de investigación a través de la combinación de Arpanet, un sistema denominado Telenet y PhoneNet, para el correo electrónico. En 1985, la Fundación Nacional de la Ciencia (NSF, por sus siglas en inglés) construyó cinco superordenadores en todo el país para que fueran la columna vertebral de una NSFNET más grande, que reunió a las universidades en general y a las corporaciones privadas. Ello trajo aparejada la fusión en una Internet mucho más amplia con un protocolo común, lo que dio lugar a un crecimiento masivo de usuarios que podían acceder a ella a través de ordenadores personales, gracias a los proveedores de servicios de la naciente Internet surgida el 1 de enero de 1983.

A partir de los años ochenta, en el norte global, los ordenadores personales se fueron distribuyendo ampliamente, y en los años noventa su conexión a través de Internet se hizo realidad, especialmente

después de la invención de la World Wide Web en 1994. Este hito generó muchas industrias basadas en la *web* y también el auge y caída de las “punto.com” de finales de siglo XX. Finalmente, en 1995, NSFNET fue privatizada y desmantelada, quedando la columna vertebral del sistema bajo el control de proveedores privados de servicios de Internet (McChesney, 2013, pp. 102-104).

Paralelamente, otros muchos dispositivos digitales estaban tomando forma; cámaras digitales, teléfonos móviles y videoconsolas, los cuales muy pronto también serían vinculables entre sí a través de Internet. Durante la primera década de los 2000 aparecieron tanto el ya mencionado en el apartado 1.1.1., concepto de la *nube*, como el contenido generado por los usuarios en las plataformas de redes sociales, y en la década de 2010 la computación ubicua y generalizada se hizo más evidente (Kitchin, 2014b). En torno a cada dispositivo y, a menudo, en torno a todo el conjunto de funciones de intercambio de fotografías, video, audio y texto, surgieron nuevas culturas digitales y formas de consumo.

Pero los aparentes éxitos de las empresas afincadas en Silicon Valley que desarrollaban todas estas tecnologías no siempre fueron tan fructíferos. Por ejemplo, las empresas basadas en la *web* que sobrevivieron a las desastrosas crisis de finales de los años noventa todavía estaban buscando un futuro más sólido. De hecho, muchas lo encontraron después del 11 de septiembre de 2001, cuando ofrecieron sus servicios en la causa antiterrorista (Lyon, 2003a). Por lo tanto, no resultó tan sorprendente cuando diez años después de este hecho, se demostró que el Departamento de Seguridad Nacional estadounidense (DHS, por sus siglas en inglés) estaba revisando publicaciones en redes sociales y comunicaciones por correo electrónico en busca de posibles sospechosos de terrorismo, utilizando numerosas palabras clave. Después del 11-S, fue principalmente el DHS el que se encontró en el punto de mira y no fue hasta la filtración de documentos de Snowden que la atención no viró de nuevo hacia la NSA.

Volviendo a las concepciones sobre los inicios de Internet debo destacar que, a menudo, los aficionados de estos primeros tiempos, se referían a él con el término “ciberespacio”, el cual resulta muy revelador. El concepto fue acuñado por William Gibson en el relato *Johnny Mnemonic*, publicado en la revista *OMNI* en 1981, y tiene su origen en la ya citada cibernética de los años 50, que era el estudio de los sistemas reguladores y los bucles de retroalimentación en las comunicaciones. El concepto, tal como lo concibió Norbert Wiener (1948), se centraba en el estudio del control en los sistemas de comunicación y tiene su origen en la palabra griega *kubernetes*, que significa “timonel” o, de forma más general, “gobernador” (Lyon, 2015, p. 51). La cibernética se utilizaba en muchos contextos, pero en especial en relación con los sistemas informáticos, y siempre con el objetivo de mejorar una organización y gestión eficaz. Esto resultaba muy oportuno en el caso del uso del término

“ciberespacio” en el contexto del control sobre Internet.

La historia se encuentra ligada inextricablemente de nuevo a la Guerra Fría y a las trayectorias eventualmente contrastantes de la cibernética soviética y estadounidense (Edwards, 1996). El propio Wiener se preocupaba por las posibles consecuencias para las distintas sociedades de la cibernética y las “máquinas automáticas”, viendo en ellas tanto «amenazas como promesas» (Wiener, 1953/1985, pp. 673-678). De hecho este autor ya había publicado en 1947 un artículo, titulado *A Scientist Rebels*, donde no se granjeaba muchos amigos, especialmente en el Pentágono, al detallar todos esos peligros de forma bastante pionera. También fue incisivo acerca de la capacidad de la “mano invisible” del mercado capitalista estadounidense en lograr mejores condiciones para todas las personas: «Opuesto a la idea del afán de lucro como filtro para el control de la información, Wiener se revolvería en su tumba al ver cómo las empresas gigantes de hoy, como Google, poseen los datos que la NSA quiere» (Lyon, 2015, p. 52).

Y es que, en la actualidad, muchos de los dispositivos digitales más populares se caracterizan por su capacidad de registrar su propio uso. Esto ciertamente permite su uso cibernético al proporcionar circuitos de retroalimentación que ayudan a empresas como Amazon a realizar una aproximación mediada por algoritmos de qué productos es probable que nos interesen, pero también otorga una dimensión de vigilancia a cada dispositivo en el que se usa. Esto se debe a que las mismas funciones útiles que pueden, por ejemplo, guiarte a través de una parte desconocida de la ciudad también pueden “informar” de forma sencilla sobre tu paradero a las agencias policiales o de inteligencia que deseen rastrearlo.

De la Digitalización a la Datificación

A finales de la década de 1980, la vigilancia se teorizaba en Europa y América del Norte en relación con el Estado, el lugar de trabajo, la policía y también en el ámbito del consumidor, este último gracias al rápido crecimiento del *marketing* directo (Larson, 1994). En cada uno de estos campos, diversos teóricos centraron su interés en cómo las nuevas tecnologías informáticas y de comunicación mejorarían las capacidades de vigilancia. Recordemos cómo el sociólogo Gary T. Marx (1998), por ejemplo, destacaba lo que denominó la “nueva vigilancia” en la policía, profundamente influida por tecnologías. En su momento, esta nueva modalidad de control sonaba a las representaciones de ciencia ficción, como en el relato corto *The watch-towers* de J. G. Ballard, pasando por *A Scanner Darkly* [Una mirada a la oscuridad] de Philip K. Dick, hasta *Fahrenheit 451* de Ray Bradbury (citados en Lyon, 2015, p. 27).

Para Marx, del mismo modo que ocurrió con el descubrimiento del átomo o del inconsciente, las

nuevas técnicas de control «sacaron a la luz fragmentos de realidad que antes bien quedaban ocultos» (Marx, 1998, p. 207) o bien no contenían relevancia informativa. Para él, en cierto sentido, las personas se volvieron del revés y lo que antes era invisible o carente de significado se hizo visible y significativo (Marx, 1998, p. 207). Este autor también alertó sobre los diferentes métodos que se estaban utilizando para recopilar datos personales, tales como sensores de audio, vídeo, luz o calor, o cómo en relación con un perfil predictivo basado en datos agregados, se le daban diferentes significados a la conducta de un individuo. Sus preocupaciones sobre el uso del “ordenador como informante” también se extendieron a otros contextos. A medida que los gobiernos, las empresas y los lugares de trabajo se automatizaban cada vez más, controlar y rastrear a las personas a menudo significaba instalar dispositivos como cámaras de vídeo o usar los propios ordenadores como una forma de seguir el rastro de los ciudadanos, ahora también en su rol de empleados y/o consumidores.

Dentro de este nuevo entorno tecnológico se deben considerar, por tanto, las dimensiones maquínicas (término que retomaré en el apartado 2.3.3.) en la producción de la subjetividad. Para el psicoanalista Félix Guattari, ello implica que las diferentes máquinas tecnológicas de información y comunicación, entendidas desde la robótica hasta la informática, funcionarían en el centro de la subjetividad humana, no solo en sus memorias e inteligencia, sino también en su sensibilidad, afecciones e inconsciente. Al rechazar la ideología de la posmodernidad como «paradigma de todos los sometimientos y compromisos con el *status quo* existente», Guattari promueve una reapropiación y una resingularización de la utilización de las máquinas de comunicar desde una perspectiva de experimentación social: «constitución de complejos de subjetivación: individuo-grupo-máquina-intercambios-múltiples» (citado en Mattelart y Mattelart, 1995/2005, pp. 126-127).

En contraste, Paul Virilio (1990/1999) discrepa de la existencia de una teoría de la tecnología, y apunta hacia la aceleración de los cambios que ésta experimenta como aspecto digno de estudio. Es en este momento donde la invalidez, es decir, la incapacidad de moverse para actuar y la desventaja que ello supone, se convierten en el símbolo del progreso y del dominio del medio. La otra faceta de la búsqueda de la ubicuidad, la instantaneidad y la hiperpercepción la encontramos a través del confinamiento doméstico, gracias al complejo de pantallas que permite hacerlo todo en casa. El sentido de la duración, el movimiento del cuerpo y la vida social se pierden, y es a través de esta falta de tiempo para compartir con los demás, donde se pierden las capacidades democráticas de la sociedad.

Para Marc Augé (1992/1993), antropólogo de la “sobremodernidad”¹⁰, la rápida circulación de las

¹⁰ Marc Augé (2007) propone la “sobremodernidad” para reemplazar la “modernidad”, no por desaprobación, sino por exceso. Para ello, su pensamiento se enfoca en tres movimientos complementarios (tiempo, espacio e imagen) que, aunque son diferentes, favorecen ciertos puntos de vista: el primero pone énfasis en el tiempo; mientras que el segundo

personas y de los objetos ha creado “no-lugares”, esto es, espacios transitorios en los que solo se puede expresar una identidad anónima y funcional, como podrían ser los aeropuertos o los grandes centros comerciales. En esta línea, Sebastián Roché (1996, p. 11) alude a que, dentro de las sociedades postindustriales, los métodos tradicionales que garantizaban la vigilancia social y la solidaridad cercana ya no funcionan. Para este autor, estos mecanismos sociales para aprender sobre respeto mutuo y control de uno mismo se han desmoronado. «Es en este contexto que va a nacer y, después —para suplir la carencia de disciplinas y de *panoptismos*—, se desarrollará un nuevo control realizado gracias a las técnicas informáticas» (Mattelart y Vitalis, 2011/2015, p. 192).

De esta manera, fruto de las intervenciones del Estado y del desarrollo de una economía de mercado, cada persona se encuentra actualmente en varios ficheros. Todo ello sin que el individuo tenga conocimiento de los procedimientos ni de las manipulaciones realizadas a sus espaldas. Y a partir de ahí se toman decisiones sobre él con una serie de normas como referencia y sin que la ciudadanía pueda intervenir porque las tecnologías de control resultan invisibles (Mattelart y Vitalis, 2011/2015, p. 192). Si bien la idea de comunicación y de transparencia ha acompañado la creencia ilustrada del progreso social y la emancipación de los individuos, hoy en día resulta sospechosa. Para Baudrillard (1990/1991), la comunicación ha sufrido un exceso de la misma, lo que ha llevado a la implosión del sentido, la pérdida de lo real y el reino de los simulacros. Este autor detecta el avance de un sistema de control que se exalta en nuestro “fantasma de comunicación”: la compulsión general a estar presente en todas las pantallas y en el centro de todos los programas, tanto en las escaladas tecnológicas como en la intimidad doméstica, dejando sin respuesta la pregunta antropológica: «¿Soy un ser humano o soy una máquina?» (p. 30).

La respuesta a esta pregunta se vuelve en nuestros días cada vez más compleja. Ello es debido a la evolución de la digitalización, hacia el concepto de datificación del nuevo milenio, centrada en la conversión y tecnificación del cuerpo individual. Este concepto surge en un momento en el que el mundo digital va captando información cada vez más íntima y personal, es decir, información relacionada con el cuerpo y la existencia única, así como con las circunstancias y personas que nos rodean, y las acciones que realizamos.

La datificación, según Mayer-Schoenberger y Cukier (2013) significa la transformación de la acción social en datos cuantificados en línea, que permiten el seguimiento en tiempo real y el análisis

pone énfasis en el espacio, analizando el cambio de los “lugares” a los “no-lugares”. Por último, el tercero enfatiza la imagen y analiza la transición entre lo real y lo virtual. Para él, nuestra realidad ha sido definida por el tiempo y el espacio. Pero ha surgido un híbrido entre ambos, la imagen, que puede suplantarlos y, por lo tanto, crear una realidad paralela.

predictivo de los mismos. La datificación como medio legítimo para acceder, comprender y monitorear el comportamiento de las personas se ha convertido en un principio rector, no sólo entre los tecnóadeptos, sino también entre los académicos, que la ven como una oportunidad revolucionaria para investigar la conducta humana (van Dijck, 2014, p. 198).

Este concepto contiene una base ontológica que esta autora (van Dijck, 2014) sitúa en el “dataísmo”, o lo que es lo mismo, el culto al dato. Según esta visión, la confianza es depositada en la objetividad de los métodos cuantitativos, así como en la independencia e integridad de las instituciones que los implementan, ya sean plataformas corporativas, agencias gubernamentales o investigadores académicos. Sin embargo, la confianza y la independencia son nociones controvertidas en un ecosistema de conectividad donde todas las plataformas en línea están inevitablemente interconectadas, tanto a nivel de infraestructura como de lógica operativa (van Dijck, 2013; van Dijck y Poell, 2013).

La aparición de los dispositivos móviles y los *smartphones* marca otro cambio significativo, ya que con ellos se termina de implementar en nuestras vidas lo que Marx Weiser (1993) denominó «informática ubicua». Según él, era necesario realizar un cambio radical en la estructura de los ordenadores de sobremesa, dejando de depender del cableado y conseguir esparcirse por el espacio físico de manera que los dispositivos se volvieran omnipresentes e “invisibles” para el usuario. Con los *smartphones* la informática ubicua se extiende, y no debido a una naturaleza inmaterial o volátil, sino porque se comienza a utilizar nuestra propia materialidad corporal. En otras palabras, los teléfonos inteligentes, con su gran cantidad de sensores y su acceso a un Internet móvil, están conectados a nuestros movimientos y hacen que nuestra relación con el objeto digital, además de personal, sea «protésica» (López-Gabrielidis, 2020, p. 77). Cada rincón y cada momento asociado a un cuerpo específico es susceptible de ser datificado desde la llegada de los móviles.

Junto a ellos, los accesorios y aplicaciones de *self-tracking* fomentan también una datificación subjetiva como parte de una filosofía de vida sana y autónoma, al proporcionarnos herramientas para el autocontrol y el rastreo. Estos accesorios, que pueden monitorear el ritmo cardíaco, la cantidad de pasos dados y kilómetros recorridos, la calidad del sueño, los productos y calorías consumidos, etc., convierten al cuerpo en un proyecto que debe diseñarse, supervisarse y mejorarse en detrimento de la experiencia del aquí y ahora. Nos alientan a utilizar de manera personal la lógica de la optimización, reservada anteriormente al ámbito industrial, algo a lo que ya aludía Foucault (2004/2009), en su Curso del Collège de France titulado *Nacimiento de la biopolítica*, al analizar la subjetividad neoliberal y el fomento de «un *homo aeconomicus* empresario de sí mismo, que es su propio capital, su propio productor, la fuente de sus ingresos» (p. 265).

La transición de la digitalización a la datificación supone un cambio subjetivo en la forma en que se generan los datos. El proceso de datificación busca comprender los sentimientos, pensamientos, gustos, y ubicaciones de los cuerpos. Sin embargo, la datificación no anula la producción de información general; en cambio, agrega una nueva capa de información personal e íntima. La datificación es, por tanto, el resultado del perfeccionamiento y refinamiento de la capacidad perceptiva y devoradora del mundo digital, un estadio en el que se logra mejorar la diferenciación técnica del sujeto. A través de este proceso, para socializar en el mundo digital resulta necesario “convertirse en dato”, es decir, la comunicación ya no se origina en nuestros cuerpos, sino en una interpretación desmembrada de los mismos. A través de esta proyección subjetiva y abstracta en forma de información, introducimos nuestra presencia en los entornos digitales, lo que nos permite aparecer frente a los demás y frente a nosotros mismos bajo una nueva perspectiva, una que conlleva una distancia con nuestro cuerpo. Aunque, ello no implica una liberación o autonomía de sus ejes espacio-temporales, ni de sus entornos físicos y ritmos orgánicos.

De esta manera, en la subjetividad actual se observa una conexión entre componentes orgánicos e inorgánicos, así como entre «*data* y *soma*» (López-Gabrielidis, 2020, p. 78). Una especie de desdoblamiento digital resulta de la datificación como fenómeno sociotécnico dentro de esta transformación del sujeto en datos. Sin importar si generamos de forma voluntaria o no dichos datos y metadatos referidos a nosotros mismos, nuestro “yo-datificado” crece continuamente, alimentando fuentes de información personal para diferentes usos.

Abrazando al Gran Hermano

Si a uno le preguntan por libros relacionados con la vigilancia, muy probablemente el primer texto que le venga a la mente sea *1984* de George Orwell. Publicado en 1949 como una obra distópica, es decir, una descripción literaria de un estado futuro indeseable, evitable pero concebible de la sociedad. Su protagonista, Winston Smith, a pesar de intentar pensar por sí mismo, termina siendo aplastado por el Estado de vigilancia. Los medios electrónicos, limitados a lo que Orwell conocía en 1948, son la principal herramienta que manipula a las masas mediante una incesante propaganda. Pero estas formas de vigilancia electrónica también permiten a la Policía del Pensamiento mantener un control constante sobre las vidas y relaciones íntimas de cada ciudadano. La figura del Gran Hermano, que aparece en las tele-pantallas de los edificios públicos y privados, afirma controlarlo todo. De aquí proviene la famosa frase “¡El Gran Hermano te vigila!”.

A menudo se considera que *1984* trata sobre el poder de la tecnología para el control social y sobre la

pérdida de privacidad que resulta al vivir en una sociedad totalmente transparente. Por eso no sorprende que su obra haya sido tan fácilmente trasladable al lenguaje de la tecnología de la información, incluidas sus supuestas amenazas. Orwell fue muy clarividente en muchos aspectos, por ello su obra resulta muy influyente todavía en nuestros tiempos, y en multitud de ocasiones aludimos a ella como referencia en diferentes situaciones de vulneración de la privacidad. Resulta anecdótico señalar, como hace Marta Peirano (2019, p. 223), que el día que Donald Trump se convirtió en presidente de los Estados Unidos en 2017, el libro más vendido en Amazon era, efectivamente, *1984*. Y es que su autor se dio cuenta de la creciente centralidad de la información en las operaciones del Estado nación. En *Oceanía* había incluso un “Ministerio de la Verdad” para tratar asuntos como la creación y destrucción de información. Hoy la tecnología informática facilita la construcción de nuevas categorías de datos, un proceso que se ve alentado por la tendencia al análisis estadístico dentro de las organizaciones. Este enfoque en nuevas técnicas para manejar la información también resuena en el contexto de la informática y la administración. Como hemos visto, es la tecnología de la información la que es especialmente significativa para la vigilancia.

Otra característica significativa de la vigilancia del Gran Hermano de Orwell es que era en muchas ocasiones imperceptible. Los vigilados no estaban seguros de si había algún momento en el que pudieran relajarse. Al igual que en el panóptico, y en otros tratamientos literarios del tema de la vigilancia, como *El castillo* (1926) de Franz Kafka o *El cuento de la criada* (1985) de Margaret Atwood, este modelo de control mantiene a los vigilados subordinados por medio de la incertidumbre. Uno simplemente obedece porque nunca sabe cuándo “ellos” pueden estar observando. Por otro lado, Orwell muestra también cómo el poder se mantiene a un nivel más amplio a través del carácter divisivo de la vigilancia (Cohen, 1991, pp. 142-202). La clase media y los miembros del Partido necesitaban un control cuidadoso del pensamiento. Pero los *proles*, que formaban el 85% de la población, quedaban exentos de este control al quedar confinados en sus guetos, pues al fin y al cabo su suerte era la exclusión.

Sin embargo, algunas cosas han cambiado desde la época de Orwell, y el consumo de masas ha surgido como la nueva realidad globalizadora. Cualquiera que desee comprender la naturaleza de la vigilancia contemporánea debe tener en cuenta este hecho. Mientras que para Orwell la principal amenaza provenía del Estado, hoy la vigilancia del consumidor plantea una serie de cuestiones nuevas. Una visión perfectamente plausible es que en las condiciones contemporáneas el consumismo actúa por sí mismo como un medio significativo para mantener el orden social, pues a diferencia de los personajes de Orwell, a nosotros nadie nos obliga a tener la tele-pantalla encendida, lo que deja que las formas más

antiguas de vigilancia y control se ocupen del considerado «residuo no consumidor» (Lyon, 1994, p. 61).

Si bien el consumismo puede ser visto como un medio de control social, se diferencia en que por ejemplo, aquellos a los que se dirigen diferentes formas de publicidad personalizada, son objetos de un intento de canalización del comportamiento, las empresas desean incluirlos en lugar de excluirlos. Esta es la importante distinción de otras formas de control excluyentes y quizás punitivas, que pueden ser coercitivas, aunque siempre hay que tener en cuenta las tesis de Graeber (2015) sobre nunca subestimar la violencia: «[s]iempre que alguien comienza a hablar del “libre mercado” es buena idea buscar alrededor el tipo con pistola» (Graeber, 2015, p. 35). Orwell tendía a mantener los vínculos, tanto las botas militares como el Gran Hermano tienen su lugar en *Oceanía*. Pero como observa Gary T. Marx (1988, p. 231), los medios más sutiles y menos coercitivos han cobrado cada vez mayor importancia en las sociedades ricas desde la Segunda Guerra Mundial.

Después de todo, la experiencia y las observaciones de Orwell se referían a la guerra civil española, la Unión Soviética de Stalin y la Italia de Mussolini. Muchos han imaginado que este autor sólo tenía en mente estos regímenes evidentemente totalitarios cuando escribió *1984*. Sin embargo, es más que probable que pretendiera que su aplicación fuera más amplia. Como socialista democrático y libertario, era muy consciente de ciertas tendencias autoritarias dentro de las sociedades capitalistas. Lo que tal vez no previese es que las nuevas tecnologías podrían llegar a permitir una vigilancia que tendiera al totalitarismo mientras los procesos democráticos todavía estuvieran perfectamente establecidos. Como señala Gary T. Marx (1988, p. 232): «el guante de terciopelo puede ocultar el puño de hierro».

Sin embargo, a pesar de todo lo que se puede aprender de Orwell, él no podría haber adivinado el papel que jugarían las nuevas tecnologías informáticas, por un lado, y el consumismo, por el otro, en la creación de la vigilancia tal como viene evolucionando desde finales del siglo XX. El punto de inflexión se encuentra en cómo se vive esta vigilancia actual, ya que depende profundamente de la participación de quienes están siendo vigilados. Hemos visto cómo a través del proceso de datificación, no sólo ser observado sino observarse a uno mismo se ha convertido en una forma de vida.

La vigilancia actual es posible gracias a nuestros propios clics en sitios *web*, nuestros mensajes de texto, el intercambio de fotografías y nuestro monitoreo del movimiento del cuerpo. El contenido generado por la persona usuaria engendra los datos mediante los cuales se monitorean las actividades diarias. De hecho, Mathiesen (1997) sostiene que no vivimos simplemente una sociedad de vigilancia sino que ésta se combina con una “sociedad de espectadores” en la que no sólo unos pocos miran a muchos, sino también se trata de una sociedad de medios de comunicación de masas, donde muchos miran a unos

pocos, contraponiendo por tanto, el concepto del sinóptico al panóptico. Cualesquiera que sean los efectos panópticos que puedan encontrarse en la cultura contemporánea, deben considerarse en relación con los sinópticos porque estos últimos ayudan a moldear nuestra experiencia de los primeros, hasta el punto de que para Mathiesen, trabajan juntos.

Sobre la idea de quién mira a quién o por qué hemos ido cediendo ciertos terrenos pertenecientes a la privacidad de cada uno, Lyon (2007, pp. 139-155), teoriza en un momento previo a la llegada de las tecnologías ubicuas, de rastreo y de datificación del cuerpo, sobre otro acontecimiento de finales del siglo XX que provoca ese deseo de ser visto: el lanzamiento en las televisiones de todo el mundo de los *reality shows* y en concreto del programa *Gran Hermano*. Y es que con él se muestran aquí multitud de ironías; como si no fuera suficiente que la temible figura del Gran Hermano se convirtiera en un entretenimiento absorbente y escapista y que la visibilidad se convirtiera en un “viaje” agradable en lugar de una “trampa”, tal y como lo concibió Foucault en su análisis del panóptico, la telerrealidad también invierte la tendencia sobre la noción convencional de la existencia de espacios “privados” inviolables. Así, el interior de baños y dormitorios ahora resultan “públicos” en todo su esplendor banal, mundano y terrenal. Pero la ironía en realidad sólo está al alcance de aquellos que observan con un sentido histórico el cambio radical de las preocupaciones posteriores a la Segunda Guerra Mundial a la nueva parodia posmoderna.

Sobre esto, debemos tener en cuenta el previo estudio de Denzin (1995), el cual sugería que el cine “realista primitivo” de principios del siglo XX fue el que introdujo al *voyeur* en la pantalla de maneras adecuadas al capitalismo más local de la época. El cine modernista mantuvo viva la mirada pero distanciada de la vida cotidiana, aunque el *voyeur* fue parodiado en la época tardomoderna, entre los posmodernos la mirada se reconocía abiertamente y su presencia se encontraba en todas partes, incluso la sala de estar se trata como un lugar común (Denzin 1995, p. 9). Aunque estas palabras fueron escritas antes de que *Gran Hermano* hiciera su debut, su relevancia para ese género es evidente. De hecho, podría decirse que lo es en formas que van más allá de lo que explora Denzin, especialmente en relación con la afinidad posmoderna con la fase multinacional-consumista del capitalismo.

Por su parte, Pecora (2002) ve en estos programas algunos tintes de narcisismo, haciéndose eco de la “orgía de autopromoción capitalista” de Christopher Lasch (1991, citado en Pecora, 2002, p. 354), aunque va más allá de la crítica inicial de este autor, ya que Pecora vincula los deseos de los *reality shows* con los de la “teoría social ilustrada”: una consecuencia de la exigencia de hacer visible lo socialmente oculto, de exponer el funcionamiento secreto de la elección individual y la autoridad grupal y de crear un mundo cada vez más transparente, que filósofos desde Jean-Jacques Rousseau hasta Jürgen

Habermas han presentado como un ideal (Pecora, 2002, p. 355). De esta manera, el autor sugiere que, si bien el deseo de transparencia no necesariamente impulsaría el desarrollo de una mayor vigilancia, el deseo de vigilancia puede tener el efecto secundario paradójico de convertirnos en participantes en tiempo real en un experimento de psicología social en el que somos a la vez sujetos y observadores clínicos. Para Lyon (2007, p. 152), el panóptico de Foucault se encuentra aquí con la hiperrealidad de Baudrillard.

Sobre el programa *Gran Hermano*, McGrath (2004) sostiene que los tipos de deseos de vigilancia expresados y promovidos por este tipo de *reality shows* se volvieron más importantes incluso que las ideologías de control del crimen para justificar la expansión de la vigilancia. Las actuaciones ante la cámara funcionarían como una especie de analogía con la forma en que todo el mundo tiene de aceptar cada vez más el espacio vigilado. Al final, sin embargo, McGrath insiste en que estos lugares son muy diferentes de los peores escenarios que tanto preocupaban a Orwell. Para Lyon (2007, p. 154), si bien la espontaneidad y la imprevisibilidad de las actuaciones espaciales de la vigilancia son un antídoto contra el espectro sobredeterminado de la vigilancia como control, la imbricación de los participantes televisivos (en pantalla o frente a ella) en el mundo del capitalismo multinacional-consumista difícilmente puede resultar irrelevante.

Para Mark Andrejevic (2004), los *reality shows* exaltan la vigilancia, presentándola como algo moderno y atractivo, una forma de ingresar al mundo de la fama y el lujo. Para él, los verdaderos ganadores en estos programas son los especialistas en *marketing* y las corporaciones, que tienen un gran interés en que la vigilancia se venda como algo benigno. Los espectáculos fomentan esta idea, la autorrevelación resulta inocente, incluso cuando el *marketing* de relaciones con el cliente busca nuevas formas de inducir a las personas a revelarse a sí mismas. Lo que pasa por “autoexpresión” en realidad se reinterpreta como un tipo de trabajo en el que los consumidores son reclutados involuntariamente para “ser observados” de maneras que benefician principalmente a quienes los “observan”.

Este tipo de programas basados en la telerrealidad donde personas anónimas exponían sus rutinas frente a las cámaras dio paso a otros formatos similares entre los que destacaría *Keeping Up with the Kardashians* (2007). El estreno de esta serie coincidió con el advenimiento de las redes sociales y sus protagonistas tuvieron un papel crucial en el auge de la figura del prescriptor o *influencer*, que expandió la tendencia a la exposición de la gran a la pequeña pantalla. Este mundo del espectáculo y la celebridad hacía que ser visto fuese una cuestión de privilegio, de deseo. Si las posibilidades de los quince minutos de fama de Warhol se limitaban a la televisión, las redes sociales abren las puertas a que cualquiera pueda conseguirlo.

Aunque he de decir que no solo del deseo de fama y atención se alimentan las tecnologías de la vigilancia actuales. Así, Ariane Ellerbrok (2011) destaca el papel del juego a la hora de dar cuenta de la vida social de estas tecnologías. Después de todo, el juego persigue una lógica de *marketing* además de ser una práctica cultural importante. En relación a ello, Lyon (2018, p. 88) se pregunta: ¿podría el juego ayudar a facilitar el camino a tecnologías controvertidas que pueden tener implicaciones muy graves? Si es así, esto daría un giro al clásico análisis del juego de Johan Huizinga (1938/2012), que lo veía como algo diferente de la vida cotidiana y la obtención de ganancias o a la política. Para justificar su teoría Ellerbrok se centra en las tecnologías de reconocimiento facial (FRT, por sus siglas en inglés) donde ve que a través de ellas, el juego se convierte en parte de la vida cotidiana pero sirve para respaldar objetivos comerciales y gubernamentales más amplios.

La FRT es una tecnología biométrica que utiliza algoritmos para hacer coincidir rostros desconocidos con imágenes previamente existentes de personas conocidas en una base de datos. Ha sido utilizado por la policía y las agencias de seguridad y fue ampliamente comercializada después del 11-S como una herramienta clave en iniciativas antiterroristas. (Lyon, 2009). Pero como observa Ellerbrok, la FRT también está actualmente disponible en contextos de consumo, y se utiliza para la creación de redes fotográficas y la organización de imágenes digitales personales, siendo el más conocido el caso del etiquetado de Facebook. En este contexto, los objetivos de placer, comodidad y entretenimiento son mucho más visibles.

Estas tecnologías de reconocimiento facial son controvertidas en sus contextos militares, policiales y de seguridad originales, sobre todo porque hay evidencia de su uso para subordinar a ciertos grupos según características raciales, étnicas y de clase. Pero cuando Google Picasa e iPhoto Faces comenzaron a ofrecer oportunidades de FRT a sus clientes, parecían tener pocas o ninguna característica amenazadora o negativa. Al contrario, resultaba una tecnología conveniente y entretenida (Ellerbrok, 2011, p. 533). Sobre esto, la autora también destaca que el “etiquetado de fotografías” que ahora se utiliza ampliamente en diversas plataformas no parece tener asociación para las personas usuarias con el “etiquetado” electrónico de los delincuentes como medio de identificación y seguimiento delictivo. De hecho, el potencial error en el etiquetado de las fotografías se considera una fuente de humor, y se asocia con sentimientos como la despreocupación, el escapismo e incluso la fantasía.

Sobre esta cuestión son interesantes los ejemplos que recoge Marta Peirano (2019, pp. 122-125) sobre la banalización del uso de herramientas de reconocimiento facial. De esta manera, relata (Peirano, 2019, p. 122) cómo en mayo de 2018, la cantante Taylor Swift utilizó algoritmos de reconocimiento facial en el Rose Bowl de Los Ángeles bajo el pretexto de ofrecer una actividad lúdica para sus fans. Sin

embargo, la revista *Rolling Stone* reveló más tarde que el recinto estaba equipado en secreto con un *software* de reconocimiento facial, enviando fotos de los asistentes a un servidor de Nashville para compararlas con una base de datos de presuntos atacantes a la cantante.

Por otro lado, también describe el uso indiscriminado de Amazon Rekognition, un sistema diseñado para identificar a personas sin consentimiento, permiso o resistencia, el cual está disponible tanto para varias industrias, como tiendas, centros comerciales, bancos, garajes, festivales de música, gasolineras, universidades privadas y parques temáticos. C-SPAN lo utiliza para identificar automáticamente a políticos, Sky News lo utilizó en la boda de Harry y Meghan Markle, y también está presente en el Madison Square Garden lo usa como parte de su protocolo normal de seguridad. «Cada nuevo usuario pone un nuevo ojo en la red de vigilancia de Amazon, que extiende sus dominios y agudiza sus habilidades para ponerlas al servicio de sus valiosos clientes, como Palantir» (Peirano, 2019, p. 123).

Todo esto sugiere ciertas cuestiones relativas a cómo algunas personas se sienten atraídas por las nuevas tecnologías, desde el *smarthpone* hasta el Internet de las cosas (IoT por sus siglas en inglés), con una sensación de asombro y emoción por lo nuevo. Y también a cómo estos objetos pronto se vuelven familiares y se dan por sentados, especialmente cuando son invisibles y no se ajustan a las definiciones tradicionales de vigilancia y privacidad. En el siglo XX de Orwell, un vehículo vigía habría sido intervenido deliberadamente, mientras que en el siglo XXI, es común que los vehículos vigilen, en el sentido de que registran su propio uso, y esos datos están disponibles para su escrutinio, incluso antes de la profetizada (pero que nunca termina de cumplirse) llegada de los coches autónomos. Podría resultar sencillo volverse indiferente a estos supuestos, si entendemos que con el uso de estos registros, los vehículos son más seguros, y que su llegada es inevitable, por lo tanto resultarían beneficiosos o al menos neutrales.

En el caso de los teléfonos inteligentes, muchos disfrutamos de las comodidades que ofrecen, el contacto por videollamada e incluso su estética. Esto se da particularmente en la era del iPhone, ya que estos dispositivos, son vistos como objetos de deseo (Lupton, 2015, p. 166), incluso los podemos considerar como objetos íntimamente ligados a sus dueños, como extensiones o prótesis del cuerpo, asociados con su personalidad. Los usuarios pueden llegar a pensar en sí mismos en términos similares a los de un *cyborg*, particularmente cuando el iPhone se desbloquea con una huella digital o con reconocimiento facial en lugar de una contraseña. Estas acciones distan bastante de los imaginarios creados a través de *1984*, «nuestro profeta no es George Orwell sino Aldous Huxley. No *1984* sino *Un mundo feliz*» (Postman, 1984, citado en Peirano, 2019, p. 230) ya que el poder de estas tecnologías no está tan basado en la violencia como en su capacidad de distracción. Lo que sucede con las formas en

que estos objetos se convierten en parte del *lebenswelt* o mundo vital tiene que ver en cómo pensamos en ellos menos como “herramientas” —donde su función y eficiencia para sus usuarios son primordiales— y más como “presencia”, donde el usuario y el contexto específicos son cruciales. A nivel filosófico, tenemos una mayor tendencia a pensar de una manera más fenomenológica en cómo la gente “habita” con los dispositivos informáticos, en lugar de simplemente “interactuar” con ellos (Hallnäs y Redström, 2002). No solo nos preguntamos qué significan para nosotros, sino también qué “hacen”.

Así, por ejemplo, los usuarios de *wearables*, esto es, dispositivos portátiles, se preguntan sobre su normalidad: «¿Estoy haciendo esto correctamente?, ¿mi régimen dietético está dando los resultados esperados?, ¿cómo me estoy desempeñando en relación con mis compañeros y mi pasado?» (Lyon, 2018, p. 102). Sus prácticas cotidianas se derivan de estas cuestiones, a través de un uso y control asiduos de estos dispositivos buscan asegurarse de que su rendimiento está realmente a la altura de las expectativas fijadas, o incluso va más allá de lo normal. No hace falta tener mucha imaginación para ver cómo esto también puede tener efectos normalizadores a medida que la importancia de los datos se eleva y eclipsa otras formas de estar al tanto de lo bien —o no— que le va a uno mismo.

Esto se deriva, de nuevo, de entendernos y relacionarnos como datos (Cheney-Lippold, 2017). En otras palabras, los sistemas y plataformas digitales ven a sus usuarios sólo en términos de datos. «Desde la persona mayor que podría caerse en el edificio de su ciudad inteligente hasta el trabajador que debe usar un rastreador en la oficina o planta de fabricación, el sistema conoce a cada uno de ellos como datos, organizados y analizados mediante algoritmos» (Lyon, 2018, p. 104). Tal «gubernamentalidad algorítmica», como explican Rouvroy y Stiegler (2016, p. 7), ignora a los individuos encarnados a los que afecta porque su supuesto sujeto es en realidad un organismo estadístico. Como ellos dicen, los individuos son considerados como agregados temporales de datos explotables a escala industrial.

Las revelaciones de Snowden

Edward Snowden es un ex asistente técnico de la CIA que fue empleado de la empresa contratista de defensa Booz Allen Hamilton, el cual saltó a los medios de comunicación internacional en 2013 por ser el responsable de una de las filtraciones más importantes de la historia política de Estados Unidos (The Guardian, 2013). Sus revelaciones expusieron el alcance de las actividades de vigilancia llevadas a cabo por la NSA, incluida la recopilación de metadatos telefónicos de millones de estadounidenses y el monitoreo de las comunicaciones por Internet a escala global. Sus filtraciones provocaron un debate global sobre los derechos de privacidad, la transparencia gubernamental y el equilibrio entre la seguridad y las libertades civiles.

Inmediatamente después de las noticias sobre el acceso de la NSA a los datos de los suscriptores telefónicos de Verizon, llegaron las revelaciones sobre el programa PRISM, que implican directamente a las principales empresas de Internet. Si bien se produjeron intercambios urgentes, algunos de los cuales parecieron implicar cierta perplejidad por parte de las empresas, ya que admitían que se habían desprendido de algunos datos, las revelaciones parecían sugerir que se trataba de cantidades mucho mayores de las que ellos mismos habían autorizado (Lyon, 2015, p. 53). Según pudimos saber, más allá del acceso autorizado por la Ley de Vigilancia de Inteligencia Extranjera (FISA por sus siglas en inglés) a los datos en poder de las empresas de Internet, la NSA también había encontrado formas de interceptar el flujo de datos en sentido ascendente, mediante métodos como el sistema *Muscular*, desarrollado por la NSA junto con su socio, el Cuartel General de Comunicaciones del Gobierno de Reino Unido (GCHQ por sus siglas en inglés).

Si bien, corporaciones como Google, Yahoo! y Twitter afirmaron *a posteriori* que habían luchado por frenar los intentos del gobierno, de obligarlos a entregar los datos de los clientes a través de órdenes judiciales especiales del tribunal FISA (Lyon, 2015, p. 53). El hecho de que existiesen compartimentos con autorización de seguridad tampoco ayudaba, las revelaciones de Snowden revelaron que los expertos en seguridad dentro de estas empresas trabajaban con “puertas traseras” o “*backdoors*” para el gobierno estadounidense.

Ya he mencionado anteriormente a Claude Shannon (1949), quien en su teoría matemática de la comunicación, argumentaba que el contenido de los mensajes, es decir, su aspecto semántico, era irrelevante para la cuestión de la ingeniería del almacenamiento y la transmisión de la información. Como veremos más adelante, al hablar de metadatos se ha seguido en gran medida esta misma lógica (Austin, 2015, pp. 113-114). Y es que el contexto de divulgación y recepción de los mensajes no se consideraba relevante. Los metadatos resultaban una cuestión meramente técnica; el contenido no tenía conexión con él. La privacidad en estos momentos se relacionaba con el contenido, por lo que recopilar metadatos no constituía vigilancia. Sin embargo, hoy en día es imposible desenredar los metadatos y el contenido.

Hasta la década de 1970, la información todavía no resultaba un tema ampliamente discutido, aunque las organizaciones de seguridad sin duda fueron conscientes de su importancia desde el principio. Cuando en esta década se propuso la idea de que una sociedad podría experimentar una “revolución de la información”, las dos interpretaciones de la información quedaron oscurecidas pero aún presentes. El resultado práctico, y consecuente, de la doble definición de información no se haría plenamente evidente hasta los debates post-Snowden.

Aunque ya a mediados de los años noventa, el sociólogo Manuel Castells (1996/1997) había demostrado cómo la información había adquirido importancia en relación con la difusión de nuevas tecnologías electrónicas y había pasado a ser básica para la vida económica, política y social en el mundo moderno:

Lo que caracteriza a la revolución tecnológica actual no es el carácter central del conocimiento y la información, sino la aplicación de ese conocimiento e información a aparatos de generación de conocimiento y procesamiento de la información/comunicación, en un círculo de retroalimentación acumulativo entre la innovación y sus usos (Castells, 1996/1997, p. 58).

En sus obras hablaba de un modo de desarrollo informativo que era flexible, omnipresente, integrado y reflexivo. La competitividad comercial ahora dependía de que las empresas fueran capaces de generar y procesar información en una base cada vez más global y en tiempo real. Curiosamente, Castells también observó que la comercialización de Internet era el «momento clave» para una mayor vigilancia en línea (Castells, 2001, p. 170).

Cuando el llamado “contenido generado por el usuario” se convirtió en el rasgo definitorio de la “*Web social*”, Castells se refirió al fenómeno emergente como «autocomunicación masiva» (Castells, 2009, p. 55). En consecuencia, para Lyon (2015, p. 62), la sociedad red, descrita en el primer volumen de *La Era de la Información* (1996/1997), en la que todos los aspectos de los acuerdos sociales, económicos y políticos se ven afectados por su dependencia de las nuevas tecnologías, es igualmente una sociedad de la vigilancia. Esto significa que las tendencias hacia los monopolios de influencia y poder son fomentadas por las mismas tecnologías que también alientan la creencia de que la libertad de expresión es viable en Internet.

Como subraya Castells (1996/1997), existe una tensión inherente entre la “red” y el “yo”. Y si bien las tecnologías anteriores pueden haber enfatizado su poder en el tiempo (los medios impresos tienen una influencia a largo plazo) o en el espacio, las comunicaciones modernas, desde el telégrafo en adelante, apoyaron las tendencias globalizadoras (Innis, 1951). A través de Internet existe la capacidad de unir el tiempo y el espacio y por tanto, de facilitar nuevas formas de control que comprimen las relaciones sociales en nuevos moldes técnicamente configurados.

No es de extrañar entonces que el control de la información se haya convertido en una cuestión tan crucial para los gobiernos, las corporaciones y el público en el siglo XXI. El *hacktivismo*, que utiliza sistemas informáticos para protestar y promover fines políticos, surgió como respuesta, y nombres

como Wikileaks y Anonymous son sinónimos de controversias sobre quién posee qué información y qué no debe permanecer en secreto (Lyon, 2015, p. 62).

Cuando las revelaciones de Snowden aparecieron en las noticias, muchos asumimos que las actividades de la NSA eran simplemente ilegales. La indignación moral expresada por Snowden se extendió rápidamente cuando estas cuestiones parecieron muy claras. Sin embargo, a medida que salieron a la luz los detalles de cómo la FISA fue reinterpretada subrepticamente y los jueces llegaron a decisiones contrarias sobre la legalidad de lo que sucede en la NSA, la estridente oposición a la vigilancia masiva global se vio amortiguada por una masa de ambigüedades técnicas y legales. Con todo, más adelante veremos cómo en muchos ámbitos y lugares se ha comenzado paulatinamente a dar respuesta a esta problemática.

La Era del Capitalismo de la Vigilancia

El concepto de “capitalismo de la vigilancia” fue descrito por primera vez por John Bellamy Foster y Robert W. McChesney (2014), aunque también fue utilizado en la misma época por Vincent Mosco (2014). Sin embargo, su exponente más conocida en los últimos tiempos ha sido Shoshana Zuboff, quien ya en 2014 publicó un artículo en el diario alemán *Frankfurter Allgemeine* titulado “*Big Data*” as *Surveillance Capitalism*, para luego popularizar el término en su obra más notoria, *La era del Capitalismo de la Vigilancia* (2019/2020).

Aunque todos los autores mencionados al inicio hicieran uso del mismo concepto, su sentido difería en cada caso: Foster y McChesney lo aplicaron para describir la forma de operar de la financierización de los mercados de finales del siglo XX y la necesidad de una recopilación masiva de datos para su correcto funcionamiento. Para estos autores, tal sistema surgió a lo largo del desarrollo del complejo militar-industrial y de consumo que hemos podido leer también a lo largo de estas líneas. Para Mosco el término se refería a la comercialización de información sobre diferentes clientes y suscriptores a los anunciantes, circunscrito dentro de un Estado de vigilancia. Sin embargo, en Zuboff el concepto hace referencia a la mercantilización de datos personales, es decir, al hecho de convertir datos personales en productos que se pueden vender con fines de lucro:

Los usuarios no somos productos, sino, más bien, las fuentes de provisión de la materia prima del proceso. Los inusuales productos del capitalismo de la vigilancia se derivan de nuestro comportamiento. Sus productos consisten en predecirnos, pero no se preocupan en realidad de lo que hagamos o de lo que nos ocurra. (Zuboff, 2019, 2020, p. 102).

La reformulación de la información como característica definitoria del capitalismo de finales de siglo XX se puede rastrear en las obras de Fritz Machlup (1962), Daniel Bell (1973) o el ya mencionado Marc Uri Porat (1977). De modo más cercano, encontramos el concepto de “capitalismo informativo” de Manuel Castells (1996/1997), el “capitalismo digital” de Dan Schiller (1999), y más recientemente el “capitalismo de plataforma” de Nick Srnicek (2017) o el concepto de “capitalismo de datos” que aparece en los artículos de Sarah Myers (2019) o Jathan Sadowske (2019), entre otros.

Si bien podemos deducir por el estudio histórico de la vigilancia que ésta no ha sido algo exclusivo del capitalismo, en la teoría de Zuboff el capitalismo de la vigilancia se basa en una lógica específica de acumulación capitalista y un nuevo tipo de mercado radicalmente extractivista y desencajado del capitalismo informativo. No en vano, esta variante se basa en la mercantilización de la realidad y la posterior transformación de los datos basados en el comportamiento humano para su análisis y venta. Otra gran diferencia que podemos encontrar con otros postulados es que Zuboff sitúa su origen en el desarrollo de Google como empresa y, más concretamente, en su búsqueda de rentabilidad tras el estallido de la crisis de las punto.com.

Vale la pena que nos detengamos un momento para entender qué supuso esta crisis. Con tal fin debemos remontarnos a principios de los años noventa, cuando se desarrolló la ya mencionada World Wide Web, que dio lugar a un gran aumento de usuarios y a la rápida comercialización de Internet. Durante estos años, se produjo una serie de acontecimientos que marcaron la posterior crisis: la primera es la también citada desaparición de la NSFNET en 1995, que provocó que el sistema quedase bajo el control de proveedores privados de servicios de Internet; en segundo lugar nos encontramos la aprobación de la Ley estadounidense de Telecomunicaciones de 1996, la cual introdujo una desregulación masiva de las telecomunicaciones y los medios de comunicación, lo que sentó las bases de una mayor concentración y centralización de estas industrias (McChesney, 2004, pp. 51-56); y en tercer lugar destacaría la aprobación de otra ley en EEUU, la de Modernización de los Servicios Financieros de 1999, norma que liberalizó el sector financiero derogando la Ley Glass-Steagall aprobada 4 años después del llamada Crack del 29. Estos tres elementos se combinaron en una de las mayores olas de fusiones de la historia, e este modo, la concentración de capital en curso recibió un enorme impulso en los sectores tecnológicos y financieros, lo que dio lugar a niveles cada vez mayores de poder monopolístico. La burbuja punto.com estalló en el año 2000, pero para entonces Internet ya había llegado a desempeñar un papel central en la acumulación de capital, y las empresas que lo dominaban eran casi todas “monopolios”.

Es a mediados de esta época, concretamente en 1998, cuando Larry Page y Sergey Brin fundaron la

compañía Google, la cual en sus inicios se basaba meramente en su famoso motor de búsqueda, que pronto se convirtió en uno de los más usados. Nacido dentro de un proyecto universitario, el ciclo de Google «estaba orientado al individuo como sujeto de este, pero sin un producto físico en venta: flotaba fuera del mercado y era una interacción con los “usuarios”, más que una transacción mercantil con unos clientes» (Zuboff, 2019/2020, p. 101). De esta manera, los primeros ingresos de la compañía se basaron en otorgar licencias exclusivas para suministrar servicios *web* a páginas como Yahoo! o Biglobe (Zuboff, 2019/2020, p. 103). Sin embargo, la citada explosión de la burbuja de las punto.com provocó que, para mantenerse, la empresa tuviese que obtener beneficios de otras fuentes, en lo que Zuboff denomina como “el descubrimiento del excedente conductual” (Zuboff, 2019/2020, pp. 98-113).

El punto que destacar aquí es que, desde el principio, además de las palabras clave, con cada búsqueda en Google se generaba una serie de datos colaterales: el número y la pauta de términos de búsqueda, la forma en que se expresaban, la ortografía, la puntuación, la duración, dónde se hacía clic y la ubicación. Sin embargo, estos “productos conductuales secundarios” eran almacenados sin categorizar, ya que no se consideraban valiosos para otros usos operativos de la empresa.

El descubrimiento de la importancia de estas memorias caché de datos fortuitos que Google poseía fue realizado por Amit Patel, un joven titulado por Stanford y muy interesado en la minería de datos. El estudio de estos registros de datos le llevó a creer que era posible crear un historial detallado de cada usuario a partir de las señales no estructuradas que dejaba con cada actividad *online*. Los ingenieros de Google rápidamente se dieron cuenta de que estos datos sobre el comportamiento de los usuarios podrían convertir el motor de búsqueda en un motor de aprendizaje recursivo que mejorase continuamente los resultados de búsqueda e innovara en productos como el corrector ortográfico, el traductor y el reconocimiento de voz. Lo que antes se consideraba un material sin uso, rápidamente pasó a convertirse en un elemento clave de la transformación de la búsqueda de Google a través de un proceso aprendizaje continuo. Es decir, durante esta fase inicial, los datos de comportamiento estaban a disposición de los usuarios, y estos datos proporcionaban valor gratuito que se reinvertía en su experiencia en forma de servicios mejorados y gratuitos.

Sin embargo, en el año 2000 y en respuesta a las preocupaciones de los inversores de la compañía por la caída de las punto.com, los fundadores encargaron a un pequeño equipo de AdWords, la sección publicitaria de Google que hasta ahora había tenido un trabajo y rentabilidad residual, la tarea de encontrar formas de ganar más dinero. A nivel operativo, esto significó que Google dedicaría su caché de datos de comportamiento, así como su potencia informática y experiencia a un propósito: hacer

coincidir los anuncios con las consultas de búsqueda. La información recopilada hasta ese momento iba a ser usada también para mostrar publicidad dirigida a los usuarios. En otras palabras, Google ya no se dedicaría a analizar datos de comportamiento sólo para mejorar los servicios a los usuarios, sino que se centraría en analizarlos para que recibiesen anuncios supuestamente relevantes que pudiesen coincidir aparentemente con sus preferencias. Gracias al acceso exclusivo de Google a todos estos datos de comportamiento, finalmente podría llegar a ser posible saber qué piensa, siente y hace una persona en un momento y lugar determinados (Zuboff, 2019/2020, p. 113).

La nueva lógica acumulativa se extendió también a Facebook, fundada el mismo año en que Google salió a Bolsa. A finales de 2007 se produjo, por parte de Facebook, el primer intento de imitar la lógica acumulativa de Google. Lo hizo a través de su primer producto publicitario denominado Beacon, que reenviaba automáticamente las transacciones realizadas en sitios asociados a los “amigos” de los usuarios, incluso si éste no había iniciado sesión en ese momento y sin su conocimiento. Tras una serie de quejas, tanto de usuarios como de algunos socios de Facebook como Coca-Cola, tuvieron que dar marcha atrás y Beacon se convirtió en un programa de reclutamiento voluntario. Tras este intento fallido, en marzo de 2008, Zuckerberg contrató a Sheryl Sandberg, que en Google había liderado la expansión de AdWords y convertiría Facebook en el «vector del capitalismo de vigilancia» (Zuboff, 2019/2020, p. 130).

En efecto, a partir de ese momento Sandberg fue responsable de transformar Facebook de una mera plataforma de redes sociales a un gigante publicitario que aprendería a rastrear, recopilar, almacenar y analizar los datos de sus usuarios para poder crear sus propios algoritmos de orientación de anuncios. Si a ello sumamos la simultánea manipulación de la cultura de privacidad e intercambio de información que fomentó, todo ello podría explotar el excedente conductual no solo para satisfacer la demanda existente sino también para crearla. A estas empresas se unirían otras que comenzarían a hacer uso de los datos de comportamiento de sus usuarios para crear predicciones sobre sus intereses de compra para su propio uso, como es el caso de Amazon o para venderlos a terceros.

Zuboff (2019/2020, pp. 132-137) resume así el funcionamiento del capitalismo de la vigilancia sobre la lógica, los medios de producción, los productos y el mercado:

En primer lugar, la autora sintetiza su “lógica” a través de la citada forma en cómo Google transformó sus interacciones no mercantiles con sus usuarios en “materia prima excedentaria” apta para generar predicciones que ofrecer a sus nuevos clientes reales, los anunciantes. Si bien al comienzo esta información se encontraba directamente vinculada con las acciones de búsqueda de los usuarios, más

tarde hicieron uso de una vigilancia más estricta para capturarla en mayores cantidades. La pauta que se repite en todo este conjunto es la dependencia y la jerarquía. La relación actual de este tipo de empresas con sus usuarios depende de la capacidad de explotar los excedentes de comportamiento y utilizarlos para servir a los objetivos de otros. Para esta autora: «somos, más bien, los *objetos* de los que se extrae una materia prima que Google expropia para su uso en sus fábricas de predicciones» (Zuboff, 2019/2020, p. 134).

El perjuicio derivado de estas prácticas no se limita a que los usuarios no reciban compensación por la información que suministran; de hecho, profundizar en esta crítica sería un error conceptual, lo que significaría recurrir al mecanismo de precios para institucionalizar y con ello legitimar la explotación del comportamiento humano con fines de producción y venta. Las cuestiones más notables que destaca Zuboff en este contexto son: que nuestras vidas se están convirtiendo en meros datos de comportamiento; que la ignorancia de este hecho por nuestra parte es una condición necesaria para tal entrega universal para su conversión; que estamos perdiendo el poder de decidir antes de darnos cuenta de que tenemos que tomar alguna decisión; que al limitar nuestros derechos existen una serie de consecuencias que no podemos ver ni predecir; que ni siquiera los medios populares de expresión, voz o (incluso) lealtad son opciones disponibles porque estamos condenados al desamparo, la resignación y la parálisis mental; y por último destaca que el cifrado de nuestra información es la única acción que podemos llevar a cabo para «ocultarnos de esas fuerzas que se ocultan de nosotros» (Zuboff, 2019/2020, p. 134).

Sobre los “medios de producción”, alude a que las capacidades de inteligencia de las máquinas de Google están impulsadas por el ya denominado excedente conductual, y sus productos predictivos son más precisos cuanto más consumen de él. La contradicción entre cantidad y calidad es una de las principales diferencias entre los nuevos medios de producción y el modelo clásico industrial. Debido a que solo puede explotar su potencial cualitativo a través de un enfoque holístico, la inteligencia de máquinas es una síntesis de esta tensión.

Acerca de la naturaleza de los productos de Google explica por qué, la empresa afirma y reitera que no vende datos personales, ya que en realidad vende predicciones que sólo puede generar a partir de enormes colecciones de la información que recopila. Google se convierte así en una especie de adivino basado en datos, para supuestamente predecir nuestros futuros y potenciales intereses y venderlo a los clientes publicitarios para obtener sus ganancias.

Por último habla de un “mercado” completamente nuevo que está enfocado en las conductas futuras.

Para Zuboff, resulta evidente que los nuevos sistemas de predicción se hayan enfocado en la publicidad, dado que cualquier actor interesado en comprar información probabilística sobre la conducta o en influir en el comportamiento futuro puede pagar para conocer el futuro conductual individual, colectivo y hasta no humano. El mundo, el yo individual y el cuerpo quedan reducidos al estado permanente de objetos disueltos en un nuevo y colosal concepto de mercado desde el punto de vista de la vigilancia del capitalismo y sus imperativos económicos.

Para entender cómo se ha extendido esta forma de operar hasta llegar a convertirse en una de las empresas más importantes de los últimos tiempos, tenemos que tener en cuenta una serie de factores clave:

El primero tiene que ver con los esfuerzos por continuar operando en un espacio poco regulado. A pesar del crecimiento de Google hasta convertirse en una de las empresas más poderosas del mundo, Schmidt, Brin y Page han defendido con fervor su derecho a continuar actuando sin restricciones legales. Esto lo justifican a través de la idea de que las empresas tecnológicas avanzan más rápido que los Estados, lo que significa que cualquier esfuerzo por intervenir o limitar su avance sería un error de concepto e incluso una estupidez; ya que la regulación siempre es una fuerza perjudicial que obstaculiza la innovación y el progreso. Para ello, Google ejerce fuertes presiones políticas para anular las protecciones a la privacidad en línea, debilitar o bloquear toda legislación que promueva la privacidad y frustrar cualquier intento de limitar sus prácticas, ya que estas leyes amenazan el flujo libre y sin restricciones del excedente conductual.

Dentro de este legado neoliberal, cuya máxima tesis es la de la autorregulación, se genera un modelo que trata la privacidad como un bien competitivo, basado en que los “consumidores” solo van a hacer uso de aquellos servicios que les brindan el nivel de privacidad que buscan.

En segundo lugar, el desarrollo de estas empresas ha tenido lugar dentro de unas específicas circunstancias históricas y políticas, así como de una orientación jurídica dentro del paradigma neoliberal, que han brindado protección a su desempeño. Cabe destacar el gran interés de los Estados después de los atentados terroristas de septiembre de 2001 por seguir impulsando las capacidades emergentes de análisis de excedente conductual y la elaboración de pronósticos y predicciones a partir de dicho análisis, para lo que estas empresas sirvieron de gran ayuda.

Y es que, desde las semanas posteriores al 11S, el presidente Bush autorizó a la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) a realizar una serie de actividades de vigilancia dentro de EEUU que habían estado prohibidas por la Constitución estadounidense y la política de la agencia

durante décadas. Cuando el programa de espionaje de la NSA fue expuesto por primera vez por el New York Times en 2005, el presidente Bush admitió un pequeño aspecto del programa (lo que la administración denominó “Programa de Vigilancia del Terrorismo”) en el que la NSA monitoreaba, sin órdenes judiciales, las comunicaciones dentro de EEUU de entre 500 y 1000 personas con presuntas conexiones con Al-Qaeda. Pero otros aspectos del Programa no estaban dirigidos solamente a individuos específicos, sino a millones de estadounidenses que nunca fueron sospechosos de ningún delito (Electronic Frontier Foundation, s.f., párr. 3-4).

La recopilación de información sobre la población se tornó aún más fundamental para los regímenes de seguridad. A través de un seguimiento primero, objetivo después, se invirtieron todos los modos anteriores de práctica de vigilancia, de modo que a partir de ese momento todos los datos eran potencialmente relevantes. Como lo expresa de manera sucinta, aunque sarcástica, Mark Andrejevic (2013, p. 38): «No recopilamos datos sobre usted porque sea sospechoso, sino porque puede ayudarnos a identificar quiénes son los verdaderos sospechosos». Con el tratamiento de datos a gran escala no hay anonimato, y con demasiada frecuencia el interés pasa sin problemas de las causas a las correlaciones. Estas empresas, al contar con grandes cantidades de datos de usuarios, supusieron un gran espacio de recopilación para la seguridad nacional.

Si bien la obra de Zuboff nos ayuda a entender las formas de operar de la mayoría de las empresas tecnológicas que lideran los índices bursátiles de nuestro tiempo, a través de un extenso estudio sobre ciertos conceptos como el extendido y adoptado “capitalismo de la vigilancia” o el “excedente conductual”, su teoría no está exenta de críticas. Una de las más extensas fue escrita por Evgeny Morozov (2019, 2022), en la cual argumenta que gran parte de lo que escribe Zuboff sobre el “capitalismo de la vigilancia” se puede explicar a través del capitalismo propiamente dicho. Para el autor bielorruso, así, las críticas de Zuboff encajarían con los imperativos capitalistas ampliamente conocidos: expandirse a todos los espacios, tomar, mercantilizar, vender y explotar la experiencia humana para obtener ganancias, así como derribar las barreras legales y políticas que se interponen en su camino.

Al insistir en que la forma de vigilancia del capitalismo opera tomando el control de nuestro “yo” y dirigiéndonos hacia patrones predecibles, Morozov achaca a Zuboff la ignorancia de gran parte de la explotación material, prefiriendo en cambio concentrarse en el tipo de actividades que podrían molestar principalmente a la clase media del mundo desarrollado. Mientras tanto, como hemos visto en el apartado 1.1.1., el *hardware* de vigilancia de estos dispositivos todavía es ensamblado por trabajadores con condiciones laborales penosas y las materias primas necesarias para su funcionamiento, como el cobalto, son extraídas por la población de países de África, Asia o Latinoamérica en condiciones

todavía peores a los anteriores.

Otro de los aspectos que cuestiona Morozov tiene que ver con el modelo de negocio de Google, al indicar que existe una falta de atención en la obra de Zuboff sobre de dónde proviene la información indexada que el rastreador *web* muestra a sus usuarios y por qué éste, al no pagar ninguna tasa por cada dato que muestra en su página de resultados, obtiene unos altos beneficios. «Google ofrece su producto de búsqueda de forma gratuita, lo que a su vez, le permite vender a los anunciantes otro producto muy rentable: la atención de sus usuarios, mediante el acceso a sus pantallas» (Morozov, 2022, p. 123). La solución para Zuboff, según este autor, pasa por el abandono de Google de la venta de espacios publicitarios y la extracción de datos asociados a esta prácticas para comenzar a cobrar por sus servicios de búsqueda. «El hecho de que esto normalice inadvertidamente toda la “desposesión digital” que se produce en la fase de indexación, consolidando el poder de Google y su control sobre el imaginario institucional de la sociedad, no preocupa demasiado a Zuboff» (Morozov, 2022, p. 124). Por todo ello, el autor de *El desengaño de Internet* ve en las teorías de Zuboff, no tanto un “capitalismo de vigilancia” cuanto un “usuarismo”¹¹ que centra el problema no en el capitalismo como tal sino en la vigilancia sobre el usuario-consumidor.

Otro aspecto que Zuboff parece ignorar en su obra es la larga tradición de la vigilancia como parte integral del capitalismo, insistiendo en que se ha producido una ruptura radical en la última década. El capitalismo de la vigilancia ha demostrado no ser la revolución de la información, sino la reacción a la misma. Para la autora, en lugar de hacernos avanzar por el camino de la individualización, el capitalismo de la vigilancia nos ha atrapado, capturado y despojado de nuestro derecho a decidir por nosotros mismos como seres autónomos plenamente realizados. Así como Marx vio que el capitalismo sólo había reemplazado la explotación del feudalismo por la explotación a través del trabajo asalariado, también el capitalismo de la vigilancia nos ha atrapado en una red de control del comportamiento para negar, en lugar de ampliar, nuestra individualidad.

Sin embargo, la crítica posmoderna que enfatiza la subjetividad y las posiciones de sujeto ha puesto en tela de juicio durante mucho tiempo la concepción humanista del individuo. Las instituciones, como las

11 En relación con el término “usuarismo” para Morozov (2002, p. 121):

el sistema económico que describe [Zuboff] no es ni capitalista ni feudal. Es lo que podría llamarse, a falta de un término mejor, *usuarismo*, en analogía directa con el *operaismo* italiano. Los italianos no podían imaginar cómo las empresas capitalistas no rentistas y ligeras de mano de obra podrían obtener beneficios capitalistas simplemente atrayendo el plusvalor producido en otros lugares; en consecuencia, acabaron introduciendo conceptos forzados como «trabajo digital gratuito». Zuboff, a su vez, no puede imaginar que la experiencia humana congelada en datos del usuario, que son objeto de apropiación en el momento mismo en que este interactúa con los artefactos digitales, no sea el principal motor de los exorbitantes beneficios de Google. El *usuarismo* postula que, de Google a Facebook, la parte fundamental de los beneficios de estas empresas se deriva de su expropiación de los datos de los usuarios.

escuelas, las prisiones, los asilos, y en definitiva los panópticos de todo tipo, así como las agencias de crédito, las compañías de seguros o los departamentos de personal corporativo, todos realizan una enorme cantidad de vigilancia, llevan registros y categorizan a las personas. No sólo controlan o moldean el comportamiento, sino que plantean las condiciones de posibilidad al colocar a las personas en ciertas categorías, definiéndolas como ciertos tipos de individuos.

De hecho, en otra obra anterior suya, *The Support Economy* (2002), Zuboff imaginó que la tecnología de la información se aprovecharía para el individualismo puro, sin poder, sin categorías reductivas. Pero los datos nunca pueden estar libres de categorías; cuanto más datos, mayor es la necesidad de formas de organizarlos y clasificarlos. Como señaló Foucault (1975/2002), la subjetividad implica tanto una individualización extrema como la inclusión de los individuos en ciertas categorías. Estas categorías regulan la sociedad de masas, pero no son lo opuesto a la individualización. Las dos trabajan juntas: los individuos se forman en los muchos mecanismos de poder que nos rodean y se infiltran en nuestras vidas por muchas vías. Este capitalismo de la vigilancia opera como otros sistemas, pretendiendo ayudarnos, apoyarnos y liberarnos, al mismo tiempo que nos controla y nos categoriza en posiciones de sujeto.

Más allá de si el término “capitalismo de la vigilancia” es todo lo conciso y acertado que nos gustaría, debemos admitir que se trata de un concepto que se ha expandido a gran escala y que ayuda a visualizar con cierta rapidez y sencillez las formas de extraer beneficios de muchas de las empresas que operan en el entorno digital. Hablamos no solo de gigantes como Google, Meta o Amazon, sino también, por ejemplo, de otras corporaciones que desarrollan aplicaciones de recopilación de datos biométricos, así como también ayuda a desentrañar las diferentes alianzas que establecen con los servicios de seguridad de los Estados.

La pandemia de la COVID-19: un giro epidemiológico en la vigilancia digital

Para muchos, la pandemia de la COVID-19 alteró nuestra vida tal como la conocíamos. Entre el 2020 y el 2022 tuvimos que enfrentarnos a una situación acuciante, con la serie de confinamientos debidos a la expansión desbocada del virus SARS-CoV-2, que nos abocaron a una presencia más amplia dentro del “mundo *online*”. En medio de esa dinámica de sobreexposición e hipermedicación en redes digitales, resultaba verdaderamente difícil eludir los sistemas de recopilación de datos y vigilancia mientras cumplíamos nuestros compromisos en el entorno educativo y laboral y nos manteníamos presentes con nuestro círculo personal. La vigilancia dentro de este entorno pandémico permitió a gobiernos y empresas monitorear y vigilar la propagación del virus y asegurarse de que los ciudadanos cumplíamos

con las medidas que habían establecido. Esto es evidente en la movilización masiva y sin precedentes de datos de salud pública para contener y combatir el virus, así como en la proliferación de tecnologías de vigilancia como las aplicaciones de rastreo de contactos, el reconocimiento facial, el escaneo de la temperatura corporal y el seguimiento de la población.

Para entender el desarrollo de los acontecimientos que tuvieron lugar en estos últimos años, debemos tener en cuenta que desde la Segunda Guerra Mundial, la atención sanitaria había ido tomando forma a través de la lógica militar, en especial en los casos de una posible “amenaza” global. De hecho, el primer uso del término “vigilancia” en relación con la atención sanitaria se le atribuye al epidemiólogo Alexander Langmuir, quien comenzó a trabajar en los Centros para el Control y la Prevención de Enfermedades en Estados Unidos en 1949 (Lyon, 2022, p. 29). Este médico se basó en su experiencia en tiempos de guerra en el Comité de Guerra Biológica del Departamento de Defensa para diseñar y atraer fondos para la vigilancia de enfermedades.

Sin embargo, este patrón no sólo se vio reforzado por las guerras del siglo XX, sino también por el 11-S y la consiguiente “guerra contra el terrorismo”, al estimular la incorporación de la seguridad en la prestación de servicios de salud, especialmente en EEUU. De esta manera, los hospitales y los profesionales de la salud “requerían” nuevas inversiones en tecnología e infraestructuras como solución a eventos como las pandemias (Fisher y Monahan, 2011). Si bien es cierto que otras epidemias, como la del virus H1N1 que tuvo lugar entre 2009 y 2010, se dieron en un mundo donde las tecnologías de la información estaban ampliamente extendidas, la crisis de la COVID-19 fue la primera en ocurrir en un contexto que podríamos enmarcar de lleno en el ya citado capitalismo de la vigilancia.

De esta manera, la reciente pandemia, y con ella algunos nuevos avances en materia de vigilancia, se desplegaron en condiciones sociales y culturales novedosas, provocadas por la declaración de una crisis de salud pública a nivel mundial. No sólo existieron limitaciones vinculadas a la propagación del virus, que modificaron la movilidad y centraron las actividades diarias tanto en el hogar como fuera de él, sino que, además, estas actividades podían ser monitoreadas por organismos externos y remotos., se fomentó la autovigilancia de los síntomas y la vigilancia mutua para el cumplimiento de las normas que se fueron estableciendo para mitigar la plaga. Estas actividades también se digitalizaron, de modo que los teléfonos inteligentes, junto con otros dispositivos compatibles, se convirtieron en un medio para cumplir cada función impuesta, ampliando y normalizando los sistemas de datificación del cuerpo.

Esta pandemia provocó un cambio sin precedentes en las tecnologías digitales no sólo de cara a las diferentes soluciones de atención médica”, sino también en el entorno laboral, educativo, de consumo y

social. Esto supuso un incremento en la presión por parte de las empresas tecnológicas por obtener ganancias de este amplio traspaso de la vida cotidiana al mundo digital, junto con el énfasis en el control gubernamental de la pandemia. De nuevo asistimos a un acuerdo entre corporaciones privadas y gobiernos para monitorear a la población. Un ejemplo de ello lo podemos ver en el enlace Apple-Google para la API que habilitaba las aplicaciones de rastreo de contactos a través de Bluetooth (Lyon, 2022, p. 107). Estas acciones ayudaban a fomentar la sensación de que los gobiernos estaban llevando a cabo medidas para paliar la situación. Sin embargo, estas iniciativas también distraían la atención sobre la realidad de cómo presenciábamos una preparación inadecuada para la pandemia por parte de muchos gobiernos, fruto en gran medida de un insidioso debilitamiento de la atención sanitaria pública, que provocó unos efectos desiguales en cómo se vivió esta crisis por parte de la población.

Para Taylor *et al.* (2020), las rápidas “soluciones” que se adoptaron durante los confinamientos provienen del hecho de que desde hace algunos años se viene observando un “giro epidemiológico en la vigilancia digital”, que cobró impulso con la pandemia. Según estos autores, algunos de estos sistemas ya se utilizaban en el ámbito del desarrollo y la ayuda humanitaria mientras otros, que procedían de grandes corporaciones, fueron adaptados para la COVID-19. El dilema que se plantea aquí deriva de la difícil tarea de desenlazar estas aplicaciones de los ámbitos en lo que tuvieron presencia en estos años. Así, muchas empresas han estandarizado el uso de aplicaciones como Zoom para sus reuniones o vemos todavía la acuciante presencia de Google Classroom en las aulas de los centros de educación pública¹².

El rastreo de contactos durante la pandemia fue un proceso minucioso que requirió mucho trabajo manual, por lo que la idea de automatizar el proceso mediante aplicaciones móviles de rastreo de la ubicación resultó muy atractiva para los funcionarios de salud pública de diferentes países, que de manera rápida e individual desarrollaron diferentes sistemas de rastreo de contactos. Algunos como India, Corea o China establecieron sistemas centralizados de uso obligatorio para la población mientras que otros, sobre todo dentro de la UE, desarrollaron sistemas descentralizados y voluntarios de rastreo.

Aquí tenemos que asumir que la eficacia del rastreo digital de contactos es evidentemente crítica, de hecho, Rob Kitchin (2020) advirtió tempranamente de que, incluso antes de que se estableciera la idoneidad para su uso, las aplicaciones de rastreo de contactos presentaban implicaciones significativas para las libertades civiles, la gubernamentalidad y la ciudadanía. Y refutó la idea de que la salud pública prevalece sobre las libertades civiles, ya que, por un lado, es posible que las tecnologías no funcionen

¹² Sobre los dilemas derivados de la instauración de Google Suite for Education en las aulas de la escuela pública ver: <https://xnet-x.net/es/no-autorizar-google-suite-escuelas/>

adecuadamente, creando una falsa sensación de seguridad, y en segundo lugar, intercambiar libertades civiles por salud es una posición tecno-solucionista, en la que se cree que sólo la tecnología puede ayudar, o que, incluso si es defectuosa, la tecnología aún puede ayudar. Esto simplemente crea un escenario en el que, de cualquier manera, se debe utilizar la tecnología.

De hecho, transcurrido un tiempo desde su implementación, muchas de estas aplicaciones han sido criticadas y sancionadas. Por ejemplo, según Lyon (2022, p. 7), en febrero de 2020 los ciudadanos surcoreanos descubrieron que el gobierno estaba publicando en sitios *web* los detalles de los movimientos exactos de individuos no identificados para todos los casos de COVID-19. En el caso de la aplicación española Radar Covid, además de tener una tasa de penetración del 21%, tan solo comunicó un 1,17% del total de contagios registrados (Sánchez, 2022). Además, la Agencia Española de Protección de Datos (AEPD) sancionó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) y a la Dirección General de Sanidad Pública (DGSP) por diversas infracciones del Reglamento General de Protección de Datos cometidas en el desarrollo, implementación y funcionamiento de la aplicación para el rastreo de posibles contactos positivos de COVID-19 por parte de esta aplicación (Rubí Puig y Herrerías Castro, 2022, p. 1). Y ello por no hablar de que, a pesar de estar desarrollada con *software* libre, sus desarrolladores tardaron en publicar el código y cuando lo hicieron su verificación fue imposible al haberlo ofuscado (Pérez Colomé, 2020).

En suma, no cabe duda de que los datos pueden ser muy útiles, tanto durante una crisis sanitaria como en otros momentos, ya que pueden resultar vitales para comprender algunas situaciones, elaborar respuestas, asignar recursos y evaluar la eficacia de diferentes políticas. Sin embargo, los datos incompletos o incorrectos también pueden “enturbiar las aguas”, oscureciendo matices importantes dentro de las comunidades, ignorando factores importantes como las realidades socioeconómicas y creando una falsa sensación de pánico o seguridad, sin mencionar otros daños como exponer innecesariamente información privada (Balsari *et al.*, 2020).

Algunas conclusiones sobre la vigilancia digital

Hoy en día, la vigilancia se presenta en formas más fluidas y flexibles, en contraste con las formas sólidas y fijas anteriores, lo cual resuena con las modernidades más líquidas del presente (Lyon, 2018, p. 31). Este sistema que Bauman y Lyon (2013, pp. 61-84) bautizan como “vigilancia post-panóptica”, se caracteriza por la citada fluidez, además de la movilidad y la conectividad. Los territorios y las instituciones políticas y sociales pierden su relevancia en favor de las tecnologías y las redes de información y comunicación. En este contexto, según Virilio (1996), la libertad de movimiento:

no está amenazada por una prohibición, como en la época de *Vigilar y castigar* de Foucault, en donde se encerraba a las personas en una prisión para que no pudieran moverse. Ahora, se les encierra en la rapidez y en la futilidad del desplazamiento continuo (p. 57).

Y es que la vigilancia funciona a distancia tanto en el espacio como en el tiempo, canalizando flujos de datos y clasificando socialmente a las personas. Sin embargo, ésta opera también cada vez más de manera consensuada, y depende de cómo las personas la perciben y actúan en relación con ella. Esta forma de entenderla y practicarla se retroalimenta; los imaginarios que se crean a su alrededor proporcionan la sensación de lo que implica vivir bajo vigilancia, mientras que las prácticas sobre las que se experimenta permiten que se produzca una iniciación, un cumplimiento, una negociación o una resistencia reales:

Subrepticamente, nuestra sociedad, en nombre del paradigma de la seguridad, se acostumbra al uso de marcadores biométricos y finalmente cada uno acepta, incluso con cierta indiferencia, ser fichado, observado, localizado, rastreado. En el plano de las mentalidades colectivas, se ha creado una suerte de habituación que ha ampliado los umbrales de tolerancia y ha hecho que muchos consientan, muchas veces sin siquiera darse cuenta, importantes abandonos de su esfera privada y de sus derechos fundamentales. Y ello no solo en relación con las técnicas de vigilancia y fichado, sino también de los instrumentos de medida y captación de las vivencias individuales por parte del complejo mediático y publicitario (Mattelart, 2007/2009, p. 252).

Por su parte, Staples (2000, p. 9) señala que la vigilancia actual se produce en culturas caracterizadas por la fragmentación y la incertidumbre, a medida que muchos de los significados, símbolos e instituciones de la vida moderna que alguna vez se dieron por sentados se disuelven ante nuestros ojos. Así, actualmente los sistemas de vigilancia tienen que ver más con tratar de controlar los flujos de información sobre los usuarios dentro de los nuevos medios de comunicación. Nos encontramos, pues, con formas de vigilancia ubicuas e imperceptibles que ejecutan la traslación de nuestra presencia a un mundo cada vez más digitalizado, esto es, a un mundo que ha sido datificado (van Dijck, 2014). La datificación es un concepto que se atribuye al funcionamiento de multitud de aplicaciones basadas en el registro y control de datos sobre nuestro cuerpo. Bajo él yace la creencia en el dataísmo (van Dijck, 2014), esto es, la convicción en la posibilidad de una cuantificación objetiva a través del seguimiento potencial de todo tipo de comportamiento humano, amén de la plena confianza en quienes recopilan y analizan nuestros datos. Estas convicción y confianza son muy relevantes en un mundo donde la

vigilancia utiliza grandes cantidades de datos que almacena y en algunos casos distribuye para cuestiones totalmente alejadas del motivo principal de su captura.

Como hemos visto, uno de los principales medios de generación de riqueza para la empresas que operan en Internet, es a través de la vigilancia de la población. La digitalización de la vigilancia ha cambiado radicalmente la naturaleza de la publicidad, el antiguo sistema en el cual los anunciantes compraban espacio publicitario o tiempo en los medios con la esperanza de que sus audiencias los percibiesen mientras buscaban noticias o entretenimiento ha quedado obsoleto. Los anunciantes cada vez necesitan menos subvencionar el periodismo o la producción de contenidos mediáticos para llegar a sus públicos objetivos, pues pueden identificarlos y localizarlos dondequiera que estén en línea —y a menudo también en el espacio físico— gracias a los sistemas de vigilancia ubicua. La premisa del sistema es que no haya privacidad efectiva.

Estas entidades corporativas, que a menudo se concentran en grandes monopolios, también cooperan con los sistemas de vigilancia de los Estados en los sectores militares, de inteligencia y policiales. El resultado es que el complejo militar-industrial se fortalece enormemente, en relación con el gobierno en su conjunto. Las alertadoras revelaciones como las de Edward Snowden sobre programas como Prism de la NSA, junto con otras filtraciones, han mostrado un patrón de entrelazamiento estrecho de los militares con corporaciones gigantes de Internet, creando lo que se ha llamado un «complejo militar-digital» (McChesney, 2014, pp. 158-171).

De hecho, según Foster y McChesney (2014, párr. 69), en el período 2005-2007, tanto los gastos de *marketing* como los gastos militares de EEUU ascendían a alrededor de 1000 millones de dólares al año cada uno; mientras que los gastos en finanzas, seguros y bienes raíces a aproximadamente 2500 millones de dólares. En la era digital, estos tres sectores de la economía, «cada uno de ellos surgió parasitariamente de la base de producción de la economía y se interconectaron cada vez más en una red de tecnología e intercambio de datos» (Foster y McChesney, 2014, párr. 69). A medida que las tecnologías más avanzadas (generalmente desarrolladas para el ámbito militar) se privatizaban, muchos de los involucrados en la economía bélica se encontraron en condiciones de explotar el conocimiento y las conexiones que habían obtenido al pasar al sector privado, siendo bastante sencillo el traspaso de un sistema de seguridad y vigilancia a otro.

Los automatismos, particularmente los algoritmos de procesamiento de datos, permiten el seguimiento continuo y la predicción de los comportamientos humanos. Este sesgo de anticipación es el sello de la cibervigilancia, además de ser uno de los rasgos distintivos que la diferencia de las formas más

convencionales de verificación de la conformidad de las normas. Se trata de anticipar las acciones de las personas en un afán por reducir riesgos o prever ofertas comerciales que supuestamente satisfacen sus necesidades futuras. «El tiempo inmediato y anticipativo de la cibervigilancia es un tiempo de automatismos que no deja más que un espacio reducido a la intervención humana» (Mattelart y Vitalis, 2014/2015, p. 200).

Los acuerdos político-económicos actuales en los que operan estos algoritmos significan pobreza para la mayoría global y producen alienación, represión, competencia y conflicto. En este contexto, la vigilancia actual sin duda contribuye a ello, en la medida en que reemplaza a la confianza, la categorización produce desventajas acumulativas y las personas son tratadas de acuerdo con sus caracterizaciones como datos abstractos e incorpóreos. Frente a la tendencia datificadora del sistema económico actual, en próximas secciones veremos cómo se desarrollan mecanismos de defensa y garantía de la autonomía humana.

2.2. Situando la privacidad

El término “privacidad” a menudo resulta complejo de comprender ya que con él se entretrejen diferentes conceptos relacionados con: la libertad de pensamiento, el control sobre el propio cuerpo, la soledad en el hogar, el control sobre la información personal, estar libre de vigilancia y la protección sobre nuestra reputación, así como frente a registros e interrogatorios. Ello ha llevado a que diferentes teóricos y filósofos encuentren una dificultad en el hecho de hallar una conveniente definición para la privacidad.

Si optamos por navegar por su desarrollo etimológico, encontraremos que su connotación antigua era negativa, “privacidad” y “privado” comparten etimología latina, “*privatio*” que significaba “quitar algo”, como en “privar”; o el adjetivo *privatus* que resultaba en algo “retirado de la esfera pública”. Lo privado se oponía a lo público, que era donde las personas desarrollaban su potencial. En este sentido, alguien que llevaba una vida completamente privada no se consideraba plenamente humana (Duby, 1988, citado en Véliz, 2024, p. 16):

El acto privado era el que se realizaba no en público, en el foro, ante los ojos de todos, sino dentro de la propia casa, en aislamiento, oculto a la vista de los demás. El sustantivo *privatum* se refiere a los recursos propios de una persona, a la propiedad para su propio uso; y, de nuevo, al hogar en privado, *ex privato*; dentro o fuera del hogar.

De esta manera, el sentido fundamental de lo público era el que poseía el pueblo como comunidad. Por el contrario, lo privado tenía la connotación de, por un lado, lo que se aparta de lo comunal y, por otro, lo que se relacionaba con la domesticidad. Más adelante, en el lenguaje románico, Véliz (2024, p. 17) encuentra un cambio en el significado de “privado” hacia lo “secreto” o lo “íntimo”. Así, relata que en la crónica *Roman de Rou*, escrita por Wace entre 1160-1170, los notables normandos que buscaban formas de evitar los impuestos que les imponían los francos se reunían en *privément*. Wace describe su reunión como una que se celebraba a puerta cerrada. Por lo tanto, la privacidad se asoció con reuniones secretas, que permitían a los conspiradores confabularse contra el poder gobernante. De nuevo, lo privado y lo público se consideraban fuerzas en conflicto, y las autoridades a menudo se sentían obligadas a detectar actividades privadas que podrían amenazar su poder (Duby, 1988, citado en Véliz, 2024, p. 17).

Si bien es cierto que las personas siempre hemos buscado privacidad para escapar de las cargas y los riesgos de la interacción social, refugiándonos en espacios de soledad y lejos de la mirada de los demás

para estar seguros y tranquilos, a veces renunciamos a dicha privacidad voluntariamente a cambio de otros bienes que valoramos —como cuando compartimos nuestros secretos con nuestros allegados. Sin embargo, para que no surja un conflicto con nuestro derecho a la privacidad, ha de darse una serie de contraprestaciones en las que desempeña un papel muy importante el consentimiento y una expectativa de confidencialidad por ambas partes.

En relación a la exclusiva consideración de la privacidad como perteneciente al entorno privado, si bien hubo un tiempo en que con cerrar la puerta de entrada de nuestra casa era posible aislarse del mundo exterior, en la era digital, el mundo y nuestras rutinas domésticas operan cada vez más a través de Internet. Este cambio no solo provoca que nuestros electrodomésticos tengan cada vez más la capacidad de monitorear nuestras actividades cotidianas, sino que la gran cantidad de notificaciones que los acompañan nos alejan de esa sensación de soledad y concentración que buscábamos en un principio.

En suma, el hecho de aceptar concepciones pasadas sobre qué es la privacidad puede generar el riesgo de creer en el mito de que la privacidad pertenece sólo a la esfera privada. En primer lugar, dicho riesgo procede de que con tal creencia estamos negando a las personas la privacidad en espacios públicos, concepto que a primera hora puede parecer un oxímoron (Lessig, 2006/2009, p. 322). Y en segundo lugar, al restringir la privacidad a la esfera privada tradicional, esto es, el interior de nuestros domicilios, en un momento en el que, con el advenimiento del Internet de las Cosas (IoT por sus siglas en inglés), hemos visto cómo se han erosionado seriamente, la privacidad podría terminar desapareciendo por completo.

Para conocer el significado de la privacidad en nuestros días, a lo largo de las siguientes líneas realizaré un recorrido sobre cuál es el valor de la privacidad, qué concepciones teóricas se han propuesto al respecto y con qué límites se han encontrado, para luego presentar la detallada «taxonomía de la privacidad» realizada por Solove (2009) sobre este término. Por último, me detendré en el concepto de «privacidad como integridad contextual» de Nissenbaum (2004, 2009) por resultar una teoría realmente esclarecedora de cara a acotar lo que suponen las lagunas de privacidad en el entorno digital y qué implicaciones entraña su protección.

2.2.1. El valor de la privacidad

Lo primero que debemos tener en cuenta es que la mayoría de los derechos y libertades no son absolutos, de ahí que, en el caso que nos ocupa, la privacidad pueda entrar en conflicto con otros valores fundamentales, como la libertad de expresión, la seguridad y la transparencia. Por lo que debemos realizar un análisis honesto y directo de por qué los intereses que ella representa son importantes y cómo deben equilibrarse con otros, ya que la privacidad no tiene un valor universal en todos los contextos.

De hecho, para varias académicas feministas, (Boling, 1996; DeCew, 1997; Olsen, 1993) la privacidad resulta problemática cuando se utiliza para ocultar el abuso y la opresión de las mujeres dentro del entorno doméstico. Estas autoras afirman que los hombres han dominado históricamente la esfera pública, mientras que las cuestiones ligadas a las mujeres, la familia y el hogar constituían la esfera privada. Las mujeres, al ser excluidas de la vida pública, sufrían la omisión o degradación en el discurso público de muchas de las cuestiones que les atañían, las cuales eran (des)consideradas como meros asuntos privados. Para Carole Pateman (1989, p. 121) la dicotomía entre lo privado y lo público oscurecería la sujeción de las mujeres a los hombres dentro de un orden aparentemente universal, igualitario e individualista. Es por ello que el feminismo trate lo personal como político con el objetivo de transformar esta visión (MacKinnon, 1989).

Esta crítica feminista respondería a la consideración por parte del liberalismo tradicional de la privacidad como un derecho que poseen los individuos y que está en tensión con la comunidad en general. Ahora bien, como indica Solove (2009, p. 89), la privacidad queda infravalorada si se limita a la individualización. En efecto, es habitual que la privacidad reciba una protección inadecuada al centrarse en compensar el daño emocional o de reputación individual sin tener en cuenta los efectos de la pérdida de privacidad en otros aspectos tan importantes como la libertad, la cultura, la creatividad, la innovación y la vida pública. Por ello, la privacidad no debe entenderse como un derecho individual que prevalece sobre el interés de la comunidad.

De hecho, para Richard Hixson (1987, p. 14), la privacidad depende de la sociedad para su existencia, entendiéndola como un legado social, y no como una posesión individual. De manera similar, Amitai Etzioni (1999, p. 196) sostiene que la privacidad es una “licencia social” que exime a una categoría de actos, pensamientos y emociones del escrutinio comunitario, público y gubernamental. Ambos autores enfatizan que la privacidad no puede verse en términos puramente individuales, sin la debida consideración por el bien común. De esta manera, Etzioni (1999, pp. 187-188) sostiene que el hecho de

que el derecho a la privacidad establecido en la ley la trate como algo que no tiene límites supone un error, dado que la privacidad no es un valor absoluto y no tiene prioridad sobre otros derechos o preocupaciones relacionadas con el bien común. Según él, el individualismo se ha extendido a costa del bien común, y las formulaciones sociales derivadas de ambos deben estar en equilibrio (Etzioni, 1999, p. 198).

A mi entender, el problema es que críticas como las de Hixson y Etzioni todavía asocian la privacidad con el individuo, a pesar de reconocer que el discurso sobre la privacidad ha ignorado el bien común y ha visto la privacidad como un derecho inherente al individuo. Por lo tanto, los ciudadanos continúan entendiendo la esfera privada como enemiga de la esfera pública debido a la asociación de la privacidad con el individuo y al supuesto conflicto entre éste y el bien común. La privacidad se considera aquí una forma de indulgencia individual a expensas de la sociedad, una forma de protección del individuo que va en contra de las necesidades más esenciales de la sociedad. Aunque estos teóricos comunitarios defienden tanto el bienestar individual como el común, con frecuencia no los integran; y de hecho llegan a presentarlos como sujetos a un conflicto irreconciliable. «Equilibrar los derechos individuales con las responsabilidades sociales y la individualidad con la comunidad» es la tarea de los comunitarios, según Etzioni (1999, p. 198).

Otra manera de entender mejor por qué la privacidad no debe entenderse únicamente como un derecho individual está en comprender cómo está definida por las normas sociales. La privacidad protege al individuo, pero no por algún valor inherente respecto a la personalidad del mismo sino debido a los beneficios que brinda a la sociedad.

Tal y como mencioné anteriormente, varias autoras feministas afirmaban que la privacidad históricamente había servido para excluir a las mujeres de la esfera pública, silenciar las discusiones sobre temas femeninos e ignorar las denuncias de abuso conyugal. Lo cierto es que, a pesar de su historia contaminada, académicas feministas señalan otras formas en que la privacidad puede aislar normas obsoletas de los motores de la reforma, haciendo que las mujeres puedan ver el gran valor que tiene la privacidad para ellas. De esta manera, Anita Allen (1988, p. 36) observa que la privacidad puede fortalecer las características relacionadas con la personalidad, la individualidad y la autodeterminación. Para Ruth Gavison (1992, p. 43), el verdadero problema no radicaría en la separación verbal entre lo público y lo privado, sino en las estructuras de poder que los manejan de manera injustificada. Por su parte, Judith DeCew (1997, p. 94) se contraargumenta a sí misma al sostener que disolver la distinción entre lo público y lo privado presenta riesgos porque puede otorgar al Estado de un “poder excesivo”.

De hecho, como veremos más adelante, la privacidad tuvo un papel fundamental en la lucha feminista en Estados Unidos a finales de la década de 1960, al abarcar la protección de la anticoncepción y el derecho al aborto. Además, debemos recordar que históricamente, las mujeres se han visto afectadas tanto por la falta de privacidad como por la imposición del ámbito privado como su lugar en la sociedad. Por lo tanto, a pesar de que la privacidad puede fortalecer las normas y otras formas de control social, también puede contribuir a liberar a las personas de ellas.

Debemos poner en valor entonces cómo la privacidad permite, por ejemplo, a las personas contemplar y discutir el cambio político, crear contracultura o participar en una crítica significativa de la sociedad. O cómo también permite la expresión creativa que a menudo no es posible dentro de las limitaciones de la vida pública (Westin, 1967, citado en Solove, 2009, p. 80). Las personas debemos tener la oportunidad de desarrollar nuestros puntos de vista, opiniones políticas y expresiones artísticas sin que se filtren prematuramente al mundo, donde juicios duros podrían condicionarlos o inhibirlos. El crecimiento y el desarrollo requieren experimentación y la oportunidad de cambiar las opiniones antes de hacerlas públicas. De igual manera, la privacidad permite a las personas hablar de forma anónima, fomentando una comunicación sólida sin temor a represalias. A continuación vamos a ver con más detalle asumiendo la categorización que emplea Véliz (2024, pp. 99-111), el modo en que la privacidad protege nuestro control sobre la autopresentación, nuestra reputación, nuestra autonomía, creatividad, seguridad, igualdad, justicia, bienestar y democracia.

El control sobre la autopresentación

Para Marmor (2015, pp. 3-4), solo la privacidad ofrece una medida razonable de control sobre las formas en que las personas pueden presentarse y mostrar a los demás quiénes son. De manera similar, el sociólogo Erving Goffman (1959) describe cómo este control resulta esencial para gestionar con éxito las relaciones profesionales y personales. En líneas similares, James Rachels (1975) señala que la capacidad de mantener diferentes tipos de relaciones está relacionada con el control sobre quién tiene acceso tanto a la identidad como a la información sobre uno mismo. En este sentido, Lessig (2006/2009, p. 351) afirma que:

Todos nosotros deseamos vivir en comunidades separadas, o entre o dentro de espacios normativos separados. La privacidad, o la capacidad de controlar la información sobre uno mismo, respalda dicho deseo, permitiendo la coexistencia de estas múltiples comunidades e inhabilitando el poder de una comunidad dominante para imponer sus normas sobre las demás. Pensemos, por ejemplo, en un hombre gay en una pequeña ciudad intolerante.

Podría parecer a primera vista que la era digital ha permitido a las personas tener un mayor control sobre su apariencia. Por ejemplo, uno de los principales objetivos de las redes sociales ha sido permitir que las personas cuiden la imagen de uno mismo que comparten con los demás. Sin embargo, los casos de *troleo* y humillación pública demuestran que nuestra influencia en las redes sociales es limitada (Véliz, 2022b). Las redes sociales nos hacen exponer cada vez más nuestra vida, competir con los demás y superar unas expectativas impuestas. Y cuando nos convertimos en el centro de atención de miles o incluso millones de personas, nuestro control sobre la autopresentación se ve gravemente afectado.

Por supuesto, más allá del uso de las redes sociales, existen empresas que se lucran extrayendo enormes cantidades de datos personales que les permiten obtener una imagen detallada de nosotros que escapa a nuestro control. De este modo, y sin que tengamos nosotros control sobre ello, estas organizaciones pueden inferir sobre nuestro poder adquisitivo, religión, tendencias políticas, estado de salud, o, lo que es peor, pueden compartir esa información con quien esté dispuesto a pagar por ella, sin que tengamos control sobre nuestra imagen personal. Semejante falta de control también entraña un impacto en nuestra reputación, tal y como explico a continuación.

Reputación

La privacidad, como sostiene Jeffrey Rosen (2000, p. 8), nos protege de que nos juzguen de manera incorrecta y fuera de contexto en un mundo en el que la capacidad de atención es limitada. Si bien construimos heurísticas de amplio alcance para evaluar rápidamente el carácter de las personas, éstas pueden dejar mucho que desear en cuanto a precisión e imparcialidad. Cualquier mancha en la historia de alguien puede ser un pretexto para excluirlo, incluso si es algo que no debería considerarse en un contexto específico. Los seres humanos falibles necesitan segundas oportunidades para mejorar, y la privacidad ayuda a desarrollar una especie de “olvido social” que hace que la sociedad sea más indulgente (Blanchette y Johnson, 2011, citado en Véliz, 2024, p. 102).

En este punto, las normas sociales juegan un papel importante para la privacidad porque ayudan a determinar en parte lo que debe mantenerse privado en una cultura y a disciplinar las interacciones sociales de una manera que proteja la privacidad. El deseo de buena reputación y aceptación social también juegan un papel importante en la motivación de las personas a aceptar las normas de privacidad. La necesidad de evitar el rechazo social tiende a pesar más que cualquier tentación que puedan tener las personas de invadir la privacidad de los demás, pues casi siempre existe el riesgo de ser descubierto, aunque esto no siempre se cumpla, dado que las mediaciones tecnológicas actuales modifican en gran medida esto, ampliando el rango y profundidad de prácticas de “percibir sin ser

percibido” y generando lo que Lessig en denomina “ambigüedades latentes” que nos fuerzan a debatir sobre principios (y no nos permiten aplicar los ya consensuados a la nueva situación) (Lessig, 2006/2009, p. 65). El interés de cada persona en que se respete su propio derecho a la privacidad sigue fomentando en gran medida el cumplimiento de las normas de privacidad. Como resultado, las normas sociales son esenciales para proteger la privacidad porque inspiran, complementan y respaldan las leyes.

Autonomía

Podemos definir la autonomía como la capacidad y el derecho de autogobernarse. Las personas adultas tenemos la capacidad de elegir qué es importante y significativo para nosotros y qué tipo de vida queremos tener y actuar de acuerdo con esos valores. Dicha capacidad de actuar racionalmente de un modo que responda a nuestros propios intereses es un componente crucial de la autonomía. Para Watson (2013, pp. 4-5) ser autónomo es ser capaz de reflexionar sobre sus propios valores, apoyarlos y actuar de acuerdo con ellos. Reconocer y honrar el poder de alguien sobre su propia vida es respetar su autonomía.

Aquí encontramos dos justificaciones para explicar por qué la privacidad es un requisito para la misma. De esta manera, Véliz (2024, p. 102) explica a través de dos argumentos por qué y cómo la privacidad es un requisito para la autonomía: el principio del respeto a las personas es la base del primer argumento, es decir, una persona autónoma tiene derecho a querer realizar una actividad sin ser observada. Por lo que observarla equivale a no respetar su autonomía, incluso si no se derivan consecuencias negativas de ese acto, e incluso también si la persona observada ni siquiera sabe que lo está siendo. Reconocer a alguien como una persona autónoma es reconocerlo como alguien que “elige”, lo que nos da una razón para respetar sus deseos. Espiar a alguien que no quiere ser observado no solo le niega lo que quiere (privacidad), sino que también significa cambiar lo que hace, lo que también es una forma de no respetar su derecho de elección. Por ejemplo, podría creer que está hablando con alguien en privado cuando en realidad no es así.

El segundo argumento que expone Véliz (2024, p. 102) explica la importancia de la privacidad para la autonomía centrándose en cómo la vigilancia impide el crecimiento y el mantenimiento de la autonomía. Para convertirnos en adultos autónomos y mantener esa autonomía, los seres humanos necesitamos tiempo y espacio lejos de la presión social. Ya que, en primer lugar, la pérdida de privacidad puede facilitar interferencias externas que frustran nuestra capacidad para vivir por nosotros mismos. Y en segundo lugar, la pérdida de privacidad nos lleva a limitar nuestra autonomía de manera autoimpuesta. La mayoría de las personas carecen de la capacidad moral para «soportar sin pestañear la

exposición constante a las críticas» (Benn, 1971). Tu visión de lo que haces puede verse alterada incluso si solamente te observan sin ser criticado, ya que la vigilancia provoca emociones autoconscientes, lo que puede dificultar la autonomía. Ser observado dificulta la tranquilidad mental, que es esencial para la toma de decisiones independientes, y nos empuja a actuar de la misma manera que los demás quieren hacer.

Pero, una vez más, la privacidad no solo protege a las personas, sino también a los modos de vida que mejoran su autonomía. Para Dorota Mokrosinska (2018, p. 20) la autonomía no solo está arraigada socialmente, sino también políticamente. Para esta autora, es crucial para la práctica de la justificación pública tener cierta cantidad de privacidad en el marco del liberalismo político. La justificación pública exige que, al tomar decisiones sobre leyes y políticas, debemos apelar a argumentos que puedan ser aceptados por todos. Ese compromiso limita lo que las personas deben llevar a la atención de los demás. Cuando protegemos la privacidad de otros, también protegemos formas saludables de compromiso político que promueven la autonomía.

El problema actual con la capacidad de autonomía de las personas tiene que ver con una des-alineación entre nuestros objetivos como individuos y como sociedad por un lado y los de las empresas tecnológicas por otro (Williams, 2018, pp. 8-9). Algunas empresas tecnológicas, al igual que ciertas agencias de seguridad, intentan saber más sobre nosotros para, en el caso de las corporaciones, poder exponernos a anuncios que nos inciten a hacer clic en ellos y comprar lo que anuncian, aunque también utilizan el conocimiento que tienen sobre nosotros para comprender nuestra psicología y “secuestrarla” (Zuboff, 2019/2020). Por tanto, se centran en maximizar la cantidad de tiempo que pasamos en sus plataformas y dispositivos, por eso diseñan sus productos para que sean lo más adictivos posible (Peirano, 2019).

Un argumento válido en este punto es que, dado que tenemos la libertad de desobedecer los consejos de las empresas tecnológicas, no deberíamos desconfiar tanto de ellos. Por ejemplo, como señala Véliz (2024, p. 188) podemos ignorar el camino que nos marca una aplicación de mapas y tomar una ruta diferente. Sin embargo, no debemos subestimar el impacto que la tecnología tiene en nosotros:

Además de diseñar los productos, las empresas tecnológicas también diseñan a sus usuarios influyendo en nuestro comportamiento. Como dijo Churchill, “damos forma a nuestros edificios y, después, nuestros edificios nos dan forma a nosotros”. A menudo nos sentimos abrumados y sobrecargados cognitivamente, y hacer lo que la tecnología sugiere es tan conveniente que resulta difícil detenerse, pensar en ello y resistirse a las sugerencias

persuasivas (Véliz, 2024, p. 188).

Ya he hablado en el subapartado *De la Digitalización a la Datificación* del apartado 2.1.3. de cómo los ordenadores y otros dispositivos similares nos resultan normalmente objetos de admiración y confianza. Para Véliz (2024, p. 189), incluso si no se enfrentasen a consecuencias negativas, resulta difícil para los que toman decisiones desafiar el consejo de una “IA”. Sin embargo, si decidiesen actuar en contra de su recomendación, aquellos que toman decisiones humanas podrían estar expuestos a más responsabilidad. Para ello, pone el ejemplo de si un médico desobedeciera a una “IA” y cometiera un error que resultase letal para un paciente. Para la autora es probable que se lo considerara menos culpable si la acción del médico hubiera estado en línea con la recomendación de la “IA”, lo que en sí mismo indica que creemos que la tecnología está tomando al menos parte de nuestra autonomía.

Creatividad

Para Véliz, (2024, p. 103), la privacidad, en relación con la autonomía, protege el pensamiento independiente y la creatividad, al brindarles a las personas espacios en los que pueden estar libres de presiones que les empujarían a conformarse a las normas hegemónicas. A su vez, permite que las personas hagan cosas que no harían en público por temor a lo que los demás puedan pensar de ellas, al igual que otorga la capacidad de aprender nuevas habilidades sin temor a ser ridiculizadas, así como de experimentar y probar ideas que tal vez no deseen apoyar en público después de haberlas pensado en privado.

Además, según Cohen (2013, p. 1906), la privacidad protege los procesos de juego y experimentación de los que surge la innovación, como contrapunto a los regímenes de vigilancia y modulación distribuidos de manera generalizada, con su afán por moldear las preferencias y el comportamiento individual de maneras que reducen la casualidad y la libertad de experimentación que hacen prosperar la innovación (Cohen, 2013, p. 1920). En este sentido, Reisz (2019) apunta hacia que existe una respuesta natural a una cultura de exposición, esto es, ser lo más aburrido posible. En este sentido, el aburrimiento no es la falta de entretenimiento, sino que las personas, los discursos, los libros y los proyectos aburridos no son paradigmáticos del tipo de contribución que mejora el mundo. Algo aburrido, tal y como complementa Véliz (2024, p. 193), suele ser entendido como algo que no es importante, no tiene implicaciones interesantes, no desafía el estado actual o no conduce al progreso. Si un argumento dice la verdad al poder y tiene implicaciones interesantes que impulsan el cambio y el progreso, entonces no es aburrido; pero en una sociedad vigilada puede ser peligroso, porque en la economía de datos a uno se le trata en función de éstos.

Seguridad

Lejos de lo que se puede pensar en un primer momento, existe una estrecha conexión entre privacidad y seguridad, y esto es sencillo de entender solo dándonos cuenta que cuanto más sepa alguien sobre ti, más vulnerable eres ante esa persona. Al hilo de esta cuestión Lessig (2006/2009, pp. 371-372) se apoya en las diferencias entre la falta de regulación en EEUU sobre la protección de la privacidad en contraposición a la normativa en cuestiones relativas a la propiedad intelectual:

He aquí lo que distingue la privacidad de la propiedad intelectual: que los individuos deberían estar capacitados para controlar la información sobre sí mismos. Deberíamos estar ávidos por ayudarles a proteger esa información, proporcionándoles las estructuras y los derechos para hacerlo. Todos valoramos, o deseamos, nuestra paz. Y por lo tanto, un régimen que nos facilita esa paz, otorgándonos el control sobre la información privada, es un régimen coherente con los valores públicos que las autoridades públicas deberían respaldar.

Hay un segundo modo, acaso más favorable, de defender esta misma idea. La propiedad intelectual, una vez creada, no constituye un bien rival: cuánta más gente la usa, más beneficiada se ve la sociedad. Por eso nos inclinamos por la compartición y la libertad en el contexto de la propiedad intelectual.

La privacidad, por el contrario, sí que se gasta con el uso: cuanta más gente esté autorizada a pisotearla, menos quedará de ella. En este sentido, la privacidad se asemeja más a la propiedad real que a la intelectual. Ninguna intrusión individual puede llegar a destruirla, pero su valor se reduce en cierta medida con cada nueva invasión.

Lo que demuestra que a menudo existe una relación entre privacidad y seguridad tal que cuanto menos se tiene de una, menos se tiene de la otra. De hecho, ya hemos visto antes cómo existe una relación entre información y poder: se considere el conocimiento como un instrumento de poder o como una forma de control sobre los demás en sí mismo (Foucault, 1975/2002, pp. 27-29), la vigilancia constituye una relación de poder en la que los observadores pueden utilizarla para ejercer control sobre sus objetivos. La vigilancia gubernamental aumenta el poder del Estado para controlar a la población y disminuye la protección que tienen los individuos contra las incursiones estatales, incluso si la vigilancia puede mejorar la seguridad contra el terrorismo, lo cual a veces puede resultar cuestionable (Véliz, 2023).

De hecho, no todas las medidas que mejoran la seguridad son en detrimento de la privacidad: a este respecto, Solove (2011, p. 34) pone de ejemplo uno de los muchos cambios de seguridad que se implementaron después de los ataques terroristas del 11-S, a saber, cerrar con llave las puertas de la cabina de mando de los aviones. Otro ejemplo lo encontramos en las diferentes pruebas que sugieren que las farolas son tan buenas para disuadir el crimen como las cámaras de vigilancia (Welsh y Farrington, 2004) así en la investigación transversal de Piza *et al.* (2019) que tras cuatro décadas llega a la conclusión de la ineficacia de las cámaras de videovigilancia en la prevención de crímenes violentos. En muchos otros casos, proteger la privacidad es una manera de proteger la seguridad, y el conflicto percibido se puede resolver mediante una mejor comprensión de las conexiones internas entre las dos.

Igualdad, justicia y bienestar

La pérdida de privacidad afecta a la igualdad de dos maneras. En primer lugar, ya hemos visto que la vigilancia es un acto de dominación, que coloca al observador en una jerarquía superior con respecto a la persona vigilada. Para Jonathan Wolff (1998), respetar a las personas como iguales significa confiar en ellas, y la confianza significa no hacer preguntas específicas que son insultantes, por lo que sería de esperar que nadie tuviera que someterse a exámenes intrusivos en una sociedad igualitaria.

En segundo lugar, también hemos asistido a cómo la pérdida de privacidad tiene un impacto en la igualdad de una manera más instrumental, esto sucede cuando los datos personales se utilizan para discriminar a las personas, chantajearlas y otros propósitos perjudiciales para la igualdad. Por lo tanto, no resulta sorprendente que las acusaciones de pérdida de privacidad hayan sido frecuentemente dirigidas contra la discriminación y el trato desigual (Lessig, 2009, pp. 354-358; Richards, 2022, p. 160).

Las personas que, por ejemplo, reciben asistencia social suelen estar sujetas a un intenso nivel de escrutinio, ya que no solo tienen que responder preguntas indiscretas, sino que también toleran visitas a domicilio y otros tipos de vigilancia. Los más desfavorecidos sufren el uso indebido de sus datos personales con más frecuencia que los más acomodados, y las personas que tienen menos poder tienen menos probabilidades de descubrir y cuestionar los usos indebidos de los datos. Por otra parte, las personas de bajos ingresos también tienen más probabilidades de ser el objetivo del *marketing* predatorio (O'Neill, 2016/2017). No es sorprendente, por tanto, que quienes pertenecen a los hogares con ingresos más bajos declaren sentirse más preocupados por su privacidad que las personas de los hogares con ingresos más altos (Byrne, 2019).

De manera más general, encontramos que los anuncios personalizados pueden ser discriminatorios al no ofrecer oportunidades a ciertos tipos de personas. Véliz (2024, p. 107) pone de ejemplo cómo en

marzo de 2019, el Departamento de Vivienda y Desarrollo Urbano de los Estados Unidos demandó a Facebook por impedir que algunos usuarios vieran anuncios de viviendas basándose en inferencias algorítmicas sobre la raza y otras características de los usuarios (Benner *et al.*, 2019, citado en Véliz 2024).

Por último, en relación con el bienestar, Véliz (2024, p. 108) sostiene que tener un espacio libre de intrusiones nos permite dedicar nuestro tiempo y energía como mejor nos parezca sin tener que preocuparnos por los demás o atender sus necesidades.

Y es que, aunque el desarrollo humano dependa de la interacción social, tener compañía cuando no la queremos puede ser una carga pesada. La salud mental de las personas se mejora al mantener un equilibrio saludable entre la sociabilidad y tener tiempo y espacio libres de la mirada de los demás. Mantener una cierta distancia del resto de vez en cuando nos permite relajarnos, ya que participar en interacciones sociales implica tener que cumplir con las expectativas y afrontar las responsabilidades constantemente. Para Gavison (1980, pp. 446-447), la privacidad nos permite concentrarnos al liberarnos de distracciones no deseadas.

Democracia

Los seres humanos tienden a conformarse más cuando están bajo la mirada constante de los demás, por lo que la privacidad es valiosa en la medida en que queremos incentivar el pensamiento independiente. Según Gavison (1980 p. 452), en el ámbito político la privacidad contribuye a la protección de las sociedades liberales, democráticas y pluralistas.

La privacidad protege también a los disidentes políticos, como activistas y denunciantes, cuando las democracias se erosionan y el desacuerdo con el poder se vuelve peligroso. Tener la posibilidad de protestar y resistir de forma anónima es esencial para defender los ideales democráticos cuando la defensa de una injusticia puede poner en peligro la vida de una persona o de sus seres queridos.

La privacidad es valiosa no sólo para nuestra vida personal, sino también para nuestra vida como ciudadanos: nuestra participación en la vida pública y comunitaria. Es difícil imaginar cómo la gente podría participar libremente en la vida pública sin cierto grado de control sobre su reputación y su vida privada. Por tanto, la privacidad es más que una necesidad o deseo psicológico, es una dimensión profunda de la estructura social. Además de proteger a las personas, la privacidad salvaguarda las relaciones entre personas, que son esenciales para la vida familiar, el compromiso social y las actividades políticas. De hecho, para Snowden (2019, pp. 433-434): «Cualquier Gobierno electo que dependa de la

vigilancia para mantener el control de una ciudadanía o que considere la vigilancia un anatema para la democracia ha cesado de ser una democracia de facto».

Conclusiones sobre el valor de la privacidad

El valor de la privacidad debe evaluarse sobre la base de sus contribuciones a la sociedad. La protección de la privacidad de manera individual no tiene por qué ser a expensas de la sociedad; de hecho, el valor de salvaguardar la privacidad de las personas debería estar justificado por sus beneficios sociales. No vivimos aislados, sino entre otros, y el compromiso social es una parte necesaria de la vida. Para John Dewey (1908/1978) el individuo está indisolublemente ligado a la sociedad, por lo que no podemos pensar en nosotros mismos excepto como, hasta cierto punto, seres “sociales”, como ya apuntaba también Aristóteles con su concepto de “zoon politikón” en su obra *Política* (Oviedo Sotelo, 2015, p. 51).

Por tanto, no podemos separar la idea de nosotros mismos y de nuestro propio bien de nuestra idea del bien de los demás. Dewey (1936/1995) argumentó también que los derechos individuales no necesitan justificarse como posesiones inmutables de los individuos; en cambio, son instrumentales a la luz de la contribución que hacen al bienestar de la comunidad. Empleando una idea similar, hemos visto cómo varios académicos también sostienen que la privacidad es constitutiva de la sociedad, por lo que los daños a esta se extienden más allá de la angustia mental causada a individuos particulares, al afectar la naturaleza de la sociedad y al impedir las actividades individuales que contribuyen al bien social mayor.

Por tanto, la privacidad no sólo es valiosa porque protege a las personas de daños como la discriminación y la humillación pública. También es valiosa colectivamente, en el sentido de que nos interesa vivir en una sociedad que proteja la privacidad de otras personas, ya que protege bienes como la igualdad, la libertad, la democracia y la seguridad, entre otros. En este sentido, el derecho a la privacidad tiene similitudes con el derecho de los periodistas a proteger sus fuentes. Como indica Raz (1988, p. 179), el interés de los periodistas en poder recabar información se considera digno de protección porque sirve al público, esto es, se valora por su utilidad para los miembros del público en general.

Nuestro interés en que se respete nuestro derecho a la privacidad no es, por tanto, distinto del de vivir en una sociedad en la que se respete el derecho a la privacidad de los demás. Raz (1995, p. 54) también expresa este sentimiento en referencia a la libertad de expresión. De la misma manera, podría ser mejor vivir en una sociedad que disfruta de la privacidad (y de sus bienes concomitantes, como la libertad y la democracia) que disfrutar de la privacidad en soledad.

Es por tanto el aspecto colectivo de la privacidad lo que la convierte en un derecho fundamental. En palabras de este autor, los derechos morales fundamentales no pueden concebirse como esencialmente en competencia con los bienes colectivos. Al examinarlos, se descubre que son un elemento de la protección de ciertos bienes colectivos o que su valor depende de la existencia de éstos (Raz, 1988, p. 254). Por su parte Lessig (2006/2009, p. 343) vincula la privacidad al poder como un principio que «no atiende ni a la preservación de la dignidad ni a la minimización de la intrusión, sino que la define en términos sustantivos —la privacidad como un modo de restringir el poder regulador del Estado», lo cual va más allá de la simple oposición (o negación de la misma) entre lo “colectivo” como “agobio” y lo “individual”.

2.2.2. Cómo se ha conceptualizado la privacidad a lo largo del tiempo

Si bien actualmente se reconoce la privacidad como un derecho universal, se considera que este derecho es relativamente moderno y tiene una clara visión occidental. Tal y como indica Véliz (2024, p. 18-19), aquellos que cuestionan la universalidad de la privacidad argumentan que en otras épocas y en otras culturas la privacidad no tendría el valor que nosotros le otorgamos hoy día. Para ello cita a autores como Lawrence M. Friedman (2007), el cual expresa que «la privacidad, como idea y realidad, es la creación de una sociedad burguesa moderna» (p. 258), o como, Vinton Cerf, uno de los arquitectos de Internet, el cual piensa que la privacidad surgió durante la revolución industrial (citado en Fernstein, 2013). Estos argumentos sostienen que, si de verdad la privacidad fuese un desarrollo cultural reciente y en otras culturas y épocas se hubiese vivido sin ella, sería relativamente sencillo prescindir de este derecho sin que supusiese un gran agravio.

Sin embargo, estas teorías quedan rebatidas por los diferentes estudios antropológicos e históricos a los que apunta Véliz (2024, pp. 16-28). Según ellos, si bien el concepto de privacidad efectivamente se ha ido ampliando debido en gran medida al avance de los tiempos, la necesidad de seguridad tanto de nuestras comunicaciones como de nuestros cuerpos y de las relaciones interpersonales ha estado presente a lo largo de los siglos de evolución tanto en la sociedad occidental como en otras culturas.

Como ilustración, Véliz apunta que, si bien aunque es ampliamente conocido que en el antiguo Imperio romano las letrinas eran lugares comunes, cuestión que pondría en entredicho la necesidad de privacidad de su sociedad, sí existen evidencias sobre la necesidad de esta población de mantener cierta información privada, lejos del conocimiento de otros, así como un férreo recelo sobre su correspondencia (Veyne, 1985/1992). En cuanto a la importancia de la privacidad en culturas distintas a la occidental, Véliz se apoya en los estudios de Barrington Moore (1984) sobre sociedades que viven

aisladas de otras poblaciones, como es el caso de los Utkuhikhalingmiut (Utku en su forma abreviada).

De este modo, pese a residir en las tierras inhóspitas del Círculo polar ártico canadiense, donde las condiciones climáticas les imponen amplios periodos de vida en espacios confinados (los iglús), está documentado que los Utku han desarrollado una serie de normas sociales para preservar la privacidad de sus integrantes dentro de su comunidad en estos acotados espacios donde la intimidad parece algo inasequible (Véliz, 2024, p. 24).

En resumen, lo que viene a demostrar la autora es que sí existe a escala global un deseo de buscar refugio de las imposiciones y riesgos de la interacción social, ya que, para sobrevivir y prosperar como individuos, debe existir un equilibrio entre privacidad y sociabilidad. Si bien las formas de encontrar espacios y tiempo para la privacidad también varían entre culturas, éstas parecen deberse más a diferencias contextuales que a diferencias culturales. Sobre la privacidad y el contexto hablaré más adelante, pero para que nos hagamos una idea sobre lo que eso significa ahora mismo, valga de ejemplo cómo una intromisión en la privacidad de una persona puede ser inofensiva en un contexto determinado mientras que puede causar un daño grave en otro. Es por ello que, por ejemplo, en algunas sociedades puede no suscitar preocupación que se conozca la religión que profesa un individuo, mientras que en otras deben preservar esta información puesto que puede ser peligroso exponerla, de esta manera se puede justificar que:

Parte de lo que hace de la privacidad un tema filosóficamente interesante es que su opuesto, la vigilancia, también es valioso. [...] Si la privacidad fuera valiosa y la vigilancia no, no habría dilemas éticos en relación con la privacidad. La privacidad se pone constantemente en tela de juicio sólo porque podemos obtener beneficios de la vigilancia y la exposición (Véliz, 2024, p. 112).

Al igual que ocurre con el caso de la evolución de la vigilancia a lo largo de la historia, de nuevo veremos que el avance de las técnicas de control y registro supuso una serie de cambios en relación a la concepción de la privacidad. Así, el desarrollo de las tecnologías de la comunicación trajo también al debate público nuevas cuestiones relativas a la protección de la privacidad de las comunicaciones. Prueba de ello lo encontramos en la aparición del telégrafo eléctrico a mediados del siglo XIX, que para McMullan (2015) supuso un cambio en la percepción de la civilización sobre el alcance de la privacidad de las conversaciones cotidianas. En efecto, si bien antes dicho alcance estaba limitado por la capacidad humana de escucha directa, con este invento la idea de lo que estaba “fuera del alcance perceptible” cambió inexorablemente por mediaciones tecnológicas.

A medida que se expandía este nuevo espacio de comunicación surgió una nueva vulnerabilidad relativa a que ahora se podían intervenir líneas telegráficas e interceptar señales, aunque vulnerabilidad radicaba en que las claves de emisor o receptor fueran capturadas. Y, aunque los trabajadores de las líneas de cable estaban obligados a firmar acuerdos de confidencialidad, podían ser sobornados para que se filtrase la información. Con la expansión del telégrafo, también lo hizo la idea de la privacidad en las conversaciones. «A principios del siglo, los usuarios comerciales estaban preocupados por la privacidad y, por lo tanto, las compañías de cable querían asegurarse de que todo lo que se enviaba por cable era seguro» (Packer, citado en McMullan, 2015, párr. 11).

Para finales del siglo XIX, el telégrafo eléctrico había evolucionado hasta convertirse en la tecnología dominante y la primera de comunicación masiva. La seguridad de las telecomunicaciones se había extendido por todo el mundo, pero hizo falta que apareciese una tecnología rival, la radio, para que la privacidad de las comunicaciones se articulase plenamente como un concepto dentro del imaginario público. A lo largo de una generación, la gente pasó de preocuparse por lo que oídos ajenos pudieran escuchar a enfrentarse a la posibilidad de interceptaciones globales a través de sofisticados sistemas de comunicación electrónica. Sin embargo, como veremos, fue el desarrollo de otro tipo de tecnología lo que propulsó el nacimiento de la primera teoría sobre el reconocimiento legal del derecho a la privacidad.

Sin embargo, para Solove, (2009, p. 14) la mayoría de los intentos por conceptualizar la privacidad han seguido un método tradicional de definición *per genus et differentiam*, es decir, delimitando primero el *genus* (las normas) para luego identificar la *differentia* específica de principios y reglas de conducta. En otras palabras, los teóricos han tendido a buscar un conjunto común de elementos necesarios y suficientes para distinguir la privacidad de otras concepciones.

Aunque las terminologías que se emplean en las diferentes teorías pueden diferir, la mayoría de los teóricos se esfuerzan por localizar algo así como la esencia de la privacidad, esto es, el denominador común central que hace que las cosas sean privadas. El método tradicional intenta conceptualizar la privacidad construyendo una categoría que esté separada de otras categorías conceptuales (como la autonomía de la libertad) y que tenga límites fijos y claros para que podamos saber cuándo ciertas cuestiones estarían dentro o fuera de esta categoría. En última instancia, el problema surge del hecho de que los teóricos están intentando conceptualizar la privacidad tratando de aislar sus características centrales. A continuación presento una breve recopilación a través de los estudios de Solove (2009, pp. 12-38) y Véliz (2024, pp. 47-74) de estas teorías y los límites conceptuales que plantean.

El derecho a ser dejado en paz

En 1890, el abogado Samuel D. Warren (1852-1910) y el juez Louis Brandeis (1856-1941) escribieron *The Right to Privacy* [*El Derecho a la Privacidad*], que supuso el primer intento teórico de exponer la naturaleza y la importancia de este principio y de defender su reconocimiento legal como el “derecho a ser dejado en paz” (*the right to be let alone*, en su idioma original).

Warren y Brandeis describían cómo los nuevos desarrollos tecnológicos que estaban teniendo lugar representaban una amenaza potencial al “derecho a la vida”, a disfrutar de la vida, dotándolo de nuevos contenidos, entre los cuales veían urgente, incidir en que en ese momento el disfrute de la vida no era solo el evitar la amenaza directa de muerte (aquel “dejar vivir” que Foucault definía como divisa del poder soberano). Tal y como afirman:

En aquel entonces, el “derecho a la vida” sólo servía para proteger al sujeto de la agresión en sus diversas formas [...] Más tarde, se llegó al reconocimiento de la naturaleza espiritual del hombre, de sus sentimientos y de su intelecto. Poco a poco, el alcance de estos derechos legales se amplió; y ahora el derecho a la vida ha llegado a significar el derecho a disfrutar de la vida (Warren y Brandeis 1890, p. 193).

Y lo ejemplificaron a través de cómo las empresas de fotografías instantáneas y la prensa habían invadido los “recintos sagrados” que suponían la vida privada y doméstica, ya que estos nuevos dispositivos mecánicos amenazaban con hacer realidad el vaticinio de que «lo que se susurra en el armario se proclamará desde los tejados» (Cooley, citado en Warren y Brandeis, 1890, p. 195).

Debemos tener en cuenta que en sus inicios la fotografía era practicada en gran medida por profesionales, ya que las cámaras eran grandes, costosas y su instalación requería mucho tiempo. Sin embargo, en 1888, la Eastman Kodak Company desarrolló una nueva serie de cámaras fotográficas más pequeñas y baratas que permitían a cualquiera convertirse en fotógrafo. De hecho, un año antes de que Warren y Brandeis publicaran su artículo, la fotografía se había vuelto tan popular que los periódicos la calificaban como «una gran moda» (Gerety, 1977, p. 263).

A Warren y Brandeis no solo le preocupaban estas tecnologías, sino la repercusión que suponía su uso por parte de los medios de comunicación de la época, con la vista especialmente puesta en una prensa amarillista y sensacionalista cuyos reporteros gráficos tomaban fotografías de manera invasiva y difundían molestos cotilleos sobre diferentes personas, entre las que se contaba el propio Warren (Véliz, 2024, p. 48). Estos autores sostenían que la privacidad estaba arraigada en la cultura y que evolucionaba como respuesta a los avances sociales y tecnológicos. Argumentaban que «los cambios

políticos, sociales y económicos implican el reconocimiento de nuevos derechos» y que las leyes debía evolucionar para «satisfacer las demandas de la sociedad» (Warren y Brandeis, 1890, p. 193). Para estos autores la privacidad estaba íntimamente relacionada con el hecho de que a uno lo dejen en paz.

Esta visión consideraba la privacidad como un tipo de inmunidad al aislamiento, si bien la definición resultante es considerada demasiado amplia por Solove (2009, p. 18). Además, como sostiene Véliz (2024, p. 49), dejar a alguien en paz no es suficiente para que se conserve su privacidad, como sucede, por ejemplo, cuando se despliegan métodos de vigilancia de los que la víctima no es consciente. En este sentido, la autora explica que podría parecer que si no tocáramos a la persona ni nos acercáramos a ella, sino que nos limitáramos a observar remotamente todas sus actividades (en Internet, por ejemplo), la estaríamos dejando sola, en el sentido de que la dejamos hacer lo que quiera sin interferencias; sin embargo, para Véliz no cabe duda de que al mismo tiempo estaríamos invadiendo su privacidad.

La privacidad como un acceso limitado a uno mismo

Al tiempo que se publicaba el artículo de Warren y Brandeis, un conocido escritor de finales del siglo XIX, Edwin L. Godkin, publicó un artículo en el que señalaba que la privacidad constituía el derecho a decidir cuánto conocimiento de los pensamientos y sentimientos de una persona, así como de sus actos y asuntos privados, debe tener el público en general (Godkin, 1890, p. 65). De hecho, para Turkington y Allen (1999, pp. 40-41) este artículo tuvo una gran influencia en el escrito por Warren y Brandeis.

Esta conceptualización de la privacidad como un “acceso limitado” a uno mismo reconoce el deseo del individuo de ocultarse y estar apartado de los demás, lo cual lo relaciona estrechamente con la concepción del derecho a ser dejado en paz. Semejante visión del “acceso limitado” puede considerarse incluso una formulación más sofisticada de la misma, ya que las teorías que se derivan de ella van más allá de la soledad, al abarcar, por ejemplo, la libertad frente a interferencias del gobierno, así como frente a intrusiones tanto de la prensa como de otras personas. De tal modo, estas concepciones sobre el “acceso limitado” reconocen que la privacidad va más allá del mero hecho de estar apartado de los demás (Solove, 2009, p. 19).

Sin embargo, para Solove (2009 p. 20), sin una noción de qué asuntos son privados, las concepciones sobre el “acceso limitado” no determinan qué cuestiones resultan sustantivas y qué modo de acceso implicaría una violación de la privacidad. Ciertamente, no todo acceso a uno mismo infringe nuestra privacidad, sólo el acceso relacionado con dimensiones específicas sobre nuestra persona o con asuntos e informaciones particulares. Para Solove, entre la falta absoluta de acceso a uno mismo y el acceso total, la pregunta importante es dónde deben trazarse los límites: es decir, ¿qué grado de acceso

debemos reconocer como razonable? Al igual que la concepción del derecho a ser dejado en paz, la concepción del acceso limitado adolece de ser demasiado amplia y vaga. En líneas similares, Lessig (2006/2009, p. 372), argumenta que:

Puede haber hechos acerca de nosotros mismos que no se nos permita ocultar; y más importante aún, puede haber afirmaciones acerca de nosotros mismos que no se nos permita formular (“soy abogado” o “llámeme, soy médico”). No debería permitirse que incurriéramos en fraude o que perjudicáramos a los demás. Esta limitación es análoga al “uso justo” de la propiedad intelectual —un límite al espacio que puede proteger la privacidad.

La privacidad como secreto

Una de las concepciones más comunes acerca de la privacidad es que constituye el hecho de mantener ciertos asuntos en secreto. Según esta perspectiva, la privacidad se viola mediante la divulgación pública de información que previamente estaba oculta. Entenderla desde esta perspectiva supondría tratar la concepción de la privacidad como un subconjunto de la teoría relacionada con el acceso limitado a uno mismo, ya que mantener la información personal en secreto es una forma de limitar el acceso a ella.

Pero este concepto resultaría incluso más limitado que el anterior, ya que el secreto cubre sólo un aspecto del acceso personal: la ocultación de la información personal. En suma, entender la privacidad como secreto puede suponer un problema, ya que privado y secreto no siempre son términos coextensivos, es decir, no toda la información que es privada es información secreta. Sobre esto, Véliz (2024, p. 63) pone el ejemplo de nuestra información genética, la cual, sin ser un secreto —dado que uno pueda tener conocimiento de ella o no—, sí que resulta privada.

Además, esta concepción no reconoce que los individuos puedan querer mantener cierta información en privado para algunas personas pero no para otras. En otras palabras, a veces no queremos que algo sea un secreto universal; más bien deseamos confidencialidad, que consiste en compartir la información con un grupo selecto de personas que son de nuestra confianza. El libro que leemos, los productos que compramos y las personas con las que nos asociamos a menudo no son secretos, pero aun así los consideramos asuntos privados (Solove, 2009, p. 24). Sobre esto, es interesante retomar las tesis de Lessig (2006/2009) anteriormente mencionadas donde apuntaba al concepto de “privacidad comparada”, donde a través de los célebres conceptos de “no exclusividad” y “no rivalidad” que permiten discernir la “propiedad intelectual” de la propiedad física que se toma como paradigmática,

éste autor les da la vuelta para introducir matices clave en torno a que la privacidad no va (o no solo) de secretos.

La diferencia radica en los principios subyacentes que dan forma sustancial, o deberían hacerlo, a la información en cada contexto. En el contexto de la propiedad intelectual, deberíamos inclinarnos por la libertad. [...] deberíamos interpretar el acuerdo al que la ley llega con los titulares de derechos de autor de la forma más restrictiva posible. [...] Ahora bien, la información personal (al menos algunos tipos de ella) debería tratarse de forma diferente. Nadie llega a un acuerdo con la ley con respecto a la información personal o privada; y la ley no nos ofrece un derecho de monopolio a cambio de que publiquemos esta información (Lessig, 2006/2009, p. 371)

El control sobre la información personal

Al igual que con lo relativo a los secretos, Solove (2009, pp. 25-29) considera la visión de la privacidad ligada al control sobre la información como un subconjunto de la concepción del acceso limitado. Más allá, el hecho de que esta teoría se enfoque solo sobre la información la hace demasiado acotada, ya que no incluye aspectos relativos a la privacidad como pueden ser el derecho a tomar decisiones sobre el propio cuerpo, la reproducción o la crianza de los hijos. Además, resulta demasiado vaga al no definir los tipos de información sobre los cuales deberíamos tener tal control. Por otro lado, no debemos perder de vista que la privacidad no es simplemente una cuestión subjetiva de prerrogativa individual, también es una cuestión de qué considera la sociedad apropiado proteger.

Además de no definir adecuadamente el alcance de la información, las concepciones del control sobre ella tampoco logran definir qué se entiende por dicho “control”. Aunque frecuentemente se entienda como una forma de propiedad de la información (Lessig, 2006/2009, 366-370), concebir la información personal de tal modo se justificaría al considerarla como una extensión de la personalidad: como autores de nuestras propias vidas, generamos información a medida que desarrollamos nuestra personalidad. El crecimiento del individualismo generó la «creencia de que las acciones de uno y su historia “perteneían” al yo que las generó y debían ser compartidas sólo con aquellos con quienes uno deseaba hacerlo» (Shils, 1966, p. 290).

Sin embargo, ampliar el concepto de propiedad a la información personal presenta dificultades. La información se puede transmitir fácilmente y, una vez conocida por otros, no se puede erradicar de sus mentes. Esto lo ilustra de manera muy acertada también Lessig (2006/2009, pp. 294-295) con la

siguiente cita de Thomas Jefferson de 1814:

Si la naturaleza ha creado alguna cosa menos susceptible que todas las demás de ser objeto de propiedad exclusiva, ésta es la acción del poder del pensamiento que llamamos idea, la cual sólo puede poseer un individuo si la guarda para sí; pero en el momento en que se divulga, se fuerza a sí misma a estar en posesión de todos, y su receptor no puede desposeerse de ella.

A diferencia de los objetos físicos, la información puede poseerse simultáneamente en la mente de millones de personas. Esta es la razón por la cual la ley de propiedad intelectual protege expresiones tangibles particulares de ideas en lugar de las ideas subyacentes en sí mismas. La complejidad de la información personal es que es a la vez una expresión de uno mismo y un conjunto de hechos: un registro histórico de nuestro comportamiento.

A su vez, existen problemas a la hora de considerar la información personal como equivalente a cualquier otro bien. La información personal a menudo se forma en las relaciones con otros, por lo que todas las partes de esa relación pueden reclamar algún derecho sobre la información que se genera. Junto a ello, a menudo el valor de mercado de la información no es creado exclusivamente por el trabajo del individuo con quien se relaciona, sino en parte por el tercero que compila la información (Miller, 1971, p. 213). Por ejemplo, el valor de la información personal para los anunciantes y especialistas en *marketing* surge en parte de la consolidación y categorización de dicha información.

Algunos teóricos critican también la concepción del control sobre la información ya que se centra demasiado en la elección individual. Paul Schwartz (1999, p. 1661) sostiene que es un error suponer que los individuos tienen autonomía para ejercer control sobre sus datos personales en todas las situaciones, pues ello no reconoce «que la autodeterminación individual está determinada por el procesamiento de datos personales». Schwartz (1999, pp. 1661-1664) también cuestiona la suposición de que los individuos somos capaces de ejercer decisiones significativas con respecto a nuestra información, dadas las disparidades en el conocimiento y poder de negociación sobre la transferencia de nuestra información. En esta línea, la privacidad implicaría no sólo el control individual, sino también la regulación social de la información. Por ejemplo, Anita Allen (1999) sostiene que la privacidad no es simplemente una cuestión de elección individual sino que en ciertos casos debe ser “forzada” por el gobierno. En otras palabras, la privacidad es un aspecto de la estructura social, una arquitectura de regulación de la información, no sólo una cuestión de ejercicio de control individual. Sobre esta idea, podemos apoyarnos en Lessig (2006/2009, p. 265), sobre los límites de elección:

Una clase de legislación está diseñada para limitar la libertad individual. Del mismo modo que la legislación laboral prohíbe ciertos contratos de trabajo, o que la legislación de los consumidores veta determinados acuerdos de crédito, esta clase de legislación de privacidad restringiría la libertad individual de revelar ciertos aspectos de su vida privada. El motivo de esta limitación podría ser sustantivo o procedimental —sustantivo en cuanto que refleja un juicio sustantivo acerca de opciones que los individuos no deberían elegir; o procedimental en cuanto que refleja la opinión de que, al enfrentarse a esta elección, los individuos elegirán sistemáticamente de tal modo que luego se lamentarán. En uno u otro caso, el papel de este tipo de regulación de privacidad es bloquear las transacciones susceptibles de debilitar la privacidad en el seno de una comunidad.

Privacidad como forma de proteger la personalidad

Otra teoría que destaca Solove (2009, pp. 29-34) es aquella que ve la privacidad como una forma de proteger la personalidad, esto es, esa diferencia individual que constituye a cada persona y la distingue de otra. Fue formulada por primera vez por Paul Freund (1975), quien hizo uso de este término para referirse a «aquellos atributos de un individuo que son irreducibles a su identidad» (citado en Craven, 1976, p. 702).

Esta teoría difiere de las otras analizadas anteriormente porque se construye en torno a un fin normativo de la privacidad, a saber, la protección de la integridad de la personalidad. Aunque es independiente de las otras teorías, a menudo, se utilizan conjuntamente para explicar por qué la privacidad es importante, qué aspectos de uno mismo deberían limitarse o sobre qué información deberíamos tener control.

Pero, ¿qué aspectos de la personalidad protegería la privacidad? Según Edward Bloustein (1964), la privacidad, como concepto unificado y coherente protege contra conductas que «degradan la individualidad» (p. 389), «son una afrenta a la dignidad personal» (p. 973) o un «ataque a la personalidad del individuo» (p. 974). Por su parte, el filósofo Jeffrey Reiman (1976) también reconoce un componente de la personalidad en la privacidad: «El derecho a la privacidad [...] protege el interés del individuo en convertirse, ser y seguir siendo una persona» (p. 314). Por su parte, Stanley Benn (1971) sostiene que la vigilancia restringe la gama de opciones de un individuo y por lo tanto, limita su libertad. En consecuencia, la privacidad tiene que ver con el respeto a la personalidad, definida en términos de la capacidad del individuo para elegir.

Sin embargo, las teorías de la privacidad como forma de proteger la personalidad no logran dilucidar qué es la privacidad porque, a menudo, no articulan una definición adecuada de la personalidad, resultando en muchas ocasiones demasiado amplias. Además, no podemos asegurar que nuestras personalidades son puramente privadas ya que, en multitud de ocasiones, expresamos con facilidad en público mucho de lo que sería exclusivo de uno mismo (Solove, 2009, p. 31).

Privacidad como intimidad

Teóricos como Robert Gerstein (1978) o Julie Inness (1992) entienden la privacidad como una forma de intimidad. Estas teorías reconocen apropiadamente que la privacidad es esencial no sólo para la realización individual, sino también para las relaciones humanas, ya que consideran que la privacidad consiste en alguna forma de acceso limitado al control, y sitúan el valor de la privacidad en el desarrollo de las relaciones personales.

Como formamos relaciones con diferentes grados de intimidad y autorrevelación, valoramos la privacidad para poder mantener dichos niveles deseados de intimidad en cada una de nuestras relaciones. Al centrar el valor de la privacidad en su orientación a las relaciones interpersonales, la teoría de la privacidad como intimidad intenta definir a qué aspectos de la vida deberíamos poder restringir el acceso, o qué información deberíamos poder controlar o mantener en secreto. Sin embargo, de nuevo estas teorías resultan demasiado acotadas, por centrar su atención exclusivamente en las relaciones interpersonales y los sentimientos particulares que ellas engendran. Aunque la privacidad facilita la confianza, el amor y la intimidad, estos no son los únicos fines de la privacidad. Como señala Judith DeCew (1997), la información sobre nuestras finanzas es privada pero no íntima. Además, el valor de la privacidad no reside exclusivamente en el desarrollo de relaciones humanas íntimas. La intimidad captura la dimensión de la vida privada que consiste en relaciones cercanas con los demás, pero no captura la dimensión de la vida privada que se dedica únicamente a uno mismo.

Conclusiones sobre los intentos de conceptualizar la privacidad

Aunque las concepciones descritas profundizan en ciertas dimensiones de la privacidad y contienen muchas ideas interesantes, decantarse por solo una de ellas daría como resultado una explicación reducida o demasiado vaga de la misma. Por otro lado, encontrar un denominador común lo suficientemente amplio como para abarcar casi todo lo que involucra la privacidad correría el riesgo de ser demasiado inclusivo o demasiado ambiguo, mientras que su excesivo acotamiento correría el riesgo de ser demasiado restrictivo.

Debido a estas dificultades, algunos teóricos, conocidos como “reduccionistas”, sostienen que la privacidad se puede reducir a otras concepciones y derechos. La defensora más destacada de esta perspectiva es la filósofa Judith Thomson (1975), quien afirma que el derecho a la privacidad se superpone a otros derechos. Según la autora, el derecho a la privacidad no es un conjunto de derechos diferenciados, sino que se entrecruza con el conjunto de derechos que constituyen el derecho de la persona y también con el conjunto de derechos que constituyen la posesión de bienes (pp. 272-284).

Sin embargo, los reduccionistas dan por hecho sin justificación suficiente que la privacidad deriva de otras concepciones más primarias y no al revés. Aunque la privacidad se superpone con otras concepciones, lo cierto es que revela ciertas dimensiones de la experiencia que no son captadas de la misma manera por ellas. Además, las cuestiones relativas a la privacidad son demasiado diversas como para reducirlas meramente a los derechos sobre la persona y la propiedad. Sobre ello, Thomas Scanlon (1975) sostiene que:

no se puede obtener mucha información sobre los problemas que plantea la vigilancia electrónica o los conflictos entre las consideraciones de privacidad y las exigencias de una prensa libre consultando los derechos de propiedad o incluso los derechos de la persona en la forma en que Thomson los presenta (p. 322).

Otros autores, debido a la dificultad de proponer una definición satisfactoria de la privacidad, se han decantado directamente por no definirla. Así, por ejemplo, Annabella Lever (2012, p. 7) llega a afirmar que desestima defender una definición particular de privacidad, puesto que para ella es más importante entender el terreno filosófico que se ve involucrado en su proceso de entendimiento. A pesar de que este posicionamiento puede resultar atractivo, puesto que más o menos todos tenemos una noción intuitiva de lo que se considera privacidad, la falta de una definición concisa puede convertirse en un obstáculo para la reflexión sobre las consecuencias de la carencia de privacidad.

Para Véliz (2024, p. 73) el problema de la falta de límites a la hora de definir la privacidad se extiende a la ética. La forma en que definimos la privacidad tiene un impacto en lo que creemos que debería protegerse mediante ella. Si no hay forma de seleccionar qué tipos de cuestiones pertenecen al concepto de privacidad, no tendremos ni idea de qué tipos de asuntos deberían protegerse.

Renunciar a nuestra privacidad les da a otras personas poder sobre nosotros, nos hace vulnerables. Si bien es cierto que en ocasiones esa vulnerabilidad supone un gesto de confianza frente al otro con el objetivo de fortalecer la relación, existen otras formas de entrega de privacidad en las que el otro deja de ser un cuerpo en el que confiar, adquiriendo la indeseable potestad de almacenar la información que

se le otorga para transformarla con fines diferentes a los que nosotros aceptamos en un primer momento y que, además, afectan negativamente a la privacidad de los demás.

2.2.3. Taxonomía de la privacidad

¿Es posible definir entonces la privacidad de una manera que abarque todos los aspectos que ella engloba sin resultar por ello demasiado vaga? Para Solove (2009, p. 9), la clave se encuentra en poner el foco de su definición en los problemas a los que se enfrenta. Para ello desarrolla una teoría basada en un método diferente al tradicional de conceptualización de la privacidad, en favor de la idea de “semejanza familiar” de Ludwig Wittgenstein (citado en Solove, 2009, p. 9). Según el filósofo vienés, ciertos conceptos no tienen por qué tener una característica común única, sino que más bien se nutren de un conjunto de elementos similares. De esta manera, la privacidad no se definiría a través de un denominador común de todas las cuestiones que vemos bajo ella, sino que debería entenderse de manera pluralista: no tanto como una sola cosa, sino como un conjunto de elementos distintos pero relacionados entre sí.

Y es que, para Solove, el uso del término general “privacidad” puede dar lugar a una combinación de diferentes tipos de problemas y puede llevar a una comprensión de su significado que distraiga a los tribunales y a los encargados de formular políticas que aborden estas cuestiones. Sin embargo, añade, no es casualidad que se haga referencia a varias cuestiones bajo el título de “privacidad”, ya que todas ellas presentan similitudes sustanciales entre sí. Según Solove, estas analogías entre diferentes elementos podrían ser útiles e instructivas, en la medida en que se podría intentar crear leyes y políticas similares para regularlas. Por ende, deberíamos clasificar a algún asunto como involucrado en la “privacidad” cuando se asemeja a otros que clasificamos de la misma manera. Sin embargo, no se debe confundir similitud con igualdad, y también debemos reconocer dónde divergen muchas cuestiones relacionadas a lo que llamamos “privacidad”:

Los puntos de unión estarían entonces en los problemas que se derivan de la falta de privacidad, es decir, cuando las actividades de gobiernos, empresas, organizaciones y otras personas perturban nuestra actividades. En este punto surge un conflicto de intereses, puesto que, en algunas ocasiones, estas actividades pueden llegar a ser tan valiosas para el bien común como la propia privacidad. Como hemos visto anteriormente, se trata de aspectos relacionados con la seguridad, el censo o la necesidad de tener cierta información personal sobre un individuo para desarrollar correctamente ciertas actividades en el entorno laboral. Las protecciones sobre la privacidad deberían abordar una red de problemas interconectados que impiden el correcto desempeño de actividades específicas y, en consecuencia, el

acto de conceptualizarla debería consistir en mapear la topografía de esta red (Solove, 2009, p. 74).

Para ello, Solove desarrolla una «taxonomía» (Solove, 2009, pp. 101-171) en la que diferencia cuatro grupos básicos de actividades perniciosas para la privacidad: la recopilación de la información, el procesamiento de dicha información, su diseminación y, por último, la invasión de la privacidad. Sobre decir que en este contexto, con información el profesor de la Universidad George Washington se refiere a información personal. A cada grupo le asigna a su vez una serie de subgrupos relacionados con estas actividades nocivas.

La manera en la que el autor ha organizado estos grupos corresponde a un interés principal por los individuos cuyas vidas se ven directamente afectadas por las actividades clasificadas en la taxonomía. De manera esquematizada la taxonomía que propone Solove quedaría de la siguiente manera:

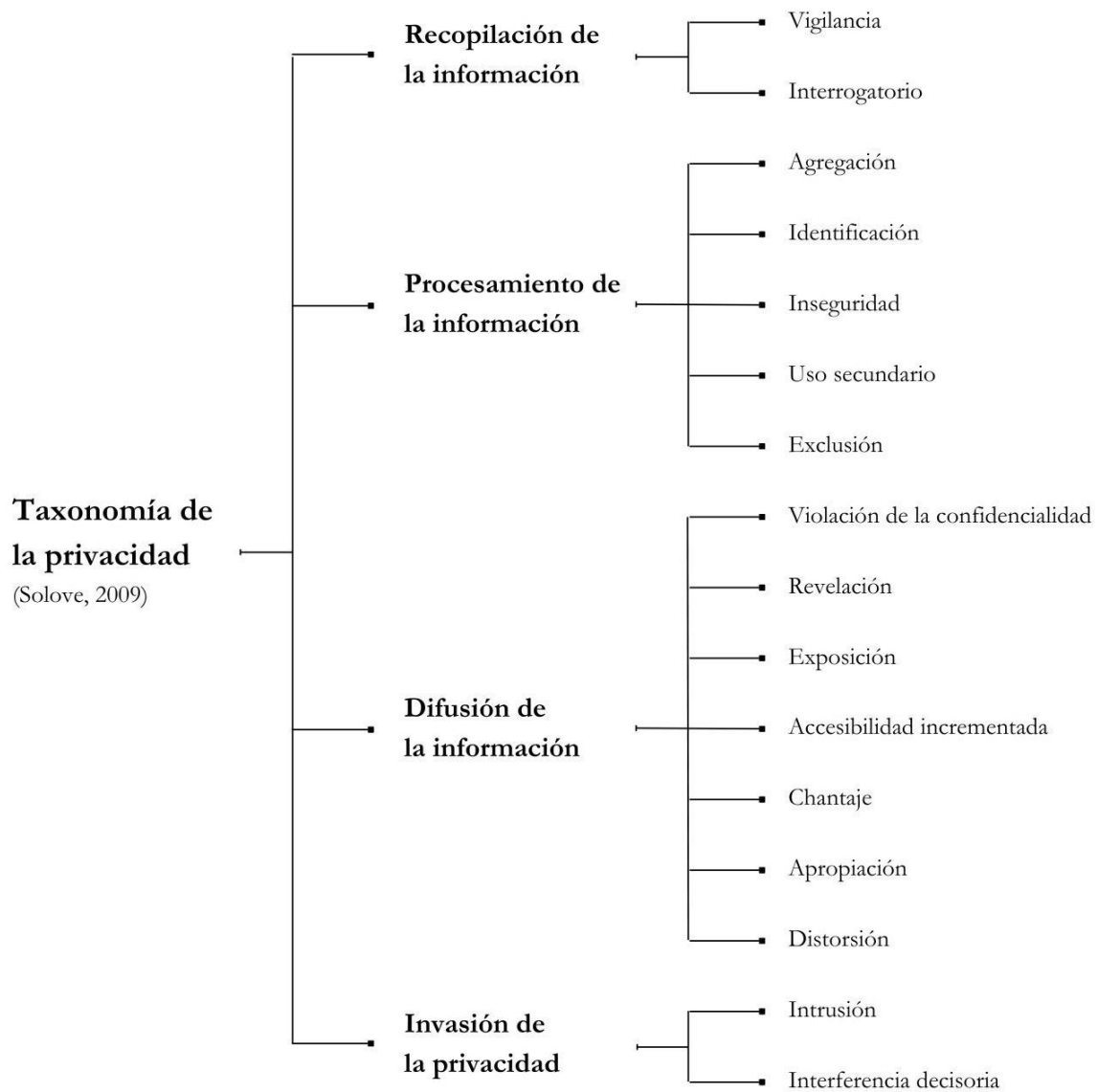


Figura 7. Esquema de la taxonomía de la privacidad de Solove (2009)

Así, en primer lugar, nos encontraríamos con cómo diferentes entidades (otras personas, empresas y gobiernos) “recopilan información” sobre el individuo en cuestión. Una vez son extraídos los datos de una persona, éstos son procesados, es decir, son almacenados, combinados, manipulados, buscados de nuevo y utilizados para un fin u otro; a estas actividades las denomina “procesamiento de la

información”. El siguiente paso sería la “diseminación de la información”, esto es, las actividades por las que se transfiere o revela la información recopilada y procesada. La evolución general desde la recopilación de información hasta el procesamiento y la diseminación provoca que los datos estén cada vez más fuera del control de los individuos. El último grupo de actividades es la “invasión”, que implica una influencia directa sobre los individuos. En este caso, no estamos ya ante una actividad alejada del individuo sino dirigida contra el mismo, sin que necesariamente haya involucrada información en el proceso.

En cuanto a los subgrupos que mencionaba dentro de esta taxonomía, éstos están divididos de la siguiente manera. Dentro de la recopilación de la información encontraríamos dos: por un lado las actividades más clásicas englobadas en la “vigilancia”, es decir, observar, escuchar o registrar las actividades de un individuo; y por otro lado el “interrogatorio”, que consistiría en las diversas formas de adquirir o captar la información.

En el grupo de actividades que implican la forma en que se almacena, manipula y utiliza la información tendríamos estas cinco: la “agregación”, esto es, la combinación de diferentes datos sobre una o varias personas; la “identificación”, que vincula cierta información a individuos particulares; la “inseguridad” de que estos datos sensibles sean robados para fines perniciosos o que se almacene dicha información de manera inadecuada; también encontraríamos el “uso secundario” de dicha información para un propósito diferente a aquel para el cual fue recopilada, siempre sin el consentimiento de la persona interesada; y por último la “exclusión”, que se refiere a no permitir que la persona interesada conozca los datos que se tienen sobre ella y no pueda participar en su manejo y uso.

Dentro del tercer grupo, la diseminación de la información, encontraríamos para empezar problemas relacionados con la “violación de la confidencialidad” y a la “revelación” de información que, aun siendo veraz, puede comprometer la reputación de la persona en cuestión. Junto a ellos, la “exposición” de las intimidades de un individuo y el hecho de que haya una “accesibilidad incrementada” a la información recopilada potencian no solo los peligros anteriormente citados sino también el “chantaje”, la “apropiación” y la “distorsión” de la información que se disemina sobre una persona. En torno a todas estas actividades planea no solo la transferencia o revelación de la información personal en sí sino también la amenaza de llegar a hacerlo (Solove, 2009, p. 105). El cuarto y último grupo, que implica invasiones a los asuntos privados de las personas, no tiene por qué implicar información personal, aunque en numerosos casos también lo hace. Entre ellas encontramos la “intrusión”, que se refiere a los actos invasivos que perturban la tranquilidad o la soledad de un individuo, así como la capacidad de “interferencia decisoria”, que implica la intromisión en las decisiones del interesado respecto de sus

asuntos privados. A continuación iré realizando un desarrollo del esquema de Solove en profundidad de cara a que podamos entender mejor su taxonomía.

Recopilación de la información

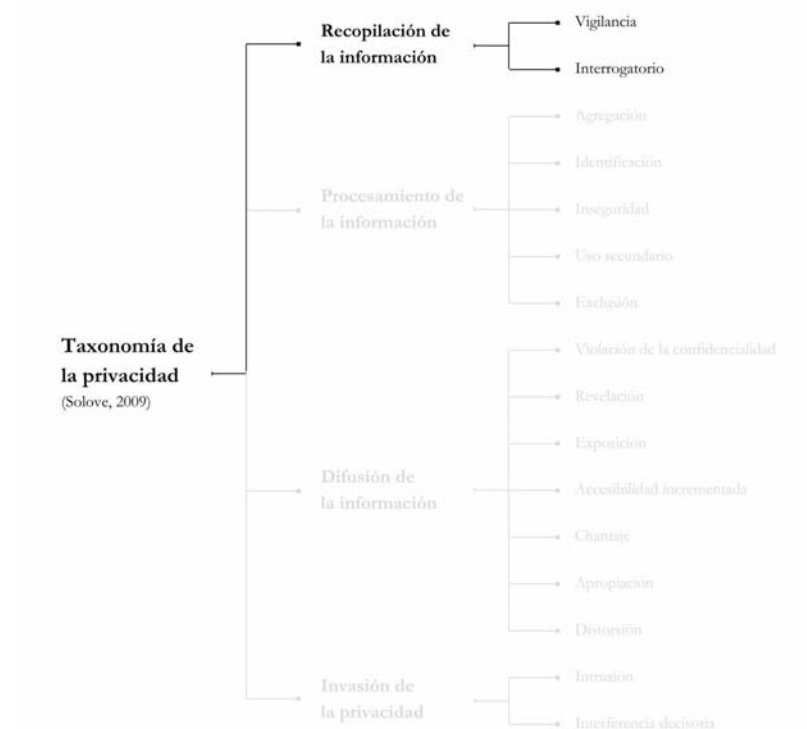


Figura 8. Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Recopilación de la Información”

La “recopilación de información” genera disrupción a través del proceso de compilación de datos. Como hemos visto, incluso si no se revela información públicamente, la recopilación de información puede causar un perjuicio a los individuos, y en las dos formas de esta que señala Solove (2009, pp. 106-116): la vigilancia y el interrogatorio.

- **Vigilancia**

Como vimos en el punto anterior, ser consciente de que se está siendo vigilado no solo genera incomodidad, sino que también puede provocar que alteremos nuestro comportamiento, aumentando la probabilidad de que nos inhibamos y autocensuremos. En este sentido, para Gilliom (2001, citado en Solove, 2009, p. 108), se vigila el comportamiento humano con la intención de controlarlo, ya sea

limitando el acceso a programas o instituciones, controlando y afectando su comportamiento dentro de esos ámbitos o haciendo cumplir las reglas y normas mediante la observación y el registro de actos tanto de cumplimiento como de desviación. Si bien ya hemos apuntado que este aspecto de la vigilancia no es invariablemente dañino, demasiado control social puede afectar negativamente a la libertad, la creatividad y el autodesarrollo. Para Julie Cohen (2013, citado en Solove, 2009, p. 108): «los regímenes de vigilancia y modulación distribuidos de manera generalizada buscan moldear las preferencias y el comportamiento individuales de maneras que reducen la casualidad y la libertad de experimentación que hacen prosperar la innovación». De manera similar, Solove (2009, p. 108) alude a las tesis de Paul Schwartz (1999), el cual sostiene que la vigilancia inhibe la libertad de elección e incide en la autodeterminación. Sin embargo, tal y como hemos visto con el Panóptico, puede haber un efecto paralizador mayor cuando las personas son conscientes de su vigilancia pero no están seguras de si están sometidas a ella en un preciso momento. Por lo tanto, la conciencia sobre la posibilidad de estar siendo vigilado puede llegar a ser tan inhibidora como la vigilancia real.

- **Interrogatorio**

Con la palabra interrogatorio a todos nos vienen a la mente imágenes de películas policiacas en las que un sospechoso se encuentra sentado en una sala con un falso espejo por el que unos agentes lo observan sin ser vistos a la vez que dentro de la sala le hacen multitud de preguntas para resolver una investigación. Sin embargo, existen formas de interrogatorio menos coercitivas a la común de nuestro imaginario cuando, por ejemplo, (otro tipo de) inspectores o funcionarios nos hacen preguntas con fines distintos del enjuiciamiento penal. A pesar de que no nos estén acusando de nada, una batería de preguntas más o menos personales puede hacernos sentir también muy incómodos. Por ejemplo, a finales del siglo XIX, hubo una fuerte protesta pública cuando el censo estadounidense comenzó a incluir preguntas relacionadas con asuntos personales, como el estado civil, el nivel de alfabetización, la propiedad, la salud o las finanzas (Solove, 2001, p. 1401). Las reacciones negativas ante el escrutinio de los censos se remontan al ya citado libro de *Domesday* dentro del apartado 2.1.1.

El interrogatorio tiene como objetivo que las personas den cierta información, para lo cual se ejerce cierta presión sobre ellas. Aunque puede tener muchos beneficios, dado que es útil para descubrir información que otros quieren saber, también puede causar daño en función del grado de coerción aplicado. En este sentido, el interrogatorio se parece a la intrusión en su carácter invasivo porque no deja de ser un sondeo, una forma de búsqueda, la cual a menudo implica la revelación de información oculta, no obstante, el interrogatorio puede generar malestar incluso si la información extraída de él

apenas se difunde. Hasta cierto punto, la vigilancia se parece al interrogatorio porque ambos implican la recopilación involuntaria de información, si bien en este el sujeto es consciente de que dicha recopilación está teniendo lugar, frente a la habitual clandestinidad de la vigilancia. Otro aspecto del poder del interrogatorio es su potencial para generar distorsión, en la medida en que el interrogador posee un control extraordinario sobre la información que se obtiene, cómo se interpreta y las impresiones creadas por sus revelaciones.

Procesamiento de la información

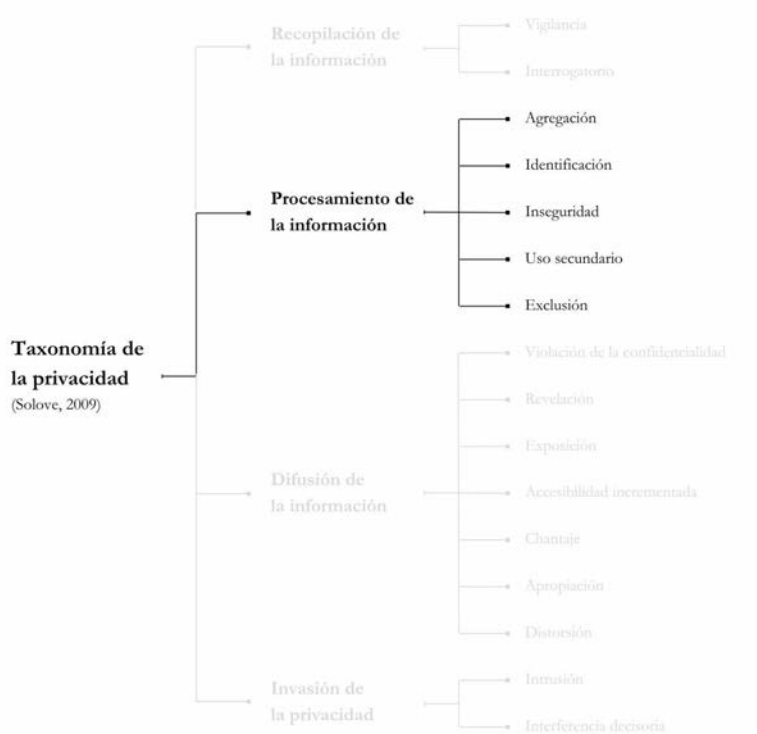


Figura 9. Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Procesamiento de la información”

El procesamiento de información abarca el uso, almacenamiento y manipulación de los datos que ya han sido recopilados. Se trata, por tanto, de cómo se manejan los datos una vez han sido recogidos. En este caso, Solove (2009, pp. 117-135) identifica cinco formas: agregación, identificación, inseguridad, uso secundario y exclusión.

El procesamiento implica varias formas de conectar datos y vincularlos con las personas a las que pertenecen. Aunque puede implicar la transmisión, se diferencia de la revelación porque la transferencia

de datos no implica la divulgación de la información, ni siquiera a otra persona. Más bien, los datos suelen transferirse entre varios sistemas de registro y combinarse con otros datos. El procesamiento difiere de la recopilación de información porque el procesamiento crea perjuicios a través de la consolidación y el uso de la información, no a través de los medios por los cuales se recopila.

- **Agregación**

Solove (2009, p. 18) se refiere al término “agregación” para definir la recopilación de información sobre una persona. Lo particular de este método es que, si bien un fragmento de información por sí solo no tiene por qué revelar mucho, cuando son combinados entre sí pueden formar el retrato de una persona, es decir, el todo sería mayor que la suma de las partes (Cohen, 2000, citado en Solove, 2009, p. 118). Cuando se analiza la información agregada, ésta puede revelar nuevos hechos sobre una persona que no se podían conocer a través de los datos originales recopilados de manera aislada. En la actualidad, el poder y el alcance de la agregación son mayores, ya que los datos recopilados sobre las personas son significativamente más extensos, el proceso de combinarlos es mucho más fácil y las tecnologías para analizarlos son más sofisticadas y poderosas.

La agregación causa un perjuicio sobre los individuos debido a la forma en que altera las expectativas. Esto es así porque las personas esperamos ciertos límites sobre lo que se sabe sobre nosotros y sobre lo que otros pueden llegar a descubrir. La agregación altera estas expectativas al combinar datos de maneras imprevistas para revelar hechos sobre una persona que no se tienen por qué conocer tan fácilmente. Las personas difundimos fragmentos de información en diferentes entornos, revelando sólo una pequeña parte de nosotros mismos en cada contexto. De hecho, distribuimos selectivamente estos pequeños fragmentos de datos a lo largo de la mayor parte de nuestras actividades diarias, aunque tenemos la expectativa de que en cada manifestación revelen relativamente poco sobre nosotros mismos. Sin embargo, cuando estas piezas se consolidan, los analistas de estos datos adquieren un conocimiento mucho mayor sobre la vida de la persona.

Al igual que la vigilancia, la agregación es una forma de adquirir información sobre las personas, si bien menos directa que la vigilancia porque se produce mediante el procesamiento de datos que ya han sido recopilados previamente. Si bien la toma de decisiones basadas en datos agregados puede ser eficiente, también puede generar problemas, pues los conjuntos de datos suelen ser sesgados e incompletos, de modo que revelan facetas de nuestras vidas de un modo reduccionista que están desconectado del contexto original en el que fueron tomados. Esto es matizado por Dan McQuillan (2022, pp. 12-14) quien lo relaciona con la idea de la “extracción”, del arranque coercitivo, llegando a usar el término

“amputación”:

Sin embargo, un problema más profundo es la idea misma de representación que estos sistemas propagan. Esto queda bien ilustrado por el conjunto de datos paradigmático de aprendizaje profundo llamado ImageNet, que consta de más de 14 millones de imágenes etiquetadas, cada una de las cuales está etiquetada como perteneciente a una de más de 20.000 categorías o clases. La suposición que impulsó la creación del conjunto de datos fue la de un etiquetado inequívoco; un conjunto de términos que describieran una imagen correctamente y que se aplicaran a todas y cada una de las instancias en las que esa imagen apareciera en el mundo.

En este gesto radical, ImageNet amputó la idea de un punto de vista y afirmó la irrelevancia del contexto o la experiencia corpórea. Un sistema entrenado con un conjunto de datos de este tipo no sabe nada de historia, poder o significado, de modo que a una foto de “un soldado israelí sujetando a un niño palestino mientras la familia del niño intenta sacar al soldado” se le puede asignar el título “Gente sentada en lo alto de un banco” (Katz, 2020) (McQuillan, 2022, p. 13).

- **Identificación**

Según Roger Clarke (1998), la identificación es la asociación de una serie de datos con un ser humano en particular. En el contexto de los sistemas de información, el propósito de la identificación es más concreto, ya que se utiliza para vincular un flujo de datos con una persona (Clarke, 1994a, p. 8). La identificación nos permite no sólo confirmar quién es una persona, sino también dirimir quién ha cometido un delito, gracias al registro de las huellas dactilares u otros datos biométricos.

La identificación se relaciona con la revelación puesto que ambas implican revelar información veraz, si bien aquí se trata de un tipo particular de esta, a saber, la propia identidad, que permite vincular bases de datos con personas. La identificación resulta similar a su vez a la agregación porque ambas implican la combinación de diferentes datos, uno de los cuales es la identidad de una persona, pero se diferencia de ella en que implica un vínculo con la persona encarnada. Por ejemplo, puede haber grandes conjuntos de datos sobre una persona en muchas bases de datos, pero es posible que estas agregaciones rara vez estén conectadas con esa persona mientras realiza sus actividades diarias. Esta situación implica una alta agregación y una baja identificación. Por otro lado, puede existir un alto nivel de identificación con un bajo nivel de agregación, como es el caso de los puntos de acceso o control, donde las personas

tienen que mostrar su identificación pero donde no hay vínculos con repositorios más grandes de datos sobre los mismos.

El problema no surgiría, por tanto, del acto en sí de identificar(se), sino de cómo se vinculan los datos con los individuos, debido a que, al conectar a las personas con los datos, la identificación adjunta a éstas un bagaje de información. Esto altera lo que otros aprenden sobre nosotros cuando participamos en diversas transacciones y actividades. Por lo tanto, la identificación está interrelacionada con otros problemas de privacidad y con cómo ellos revelan, distorsionan y la invaden. Sin embargo, la identificación diverge de las variantes anteriores porque es principalmente una forma de conectar datos con personas. Si bien la mencionada agregación ya crea lo que Solove (2006) viene a denominar una “persona digital”, un retrato compuesto de fragmentos de información combinados, la identificación va un paso más allá, ya que vincula a la persona digital directamente con una persona en el espacio real.

La identificación también afectaría a la estructura social, dado que aumenta el poder del gobierno sobre los individuos. Como hemos visto anteriormente, la identificación ha sido una herramienta fundamental para los gobiernos que buscaban controlar a la población, empezando por aquéllos que situaban en los márgenes de la misma. Por contrapartida, el anonimato y el seudónimo protegen a las personas de los prejuicios basados en sus identidades y les permiten realizar actividades tan importantes como votar, hablar y asociarse más libremente, reguardándolos del peligro de posibles represalias. Sobre esto, recordemos cómo Gary T. Marx (2002) señalaba que el anonimato puede facilitar el flujo de información y comunicación sobre temas públicos y fomentar la experimentación y la toma de riesgos sin enfrentar grandes consecuencias, como el riesgo de fracaso o vergüenza ya que la identidad de uno está protegida. En suma, el anonimato puede mejorar la capacidad de persuasión de las propias ideas en la misma medida en que la identificación puede llegar a ensombrear la recepción de dichas ideas con los sesgos y prejuicios de los lectores.

- **Inseguridad**

Los fallos, las fallas de seguridad, los abusos y los usos ilícitos de la información personal pueden provocar, además de robos de identidad, un grupo más amplio de problemas que Solove (2009, p. 127) agrupa bajo el término “inseguridad”. Considerado un problema causado por la forma en que se maneja y protege nuestra información, la inseguridad está relacionada con la agregación porque crea riesgos de daños posteriores que pueden surgir de una protección inadecuada de nuestros datos personales. Junto a ello, la inseguridad también está relacionada con la identificación: a menudo ocurre debido a las

dificultades para vincular los datos con las personas.

La distorsión, esto es, la difusión de información falsa sobre una persona, también está relacionada con la inseguridad, porque los problemas de seguridad pueden provocar que los registros personales se contaminen con datos falsos. La inseguridad, por lo tanto, puede implicar no sólo una amenaza de divulgación sino también de distorsión.

- **Uso secundario**

Bajo el término “uso secundario”, Solove (2009, p. 131) hace referencia al uso de datos para fines no relacionados con los que se recopilaron inicialmente y sin el consentimiento de la persona interesada, aunque de nuevo debo señalar que existen casos deseables para este uso secundario, como detener un delito o salvar una vida. No en vano, la variedad de posibles usos secundarios de los datos es prácticamente infinita y va desde consecuencias benignas hasta malignas. Este uso secundario a menudo también se denomina “expansión del cometido” o “expansión de los datos”, que describe la expansión gradual de los usos de la información a lo largo del tiempo (Solove, 2009, p. 131).

El uso secundario puede causar problemas, ya que implica emplear información de maneras que una persona no ha consentido y que tal vez no le resulten deseables. Los usos secundarios frustran nuestras expectativas sobre cómo se utilizarán los datos que proporcionamos, de modo que es muy posible que las personas no proporcionen datos si conocen un posible uso secundario, como *marketing* directo, *spam* u otras formas de publicidad intrusiva. Para Paul Schwartz (1999), el uso secundario genera un problema de asimetría del saber:

Es probable que los individuos sepan poco o nada sobre las circunstancias bajo las cuales se capturan, venden o procesan sus datos personales. Esta ignorancia individual generalizada obstaculiza el desarrollo a través del mercado de la privacidad de normas apropiadas sobre el uso de datos personales. El resultado de este conocimiento asimétrico serán acuerdos unilaterales que beneficiarán a los procesadores de datos (p. 1683).

Además, el uso secundario de la información puede crear problemas dado que esta información puede no encajar tan bien como se podría esperar con el nuevo uso. Cuando los datos se eliminan del contexto original en el que fueron recopilados, es más fácil que se malinterpreten.

- **Exclusión**

Con “exclusión”, Solove (2009, p. 134) hace alusión a la falta de conocimiento por parte de las personas afectadas sobre sus registros en una u otra base de datos. La exclusión reduce la responsabilidad de las agencias gubernamentales y las empresas que mantienen registros personales de informar de qué tipo de información contienen y para qué la usan. La exclusión se diferencia de la inseguridad en que la primera no sería principalmente un daño causado por la falta de protección contra la fuga o contaminación de datos, sino más bien un daño creado al privarle de un derecho a estar informado sobre cómo se utilizan esos datos y al no poder hacer nada para saber cómo se utilizan.

Al igual que ocurre con el uso secundario y la inseguridad, la exclusión crea una sensación de vulnerabilidad e incertidumbre. Cuando no podemos participar en el mantenimiento y uso de nuestra información, nos sentimos impotentes. Algunos podrían argumentar que hay muchos aspectos de la vida en los que somos impotentes, y que no hay nada especial en la impotencia con respecto a la información personal. Pero en un mundo donde la información personal cada vez más se utiliza para tomar decisiones importantes, la impotencia en esta área puede ser significativamente problemática, pues nos despoja a las personas del control sobre nuestras vidas de manera sustancial.

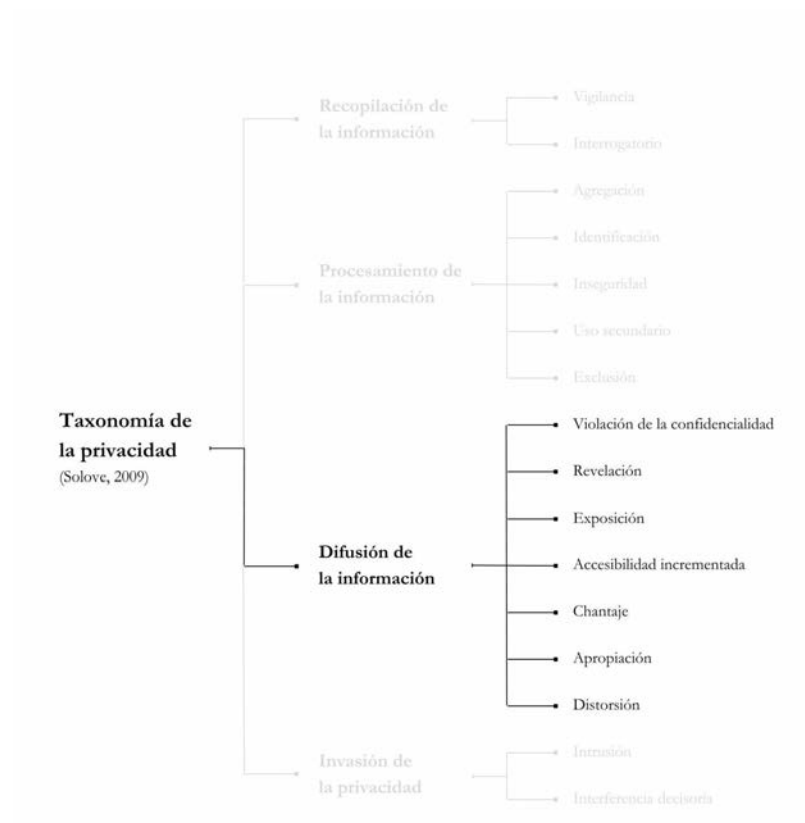
Diseminación de la información

Figura 10. Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Difusión de la información”

La diseminación de información comprende uno de los grupos más amplios de problemas de privacidad, que consisten en revelar datos personales o amenazar con hacerlo. Dentro de este grupo, Solove (2009, pp. 136-160) incluye: la violación de la confidencialidad, la revelación, la exposición, la accesibilidad incrementada a la información personal, el chantaje, la apropiación y la distorsión.

- **Violación de la confidencialidad**

Encontramos una diferencia entre los problemas para la privacidad derivados de la violación de la confidencialidad del de los derivados de la divulgación, ya que aunque ambos implican revelar los secretos de una persona, la violación de la confidencialidad también traiciona la confianza en una relación específica.

Sin embargo, Solove (2009, p. 139) apunta a que, en el caso de la normativa estadounidense, existe un reconocimiento inconsistente del daño derivado de un incumplimiento de la confidencialidad, y esto es

debido a que la Cuarta Enmienda de los Estados Unidos¹³ no lo reconoce como tal. Para ello relata el caso de *Estados Unidos vs. Miller*, en el cual funcionarios federales encargados de hacer cumplir la ley emitieron citaciones a dos bancos para que presentaran los registros financieros de un cliente. Los bancos cumplieron con las citaciones, pero el cliente no fue notificado de la divulgación de los registros hasta más tarde, cuando ya estaba en curso el proceso. El acusado sostuvo que las citaciones violaban sus derechos de la Cuarta Enmienda, pero el Tribunal Supremo concluyó que el cliente carecía de una expectativa razonable de privacidad en los registros financieros que mantenía su banco, argumentando que la Cuarta Enmienda no prohibía la obtención de información revelada a un tercero y transmitida por él a las autoridades gubernamentales. Además, el Supremo sostuvo que todos los documentos obtenidos, incluidos los estados financieros y los recibos de depósito, contienen únicamente información transmitida voluntariamente a los bancos y expuesta a sus empleados en el curso normal de sus negocios. A través de lo que se ha venido a denominar la “doctrina de terceros”, se establece que si la información es poseída o conocida por terceros, entonces, a los efectos de la Cuarta Enmienda, un individuo carecería de una expectativa razonable de privacidad en la información emitida. El problema radica actualmente en que, gran parte de lo que hacemos es registrado por terceros. Por lo tanto, la doctrina de terceros coloca una gran cantidad de información personal fuera de la protección de la Cuarta Enmienda. (Solove, 2006, pp. 201-209).

La doctrina de terceros se basa en el paradigma del secreto, esto es, que cuando otros conocen la información, ya no es completamente secreta. Pero el hecho de que la información sea conocida por terceros no sería relevante para el análisis de un Tribunal si el daño se entendiera como una violación de la confidencialidad. Cuando las personas establecen una relación con bancos, proveedores de servicios de Internet, compañías telefónicas y otras empresas, no están revelando su información al mundo, se la están dando a una parte con promesas implícitas (y a menudo explícitas) de que la información será confidencial. Además, en EEUU, existe otra ley que, a diferencia de la Cuarta Enmienda, reconoce la violación de la confidencialidad como un daño distinto. Sin embargo, este agravio por violación de la confidencialidad se aplica solo a la relación médico-paciente. De hecho, más adelante veremos cómo otras empresas que operan con datos sensibles han quedado fuera de estas regulaciones.

13 La Cuarta Enmienda de Estados Unidos reconoce que:

no se violará el derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias, contra allanamientos e incautaciones fuera de lo razonable, y no se expedirá ningún mandamiento judicial para el efecto, si no es en virtud de causa probable, respaldada en juramento o promesa, y con la descripción en detalle del lugar que habrá de ser allanado y de las personas o efectos que serán objeto de detención o incautación (Constitución de los Estados Unidos, 1791, IV Enmienda).

- **Revelación**

Existen leyes en distintos países que protegen a las personas contra la revelación de información veraz sobre ellas (Solove, 2009, p. 140). Este hecho ha provocado que algunos críticos sostengan que este derecho infringe la libertad de expresión. Para Eugene Volokh (2000, citado en Solove, 2009, p. 142), el derecho a la privacidad de la información, entendido como el derecho a controlar la comunicación de información personal identificable sobre uno mismo, es un derecho a que el gobierno impida a unos hablar sobre otros. Para Thomas Emerson (1970, citado en Solove, 2009, p. 142), el derecho a la privacidad dependería de garantizar a un individuo la libertad de no ser invadido y la libertad de pensar y creer, quedando fuera la libertad de no discutir sus opiniones, acciones o asuntos. Otros han afirmado que la protección contra la revelación inhibe nuestra capacidad de juzgar a los demás y determinar si son dignos de nuestra confianza. Según Richard Posner (1981, citado en Solove, 2009, p. 142), las protecciones contra la revelación brindan a las personas el poder de ocultar información sobre sí mismas que otros podrían usar en su contra. Según este autor, las protecciones contra la revelación brindan a las personas el poder de ocultar información sobre sí mismas que otras podrían usar para sus intereses.

Aunque la protección contra la revelación puede limitar la libertad de expresión, a su vez promueve el mismo interés en ella, puesto que ambas fomentan la autonomía individual. Y es que el riesgo de revelación puede impedir que las personas participen en actividades que fomenten su propio desarrollo personal (Solove, 2003, pp. 990-992). Dado que una cantidad sustancial del discurso político no ocurre en tribunas públicas, sino en conversaciones privadas, al igual que con la libertad de expresión las protecciones contra la revelación promueven el autogobierno democrático. La privacidad fomenta el discurso sin inhibiciones al permitir que las personas dirijamos una comunicación franca con aquellas en las que confiamos y que no nos causarán un futuro daño por lo que decimos. Así, sin protecciones contra la revelación, las personas podrían ser más reacias a criticar aspectos de su vida pública, aunque es probable que una amenaza de revelación no ponga fin a todas las conversaciones, sí alterarían su contenido. En la misma línea, la revelación también puede impedir que unas personas se asocien con otras, afectando a su vez a la libertad de asociación.

Otro punto que destacar es que la revelación conlleva la pérdida del anonimato, el cual a veces es esencial para la promoción de la libertad de expresión. Sobre esto, Julie Cohen (1996, citado en Solove, 2009, p. 143) señala que la protección contra la revelación también facilita la lectura y el consumo de ideas. La protección contra la revelación promueve así objetivos democráticos, incluidos los mismos objetivos que promueve la libertad de expresión. Además, la revelación amenaza la seguridad de

quienes desean proteger su información de otros que puedan usarla para causarles daño físico, emocional, financiero o de reputación. Por último, la revelación también plantea un riesgo para las personas porque las convierte en prisioneras de su propio pasado registrado, lo que puede obstaculizar su capacidad para cambiar su comportamiento, tener una segunda oportunidad o cambiar el rumbo de sus vidas. Además, una vez que la información se vuelve pública, puede utilizarse de muchas maneras impredecibles, creando problemas relacionados con el uso secundario.

- **Exposición**

La persona que ve expuestos ciertos atributos físicos y emocionales que considera profundamente primordiales a menudo padece vergüenza y humillación. El duelo, el sufrimiento, el trauma, las lesiones, la desnudez, el sexo, la micción y la defecación involucran aspectos primarios de nuestras vidas que son físicos, instintivos y necesarios (Solove, 2009, p. 147), pero que en la sociedades actuales tendemos a ocultar por nuestra educación recibida. Para Elías (2000, citado en Solove, 2009, 147), la referencia social de la vergüenza y el bochorno se aleja cada vez más de la conciencia, precisamente porque el mandato social de no mostrarse expuesto o realizando funciones naturales opera ahora respecto a todos.

Aunque la exposición es similar a la revelación (ambas implican la difusión de información veraz), difieren en un aspecto importante: mientras que la exposición implica información sobre nuestros cuerpos y nuestra salud, la revelación implica una gama mucho más amplia de datos que implican la reputación de una persona. Las personas sentimos mayor humillación cuando sufrimos una exposición, incluso si la información revelada no tiene ningún efecto sobre cómo otros juzgan nuestra reputación. La exposición crea un perjuicio porque hemos desarrollado prácticas sociales para ocultar aspectos de la vida que no nos agradan. Además, en algunas de estas actividades somos vulnerables y débiles, como cuando estamos desnudos o vamos al baño. Cuando estas prácticas se ven alteradas por la exposición, las personas pueden experimentar una humillación y una pérdida de autoestima graves y, a veces, debilitantes. Por tanto, la exposición impide la capacidad de una persona para participar en la sociedad. Aunque la mayoría de la gente no vería a una víctima de exposición como una persona inferior o menos civilizada, las víctimas se sienten así. Esto contrasta con la revelación, donde la información a menudo afecta la reputación de una persona.

- **Accesibilidad incrementada**

Si la información personal de alguien ya es pública, resulta lógico que nos preguntemos qué riesgos

supondría una accesibilidad incrementada a ella, quedando ya descartados los de revelación de secretos y violación de la confidencialidad. El riesgo al que nos enfrentamos con esta accesibilidad incrementada a la información personal está vinculado a la mayor probabilidad de perjuicios derivados de la revelación. Y es que esta información, en combinación con el problema de la agregación de datos, podría explotarse con facilidad para fines distintos de aquellos para los que originalmente se hizo pública. Solove (2006, pp. 131-132) pone de ejemplo de esta amenaza la actividad de las empresas que recopilan datos de registros públicos con fines comerciales y de *marketing* o para elaborar perfiles y otros análisis.

- **Chantaje**

El “chantaje” permite que una persona sea dominada y controlada por otra. Con él, el daño no estaría en la revelación misma de la información, sino en el control que ejerce quien amenaza con llevarla a cabo si no se cumplen sus imposiciones. En algunos casos, el chantaje también puede implicar información más ligada a la exposición que a la revelación. De igual manera, la violación de la confidencialidad también estaría relacionada con él en la medida en que un confidente puede amenazar con revelar un secreto a cambio de dinero. Sin embargo, su diferencia con los anteriores riesgos se encuentra en que el chantaje se ejerce sobre la base de una amenaza de revelación y no tanto de su ejecución real. Por tanto, el propósito de restringir el chantaje no sería limitar la revelación de información personal sino evitar que la amenaza de hacerlo se utilice como arma para ejercer poder y dominio sobre otros.

- **Apropiación**

Aunque su etimología conecte directamente con el concepto de propiedad, hablamos de “apropiación”, cuando se usa la identidad o personalidad de alguien para los propósitos y metas de otra. La apropiación, al igual que las perturbaciones de la privacidad causadas por la revelación y la distorsión, afecta de lleno a la forma en que un individuo desea presentarse ante la sociedad. La protección contra la apropiación establece los límites que la sociedad considera adecuados apropiado para que otros puedan moldear la identidad de una persona. El daño, entonces, está en una vulneración de la libertad de la víctima de ejercer una suerte de autoría de su propia narrativa, no simplemente en la pérdida de beneficios derivados de su identidad.

- **Distorsión**

La leyes sobre difamación, que protegen contra falsedades y calumnias que dañan la reputación de una

persona, existen desde hace siglos y tienen su origen en la antigua ley romana de *injuria* (Van Vechten Veeder, 1903, citado en Solove, 2009, p. 158). Vinculada a este concepto, la “distorsión” se define como la manipulación en la forma en que los demás perciben y juzgan a una persona, pero implica que la víctima es caracterizada de manera inexacta. La distorsión, al igual que la revelación, implica la difusión de información que afecta a la forma en que la sociedad ve a una persona, de modo que ambas pueden provocar en ella vergüenza, humillación, estigma y daño a la reputación. Al restringir ambas amenazas, el propósito es preservar la capacidad de controlar la información sobre uno mismo y tener cierto dominio limitado sobre la forma en que uno es visto. Sin embargo, frente a la revelación, el carácter distintivo de la distorsión reside en que en este caso la información revelada es falsa y engañosa.

Invasión de la privacidad

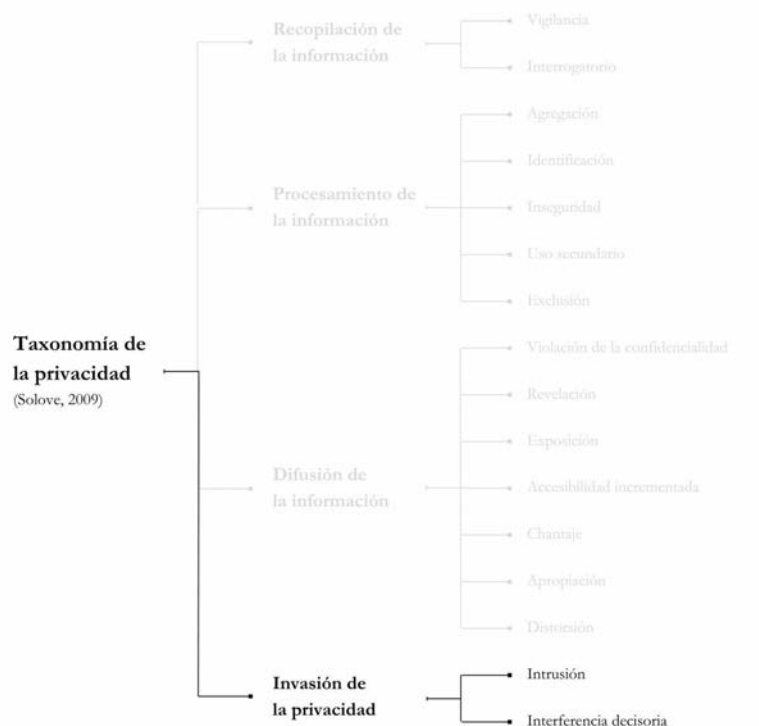


Figura 11. Esquema de la taxonomía de la privacidad de Solove (2009), resaltando “Invasión de la privacidad”

El último grupo de problemas en torno a la privacidad queda englobado en el concepto de “invasión”, que se diferencia de los problemas de recopilación, procesamiento y diseminación porque no siempre involucra información propiamente dicha. Para Solove (2009, pp. 161-170), los problemas de invasión pueden analizarse a partir de dos variantes: la intrusión y la interferencia decisoria.

- **Intrusión**

La “intrusión” implica invasiones o intromisiones en la propia vida. Ésta perturba las actividades diarias de la víctima, altera sus rutinas, destruye sus momentos de soledad y, a menudo, la hace sentir incómoda e intranquila. La protección contra la intrusión implica salvaguardar al individuo de invasiones sociales no deseadas, brindándole lo que los ya citados Warren y Brandeis (1890) nombraban como “el derecho ser dejado en paz”.

La intrusión está relacionada con la revelación porque a menudo es posible dejar a merced de actividades invasivas de recopilación de información. La intrusión en la propia esfera privada puede ser causada no sólo por incursión física y proximidad sino también por seguimientos (vigilancia) o cuestionamientos (interrogatorio) (Solove, 2009, p. 161). En este sentido, para el autor la intrusión tiene cierta semejanza con la vigilancia en el sentido de que ser observado durante períodos prolongados puede ser bastante invasivo, penetrante, perturbador e incluso aterrador. La intrusión también está relacionada con el interrogatorio porque las personas pueden experimentar el interrogatorio como una especie de intromisión en sus asuntos. El daño causado por la intrusión, sin embargo, difiere del causado por otros tipos de perturbación porque la intrusión interrumpe las actividades de alguien a través de la presencia o actividades no deseadas de otra persona.

La soledad permite a las personas descansar de las presiones de vivir en público y desempeñar funciones públicas. Según el filósofo Philip Koch (1994, citado en Solove, 2009, p. 164), la soledad permite un respiro y restauración, un tiempo y un lugar para “lamer las heridas” del conflicto social. Para Westin (1967, citado en Solove, 2009, p. 164), por su parte, ningún individuo puede desempeñar indefinidamente, sin alivio, la variedad de roles que exige la vida, por lo que la privacidad brinda a todo el mundo, desde los trabajadores de las fábricas hasta los presidentes, la oportunidad de retirarse su máscara para descansar. Sin refugio de los demás, las relaciones pueden volverse más amargas y tensas. Además, un espacio apartado de los demás ha permitido a diferentes personas a lo largo de la historia desarrollar ideas artísticas, políticas y religiosas que han tenido una influencia y un valor duraderos cuando más tarde se han introducido en la esfera pública. Para Solove (2009, p. 165) el concepto de “aislamiento” es relativo, puesto que el mero hecho de que una persona pueda ser vista por alguien no

significa automáticamente que pueda ser obligada legalmente a estar sujeta a ser vista por todos.

Por otro lado, sobre el concepto de soledad, Bordier (2024) plantea una interesante definición asimétrica de la percepción de (o aspiración a) la soledad con un marcado componente de clase que debemos tener en cuenta:

Al tratamiento de las “soledades problemáticas” corresponde, en otro nivel social, la promoción de las “soledades solucionadoras”: retiros espirituales y silenciosos, retos deportivos, alquiler o venta de islas desiertas, etc. Para que el mundo siga siendo soportable para las personas cultas o de buena cuna, necesitan librarse de las molestias de la vida y de la gente corriente. Siempre que dispongan de tiempo, energía y dinero, la soledad “a la carta” que aprecian políticos, empresarios, deportistas y escritores (o a veces todo esto a la vez) abre la posibilidad de vivir cosas extraordinarias. Y de darlo a conocer.” [...] Los escritos de estos solitarios millonarios ratifican la tesis del sociólogo Philip Slater, autor en 1970 de un ensayo sobre las raíces sociales y raciales del deseo de soledad en los Estados Unidos de la década de 1960: el hombre blanco de las clases media y alta, impulsado por fuerzas sociales segregadoras, llegó a creer que estaba solo en el mundo, que era un ente autónomo y apartado de los demás hombres, con quienes el contacto se antojaba insostenible. [...] Los que cultivan el aislamiento enriquecedor viven en el mismo mundo que los artífices de la lucha, a veces estéril, contra la ruptura del “vínculo social”. Mientras unos disfrutan de la mejor compañía posible —la suya propia—, los que sufren el aislamiento económico y social tienen que conformarse con los vínculos que les imponen porque, en lo que a ellos respecta, mejor mal acompañados que solos consigo mismos. (Bordier, 2024, p. 32)

- **Interferencia decisoria**

Con interferencia decisoria, Solove (2009, p. 166) se refiere a la capacidad gubernamental de interferir en las decisiones de las personas respecto de ciertos asuntos de sus vidas relacionados con el sexo y la sexualidad, así como con la crianza de los hijos por parte de sus padres. Estos casos de interferencia decisoria están profundamente conectados con la privacidad de la información, hasta el punto que el jurista Neil Richards (2006) señala que la jurisprudencia canónica “decisoria” sobre privacidad ha tenido durante mucho tiempo un componente informativo sustancial.

Encontramos similitudes entre la interferencia decisoria y la inseguridad, el uso secundario y la

exclusión en el sentido de que estos tres daños del procesamiento de la información pueden tener un efecto paralizador en las decisiones de una persona con respecto a su salud y su cuerpo. La interferencia y la exposición a las decisiones generalmente involucran los mismos aspectos de uno mismo, como el cuerpo y las actividades sexuales. Por lo tanto, la interferencia en las decisiones no se aplica a todas las decisiones sino sólo a un subconjunto de ellas. Este aspecto de la interferencia en la toma de decisiones se asemeja a la exposición por su enfoque en aquellos aspectos de la vida que socialmente se consideran más privados. La interferencia decisoria presenta asimismo una similitud con el daño de la intrusión porque ambos implican invasiones a ámbitos donde creemos que las personas deberían estar libres de intromisiones.

Conclusiones sobre la taxonomía de la privacidad

A través de la taxonomía que hemos recorrido a lo largo de estas páginas, la pretensión de Solove (2009) es realizar una descripción de abajo hacia arriba de los dilemas que se abordan en diferentes debates, leyes, casos, constituciones, pautas y otras fuentes en torno al dilema de la pérdida de privacidad. Sin embargo, los problemas identificados en la taxonomía no están concebidos como eternos ni inmutables. De hecho, al optar por la semejanza familiar para describir la privacidad, se corre el riesgo de combinar aspectos que no tengan relación y dejar fuera otros que sí tendrían un sentido. Con todo, la función principal de este enfoque de conceptualización de la privacidad es cambiar el tipo de discusiones teóricas que tenemos sobre la misma, pasando de buscar una concepción unificada a centrarnos en los diversos problemas a los que se enfrenta. A mi entender, tal cambio de enfoque nos proporciona mayor claridad y orientación para abordar las cuestiones relativas a la pérdida de privacidad.

En este sentido, es importante recalcar que el valor de la privacidad debe entenderse en términos de su contribución a la sociedad. Y ello pese a que siguen abundando las explicaciones de su valor en términos de derechos individuales que presuntamente entrarían en conflicto con los intereses de la sociedad, lo cual nos abocaría a protegerlos por encima de cualquier otro interés en competencia, incluso cuando este pueda entrañar una mayor utilidad social que la privacidad. Por contraposición, hemos visto que cuando la privacidad protege a los individuos, lo hace porque en última instancia ello redundaría en un beneficio general para la sociedad. En otras palabras, la privacidad no implica tan sólo la libertad frente al control social, sino una forma de protección construida socialmente, lo cual nos lleva a concluir que su valor no surge de cada forma de privacidad en sí, sino de la gama de actividades que la protegen.

Al traducir esta aspiración al sistema legal, la privacidad es codificada como una forma de protección contra ciertas actividades consideradas dañinas o problemáticas, aunque no siempre lleguen a ser socialmente indeseables o dignas de sanción o prohibición. Debido a esto, al abordar los problemas de privacidad nos topamos con la dificultad de que en muchos casos no hay un “villano” indiscutible cuyas acciones carezcan por completo de valor social. En otras ocasiones, encontramos muchos problemas que surgen como resultado de otras actividades, al igual que la contaminación en una consecuencia de la producción industrial. En este sentido, a través de su taxonomía Solove intenta demostrar que estas actividades no resultan inocuas, ya que tienen ciertos efectos no triviales en la vida y el bienestar de las personas.

Cabe reseñar igualmente cómo los problemas de privacidad más comunes, como las intrusiones físicas, la divulgación de secretos o la distorsión, son bien abordados por los tribunales y legisladores, en parte debido a que son asuntos sujetos a las ideas tradicionales de privacidad. Así, la violación de la privacidad se entiende en el paradigma del secreto como el descubrimiento del mundo oculto de una persona, algo que incluso las personas de la antigüedad podían experimentar e identificar como pernicioso. Sin embargo, algunos de los problemas de privacidad con los que nos encontramos hoy son de naturaleza distinta y contradicen las intuiciones tradicionales sobre ella. De este modo, hemos visto esfuerzos para obtener conocimientos sobre las personas sin invadirlas físicamente o incluso recopilando datos ofrecidos directamente por ellas (agregación). Junto a ello, existen problemas originados en la forma en que se manejan y mantienen los datos (inseguridad), en que se utilizan (uso secundario), y en la imposibilidad de las personas de participar en su procesamiento (exclusión). Los problemas de privacidad modernos surgen no sólo de la revelación de secretos profundos, sino también de la accesibilidad incrementada a la información oculta (o de la observación o escucha constantes (vigilancia)).

En resumen, atendiendo a esta taxonomía la privacidad implicaría un conjunto de protecciones contra un grupo de problemas diferentes pero relacionados, todos los cuales impiden actividades valiosas que la sociedad quiere proteger, como la autonomía, la seguridad, la igualdad y la justicia o la democracia entre otros. Al idear cómo crear estas protecciones, entre todos reconocemos y damos lugar a un ámbito particular de la libertad que llamamos “privacidad”, el cual nos exige una atención ineludible a sus contextos específicos, en la medida en que para sopesar la privacidad y los intereses que se le contraponen dependemos de las circunstancias de cada situación.

2.2.4. Privacidad como integridad contextual

En relación a la cuestión de la importancia que se le da a la privacidad en función del contexto, Lyon (2018, p. 143) explica que, cuando se ha entrevistado a usuarios de redes sociales o se ha preguntado en grupos de discusión sobre sus experiencias en línea —sin que se les pida que utilicen un lenguaje que involucre vigilancia y privacidad— los resultados resultan diversos y complejos. Sin embargo, resulta bastante evidente que, lejos de no preocuparse por lo que sucede con sus datos personales, con frecuencia demuestran una gran sensibilidad ante estos temas y creen que algunas actividades de *marketing* y corporativas son del todo inapropiadas o simplemente injustas. Esto no quiere decir que todos los participantes estén de acuerdo, pues de hecho queda patente que el contexto influye en la forma en que se interpretan los usos institucionales de los datos personales, al igual que lo hacen la posición social de una persona, en términos de género o edad, y el tiempo invertido en las actividades en línea.

Una forma adecuada de considerar esto es lo que Helen Nissenbaum (2004) llama “integridad contextual”. Según ella, en una época en que los datos personales fluyen libremente a través de muy diversos canales y los usos que se hace de ellos son igualmente dispares, resulta importante saber qué es lo que realmente les importa a quienes se refieren dichos datos. En este sentido, Rayne-Goldie (2010) apunta cómo, por ejemplo, muchos usuarios de las redes sociales estarían mucho más preocupados por lo que sus contactos en línea pueden ver de sus publicaciones y contenido que por lo que puedan ver las empresas. Aunque este hecho bien puede indicar más una falta de conocimiento que una falta de preocupación, no deja de ser posible que se estén aplicando diferentes estándares de privacidad a diferentes situaciones. Tal y como explica la autora (Nissenbaum, 2004, p. 138):

Una consecuencia de ello es que las prescripciones sobre privacidad, que hoy están determinadas en gran medida por factores locales, probablemente varíen según la cultura, el período histórico, el lugar, etc. Aunque algunos podrían considerar esto problemático, yo lo considero una virtud. Como han señalado destacados colaboradores de los estudios de la privacidad, las normas de privacidad de hecho varían considerablemente de un lugar a otro, de una cultura a otra, de un período a otro; esta teoría no sólo incorpora esta realidad, sino que señala sistemáticamente las fuentes de variación.

En línea con lo anterior, Nissenbaum (2004) también defiende que la privacidad debe entenderse en términos de “normas contextuales” que regulan la información, en particular, «normas de idoneidad y normas de flujo o distribución» (p. 119). «La integridad contextual», argumenta, «se mantiene cuando se

cumplen ambos tipos de normas, y se viola cuando se incumple cualquiera de las mismas” (Nissenbaum, 2004, p. 138). «Según la teoría de la integridad contextual», sostiene la autora, «es crucial saber el contexto: quién recopila la información, quién la analiza, quién la difunde y a quién, la naturaleza de la información, las relaciones entre las distintas partes e incluso circunstancias institucionales y sociales más amplias» (Nissenbaum, 2004, pp. 154-155).

Retomando este debate más adelante, Nissenbaum (2009, p. 127) precisa que «el derecho a la privacidad no es ni un derecho al secreto ni un derecho al control, sino un derecho a un flujo apropiado de información personal». Y al hilo de estas palabras, matiza que lo que establece qué resulta apropiado serían las normas sociales dependientes del contexto: los tipos de información en cuestión, los roles del sujeto, el emisor y el receptor de la información, y los principios bajo los cuales se comunica la información. En último término, la autora recalca que las violaciones del derecho a la privacidad ocurren cuando se contravienen estas normas.

A partir de su concepción de “la privacidad como integridad contextual”, Nissenbaum (2009) avanza hacia la distinción de cuatro clases de contexto: el flujo de información, las capacidades con las que actúan los usuarios, los tipos de información en cuestión y el principio de transmisión. Para ella, estos contextos ayudan a mostrar por qué algunos tipos de datos se consideran más reveladores o controvertidos que otros, y por qué algunos métodos de recopilación de datos provocan rechazo, al menos dentro de ciertos grupos de personas. De hecho, continúa argumentando, revelar ciertos tipos de detalles equivale a una negación de los derechos sobre los datos si son contrarios a las expectativas del titular de los mismos.

Sin embargo, el relato de Nissenbaum presentaría, según Véliz (2024, p. 69), algunos problemas. El primero es que, aunque hay algo intuitivamente cierto en el hecho de que la privacidad se ve invadida cuando se violan las normas sociales, de ello resultaría una explicación demasiado vaga del concepto. No en vano, las normas sociales no siempre son obvias o explícitas, y diferentes grupos sociales en la sociedad pueden tener normas diferentes. Además, cuando aparece una nueva tecnología, puede que no haya normas sociales en torno a ella durante algún tiempo. Como ilustración, Véliz toma el caso en el que alguien con millones de seguidores en las redes sociales comparte una publicación hecha por alguien con unos pocos seguidores que revela algo personal sobre sí mismo, preguntándose si ello sería considerado una violación del derecho a la privacidad. Por un lado, podría argumentarse que no, en el caso de que se sostenga que la norma social es que las publicaciones en las redes sociales son públicas y es moralmente aceptable compartirlas ampliamente. Por otro lado, la respuesta afirmativa podría aducir que la persona que compartió información personal sobre sí misma no esperaba llegar a una audiencia

amplia debido a los pocos seguidores que tenía (Véliz, 2024, pp. 69-70).

Un segundo problema que Véliz encuentra es que la teoría de la integridad contextual tiene una tendencia a ser conservadora, tal y como la propia Nissenbaum admite (2009, p. 161). Al basarse únicamente en las normas sociales, aceptaría “la tiranía de lo normal” quedándose sin recursos para desafiar las normas sociales. Pese a todo, en último término Nissenbaum encuentra ventajas en una teoría con semejante inclinación conservadora, entendiendo las normas sociales eminentemente como formas encarnadas de sabiduría acumulada : «por razones de expectativa, sabiduría acumulada y lógica establecida, tiene sentido una presunción a favor de normas de información arraigadas y relativas al contexto» (Nissenbaum, 2009, p. 164). Sin embargo, para Véliz (2024, p. 70) se ha demostrado que el *marketing* agresivo y las técnicas de recopilación de datos son muy eficaces para erosionar las normas sociales en torno a la privacidad. De nuevo, Nissenbaum (2004, p. 146) ya dejaba abierta esta vía para desafiar el *statu quo* cuando matiza:

Sin embargo, una presunción a favor del *statu quo* no excluye la posibilidad de una impugnación exitosa cuando existen razones adecuadas. Para resolver estos casos controvertidos se necesitan medios confiables para evaluar la posición moral relativa de las normas arraigadas y las prácticas novedosas que las violan o amenazan. En particular, propongo que se comparen las normas arraigadas con las prácticas novedosas que las violan o amenazan, y se juzgue si vale la pena preservarlas, o no, en términos de qué tan bien promueven no sólo los valores y bienes internos de un contexto dado, sino también valores sociales, políticos y morales fundamentales.

2.3. De las sociedades de control al extractivismo de datos personales

Tras repasar el contexto histórico de las prácticas de vigilancia y los cambios que ha supuesto en ellas el desarrollo de diferentes tecnologías; y tras revisar las distintas concepciones del concepto de privacidad y las repercusiones que conllevan, en este apartado me centraré en las relaciones que generamos con las tecnologías digitales. Y es que el traslado de nuestra vida social cada vez más a un plano digital mediado en gran medida por plataformas diseñadas por empresas con fines lucrativos ha modificado nuestras formas de relacionarnos entre nosotros, así como de ver y entender nuestros cuerpos. Dichos cambios provocan que nos entiendan y nos entendamos como datos, a veces de manera consciente y en otras ocasiones de formas que escapan a nuestro conocimiento, lo que genera una suerte de *sosias* digital que intercede por nosotros en, por ejemplo, candidaturas a un puesto de trabajo o a través del que se calcula nuestro seguro de automóvil o nuestra hipoteca.

Para entender estas relaciones, comenzaré describiendo lo que el filósofo Gilles Deleuze (1990/1995) definió como «sociedades de control». Con este concepto, Deleuze apunta al modo de gobierno y control que ha evolucionado desde las sociedades disciplinarias descritas por Foucault (1975/2002), caracterizadas por instituciones como la prisión y la escuela, a otras que se valen de las tecnologías de vigilancia para neutralizar y someter a los individuos.

Estas relaciones pueden llegar a ser mediadas a través del concepto también deleuziano, de servidumbre maquínica (*asservissement machinique*, en francés), que se refiere a la creciente dependencia de la tecnología y la automatización en diversos aspectos de la sociedad, lo que conduce a una pérdida de autonomía y control humanos. De este modo, a medida que las máquinas se vuelven más avanzadas y capaces de realizar tareas complejas, asumen cada vez más trabajos y responsabilidades que antes realizaban los humanos. Junto a ello, dichas máquinas ocupan un lugar central en la mediación de nuestras relaciones personales, deformándolas a través de nuestra versión del otro mediado por lo digital, al quedar nuestras personalidades divididas en parcelas categorizables. Si nos fijamos en las notas del editor de Marcelo Expósito en la obra de Gerald Raunig *Mil Máquinas* (2008, pp. 32-33) encontramos una síntesis del concepto que luego desarrollaré:

«Servidumbre maquínica» no significa sencillamente la relación subordinada del ser humano con el saber social objetivado en las máquinas técnicas, sino que se trata de una forma más general de administración capitalista del saber colectivo y de la constante necesidad que los sujetos tienen de una participación autodeterminada. La cualidad maquínica del capitalismo

postfordista suma a los tradicionales sistemas de opresión directa todo un espectro de mecanismos de control que requieren la complicidad de los propios individuos: con esta idea, Guattari se sitúa muy cerca de las teorías de la gubernamentalidad capitalista desarrolladas por Foucault.

En cuanto al concepto de “extractivismo de datos personales” al que aludía en el punto 1.1., y que aquí ampliaré, desempeña un papel central en las sociedades de control, ya que permite la manipulación dirigida de las personas. Así, en el epílogo que escribe el sociólogo y filósofo italiano Maurizio Lazzarato en la obra de Gerald Raunig (2008, p. 110-114) vemos que:

El sistema capitalista, mediante la sujeción social, produce y distribuye roles y funciones, nos equipa con una subjetividad y nos asigna una individuación específica (identidad, sexo, profesión, nacionalidad, etcétera). La sujeción, por una parte, nos individúa, nos constituye en sujeto siguiendo las exigencias del poder y, por otra parte, une a cada individuo a una identidad “propia y sabida”, bien determinada de una vez por todas. [...] La servidumbre maquínica consiste en la movilización y en la modulación de los componentes preindividuales, precognitivos y preverbales de la subjetividad, haciendo funcionar los afectos, las percepciones, las sensaciones aún no individuadas, aún no asignables a un sujeto, etc., como elementos de una máquina. [...] En la servidumbre maquínica hacemos literalmente cuerpo con la máquina. El funcionamiento de la servidumbre maquínica no conoce distinción entre «humano» y no humano, entre sujeto y objeto, sensible e inteligible.

2.3.1. Sociedades de control

Al final del punto 2.1, concluía que la vigilancia actual se había transformado, pasando de formas rígidas a otras más flexibles y fluidas. Este sistema, que en las conclusiones sobre la vigilancia de dicha sección denominé con Bauman y Lyon (2013, pp. 61-84) “vigilancia post-panóptica” se caracteriza por su movilidad, conectividad y fluidez, y en él las tecnologías y las redes de información se vuelven más relevantes que los territorios o las instituciones.

Sobre esta conversión de los sistemas de vigilancia de la “disciplina” al “control” teorizó Gilles Deleuze en su *Post-scriptum sobre las sociedades de control* (1990/1995, pp. 277-286), donde extendió las ideas de Foucault, quien en un primer momento había planteado la teoría de la vigilancia en el marco de espacios confinados y fijos como el Panóptico. Con todo, para Deleuze (1990/1995, p. 278), Foucault siempre recalcó que nos encontrábamos en un momento posterior al control disciplinario.

Por su parte, el co-autor (junto con Félix Guattari) de *Mil Mesetas* sugirió que esos antiguos lugares de confinamiento ya no eran los únicos ni los más destacados lugares de observación. Los sitios que anteriormente eran “analógicos” ahora poseían su equivalente en los nuevos medios digitales. Una idea que Lyon (2007, p. 60) encuentra similar a la de Paul Virilio (1994), quien habla del rápido y libre control de la “máquina de visión”. La nueva vigilancia es entonces individualizada y competitiva, apropiada para las nuevas empresas que fueron surgiendo de la reestructuración de finales del siglo XX, donde el monitoreo constante verificaba las actividades de los trabajadores y los incentivos individuales brindaban estímulos para su cumplimiento.

A su vez, Lyon (2007, p. 61) también detecta que la tesis de la sociedad de control de Deleuze guarda una sorprendente similitud con una teoría propuesta en ese mismo tiempo dentro del mundo anglosajón, la idea de una “nueva penología” de Feeley y Simon (1994). Los defensores de esta teoría argumentaron que, en lugar de atribuir culpabilidad a los individuos e imponer castigos y tratamientos, la nueva penología se ocuparía de técnicas para identificar, organizar y gestionar grupos clasificados por sus niveles de peligrosidad (Feeley y Simon, 1994, p. 180). Los nuevos enfoques de gestión de riesgos de la delincuencia invitaban a la vigilancia a realizar evaluaciones, en lugar de formas individualizadas basadas en la sospecha. Recordemos el concepto de “justicia actuarial” (Cabello y Rascón, 2020, p. 278) citado en el apartado 2.1.2. concretamente en *La estadística como forma de control social*.

Para Mattelart (2007/2009, p. 231): «Deleuze ha leído los escritos de W.S. Burroughs [(1961, 1985)] sobre el *soft control* y la *soft máquina* y saca provecho de ellos». Además, para este autor, Deleuze impulsó un concepto de sociedades de control que, aunque no logró desarrollar en gran medida, se ha establecido con el transcurso del tiempo. De hecho, este concepto está en el corazón de una variedad de iniciativas intelectuales críticas cuyo vínculo principal es la inquietud acerca de la renovación de las formas organizativas del poder y de las figuras del individuo y de la subjetividad que le son características (2007/2009, p. 231).

Nos adentramos según Deleuze «en sociedades de control que funcionan no ya por encerramiento, sino mediante control continuo y comunicación instantánea» (1990/1996, p. 236). Nos encontramos, por tanto, en una época donde la forma de acumulación del capital está experimentando cambios de escala y naturaleza, en términos de su espacio-tiempo y sus relaciones con el Estado y el contexto social. Mattelart (2007/2009, p. 231) ve en este modelo de administración social una semejanza al modelo de gestión de la empresa-red del posfordismo. Los sistemas sociotécnicos de control adaptable, a corto plazo, de rotación ágil y flujo constante se exportan a todas las instituciones. El resultado es que el modelo gerencial se adapta a las tecnologías emergentes de la información. Dicho modelo se

fundamenta en el extenso pasado de las doctrinas organizacionales, a lo largo del cual se desarrolló el paradigma de la «sociedad funcional» (Mattelart, 2007/2009, p. 231), que llega a su apogeo con la era de la información. En esta sociedad de control guiada por el modelo gerencial, la habilidad para prever el comportamiento de las personas, determinar la probabilidad de un comportamiento específico, y establecer categorías basándose en frecuencias estadísticas se erige en tema clave que permea el trabajo de la mercadotecnia, el sistema financiero, y los perfiles de la policía (Mattelart, 2007/2009, p. 233).

Para este autor, (Mattelart, 2001/2007, p. 163) las sociedades de control son plenamente visibles en los comienzos del siglo XXI, donde la intensidad del paradigma de la seguridad se concatena con el crecimiento convergente de nuevas modalidades de administración de las sociedades, impulsadas en gran parte por la logística de las tecnologías digitales. La fascinación por la seguridad incide en la estructura de los usos de los sistemas de información en dicha administración, a través de las redes de vigilancia que encontramos, por ejemplo, en el transporte y otros sectores públicos.

Si continuamos con la lógica de las sociedades de control, vemos cómo Deleuze realiza una contraposición entre el lenguaje analógico de las disciplinas, donde cada centro de encierro por el que se transita en la vida opera como una variable independiente (la escuela, la fábrica, la cárcel); y el lenguaje numérico —aunque no por ello binario— del control, que se constituye en una modulación “autodeformante”, cambiante e inseparable entre ellos (la formación permanente, la empresa, la vigilancia ubicua):

Las sociedades disciplinarias presentan dos polos: la marca que identifica al *individuo* y el número o la matrícula que indica su posición en la *masa*. Para las disciplinas, nunca hubo incompatibilidad entre ambos, el poder es al mismo tiempo masificador e individuante, es decir, forma un cuerpo con aquellos sobre quienes se ejerce al mismo tiempo que moldea la individualidad de cada uno de los miembros. [...] En cambio, en las sociedades de control, lo esencial ya no es una marca ni un número, sino una cifra: la cifra es una *contraseña* [*mot de passe*], en tanto que las sociedades disciplinarias están reguladas mediante *consignas* [*mots d'ordre*] [...] El lenguaje numérico de control se compone de cifras que marcan o prohíben el acceso a la información. Ya no estamos ante el par “individuo–masa”. Los individuos han devenido “dividuales” y las masas se han convertido en indicadores, datos, mercados o “bancos” (Deleuze, 1990/1995, p. 281).

En consecuencia, ahora dichos “dividuos” se transforman en datos o muestras dentro del régimen dominante de lo digital, que ha reemplazado a las máquinas simples (Deleuze, 1990/1995, p. 282). Por

su parte, las corporaciones se convierten en el centro del escenario social, aunque contienen un carácter fluido y ondulante, ya que el *marketing* se ha convertido en su razón de ser: «No es un capitalismo de producción, sino de productos, es decir de ventas o de mercados. Por eso es especialmente disperso, por eso la empresa ha ocupado el lugar de la fábrica» (Deleuze, 1990/1995, p. 283). Para Lyon (2007, p. 87), cuando el filósofo francés afirma que los individuos ya no están tanto “encerrados” como “endeudados” se refiere a que están atados a la corporación. Deleuze (1990/1995) atribuye también a Félix Guattari la idea de que «lo que importa no es la barrera, sino el ordenador que señala la posición, lícita o ilícita, y produce una modulación universal» (p. 284).

2.3.2. El doble de datos

Si en el estudio desarrollado por Foucault, encontramos una clave hermenéutica para la sociedad disciplinaria, en la figura paradigmática del Panóptico, en la tesis de Deleuze vemos que el núcleo de las sociedades de control es lo que él denomina la contraseña, es decir, esa competencia digitalizada para determinar quién puede transitar un espacio y quién no, según una serie de factores que escapan al control de la persona afectada. Un claro ejemplo de la transición de una a otra la encontramos en la obra *El Proceso* (1925) de Franz Kafka, en la cual un sistema judicial burocrático y difícil de manejar arresta al protagonista pero se niega a informarle de los cargos que se le imputan, manteniendo sobre él un expediente al que no tiene acceso. En un momento de la obra, el protagonista se enfrenta al dilema que se le plantea entre «la *absolución aparente* (entre dos encierros), típica de las sociedades disciplinarias, y el *aplazamiento ilimitado* (en continua variación) de las sociedades de control» (Deleuze, 1990/1995, p. 281). Frente a otros relatos conocidos sobre la vigilancia como *1984*, Solove (2009, p. 194) sostiene que la obra de Kafka centra el problema, no en un comportamiento inhibido, sino en la impotencia asfixiante y la vulnerabilidad creada por el uso de datos personales por parte del sistema judicial y la exclusión del protagonista de tener conocimiento o participación en dicho proceso.

A continuación, para entender en qué consisten estas relaciones de conocimiento y poder que operan en las sociedades de control, voy a desarrollar una serie de conceptos análogos que se encuentran asociados con los nuevos sistemas de vigilancia digitalizados, entre los que destaco tres: la “imagen de datos” de Lyon (1994); la “persona digital” de Clarke (1994b) y el “doble de datos” de Haggerty y Ericson (2000).

Imagen de Datos

En cuanto al primer concepto citado, David Lyon (1994) lo toma de Kenneth Laudon (1986), quien

ofrece la noción de imagen de datos como una llamada de atención sobre la importancia de la representación digitalizada de nuestras vidas para esos bancos de datos a los que tanta centralidad vimos que atribuía Gilles Deleuze.

Esta imagen de datos puede incluir detalles como nombre, dirección, número de teléfono, edad, sexo, origen étnico, además de preferencias de consumo, infracciones de tráfico, solvencia y logros educativos, (Lyon, 1994, p. 85), y para Mark Poster (1990, p. 96) «constituye a los individuos de acuerdo con estos parámetros». Este “otro” disfrutaría de una existencia separada del individuo cuyos datos lo componen, el cual podría verse tanto perjudicado como beneficiado por el primero.

Para Lyon (1994, p. 55), la imagen de datos que circula dentro y entre las bases de datos de las organizaciones requiere nuestra participación y tiene un impacto cada vez mayor en nuestras oportunidades de vida, pero al mismo tiempo resulta menos visible y accesible para nosotros. El poder de los ordenadores facilita una nueva convergencia entre sistemas de vigilancia formalmente distintos, pero esto no significa necesariamente centralización. Y es que el perfil cada vez más integrado que constituye la imagen de datos de cada persona es una concatenación compleja de diversos fragmentos que, aun reunidos de forma remota, impersonal y apenas perceptible, tiene consecuencias claras para la experiencia y las posibilidades de vida de la persona a la que se refiere. A menudo, sentencia Lyon (1994, p. 99), se extraen conclusiones y se toman decisiones y juicios sobre la base de la imagen de datos, en lugar de comprobar los detalles con el individuo en cuestión. De hecho, los recopiladores de datos a menudo creen que ellos, y no los sujetos de los datos, son los dueños de dichos datos personales. Este hecho ha generado desazón desde su planteamiento, valga como ejemplo el planteamiento de Stafford Beer acerca de su imagen electrónica:

Mi imagen electrónica en la máquina puede ser más real que yo. Es redonda; es completa; es recuperable; es predecible en términos estadísticos... Estoy en un lío; y no sé qué hacer. La máquina sabe más —en términos estadísticos. Por lo tanto, mi realidad es menos real que mi imagen en la tienda. Ese hecho me disminuye. (Beer, 1969, citado en Brown, 1990, p. 75).

El concepto de imagen de datos difiere de las otras definiciones que se exponen en este punto en que se basa en agregar diferentes datos personales para formar el concepto digital sobre una persona destinado a su posterior uso en gestiones administrativas, aceptación o negación de créditos y cálculos de pólizas de seguros.

Persona digital

Roger Clarke (1994b, párr. 9) define el concepto de “persona digital” como un modelo de la personalidad pública de un individuo basado en datos y mantenido mediante transacciones, cuyo fin es ser utilizado como representante del individuo. Para este autor, resulta un término útil y necesario para comprender cómo las redes informáticas establecen un modelo sobre el individuo a través del almacenamiento y el análisis de colecciones de datos personales. Al mismo tiempo, sostiene que la persona digital también puede ser potencialmente amenazante, degradante o socialmente peligrosa debido a la capacidad de su uso para monitorear, y por lo tanto posiblemente controlar, a las personas a través de sus datos (Clarke, 1994b, párr. 13).

Para este autor la habilidad para desarrollar una personalidad puede recaer en el individuo, en otras personas u organizaciones, o en ambas partes. Si bien el individuo posee un cierto nivel de control sobre su personalidad proyectada, es decir, lo que una persona quiere que se conozca sobre ella, resulta más complicado influir en las personalidades que nos son impuestas por terceros. Es posible que cada observador recolecte una serie distinta de información acerca de cada persona con la que interactúa y, en consecuencia, genere una percepción distinta de dicho individuo. En cualquier caso, el receptor establecería el significado de una personalidad digital basándose en sus propias normas de procesamiento. Además, aquellos individuos que son conscientes del uso de los datos podrían proyectarlos de manera selectiva, con el objetivo de impactar en la personalidad digital que se construye (Clarke, 1994b, párr. 10). Por otro lado, se recalca la importancia de diferenciar entre las personalidades digitales informales que se fundamentan en percepciones humanas y las personalidades digitales formales que se forman a partir de acumulaciones de datos estructurados.

Clarke concluía su escrito de 1994 con la advertencia de que los individuos estábamos siendo gradualmente sustituidos por nuestra versión de persona digital, fundamentada en un control social de los gobiernos y del *marketing* empresarial que entrañaba peligros significativos tanto para las personas como para la comunidad. Finalmente, vaticinaba que si la tecnología de la información persistía sin obstáculos, la implementación de la personalidad digital inevitablemente traería repercusiones injustas y opresivas para las personas y la sociedad. En esta línea, indicaba que sería imprescindible ejercer presión sobre los legisladores para asegurar la implementación de medidas y procedimientos reglamentarios pertinentes.

Si bien este concepto es similar al de imagen de datos, Clarke suma al mismo las interacciones sociales que pueden desarrollar las personas en el ámbito digital, así como la capacidad de tener cierto control sobre nuestra persona digital. En este sentido, pone el ejemplo del uso particular de auto-contestadores

de mensajes de correo o la capacidad del individuo de modificar su concepto de persona digital ajustando sus interacciones digitales para asemejarse a un perfil diferente al suyo.

Dobles de Datos

Haggerty y Ericson desarrollaron el concepto del “doble de datos” para explicar el creciente interés por el control, no ya de cuerpos enteros, sino de los fragmentos de datos que emanan de ellos. Así, el cuerpo se «descompone en una serie de flujos significativos discretos» (Hagger y Ericson, 2000, p. 612) a partir de fotografías, sustancias químicas y otras entidades para que pueda ser observado.

Este doble de datos no es una representación de la persona, pero provoca efectos en la vida diaria y encarnada de la misma. De hecho, en algunas circunstancias la evidencia del doble de datos puede tener prioridad sobre la palabra de la persona encarnada. Para explicarlo, Lyon (2007, p. 88) pone de ejemplo los casos de los robos de identidad, cuando diferentes personas cuyas cuentas de tarjetas de crédito han sido utilizadas de manera fraudulenta por otros encuentran que se necesitan mucho tiempo y esfuerzo para persuadir a bancos, oficinas de crédito y otras agencias de que son clientes fiables. La vida virtual del doble de datos se percibe como más real, a efectos prácticos, que la vida física de la víctima, agotada de intentar contar su versión de la historia.

Para Haggerty y Ericson, asistimos a una fusión de lo que anteriormente eran sistemas de vigilancia discretos, la cual combina datos personales, técnicas derivadas de prácticas militares, administrativas, laborales, policiales y de *marketing* hasta generar un “ensamblaje de vigilancia”. Este conjunto opera alejado de los cuerpos encarnados y de su estructura territorial, dividiéndolos en una serie de flujos discretos que posteriormente se reagrupan en diferentes dobles de datos que pueden ser analizados y transformados en objetivos de intervención. Este ensamblaje, si bien surge de deseos identificables emanados sobre todo de la búsqueda política y tecnológica de la integración, ondula, pulsa y muta constantemente.

Para Lyon (2007, p. 114), el ensamblaje de vigilancia parece crecer, como anticipaba Deleuze (1990/1995, p. 207), no como una estructura jerárquica sino como un rizoma, un organismo parecido a una planta en expansión que se reproduce a través de brotes en diferentes direcciones, cada uno de los cuales puede echar raíces por sí mismo. En estas circunstancias, resulta difícil ver cómo prohibir partes de su operación o limitar las instituciones que la utilizan para desacelerar su crecimiento general. Aunque, recalca Lyon, esto no significa que participar en los esfuerzos por redirigirlo y canalizarlo de manera ética y socialmente positiva sea inútil.

La gran diferencia entre este concepto y los anteriores es que los primeros se constituían sumando piezas de datos para constituir la personalidad de un individuo concreto. En contraste, en el caso del doble de datos se divide la personalidad en categorías de potenciales perfiles con los que puede encajar en función de las necesidades del que maneja la información. Esto significa que, para que una persona sea encasillada en una categoría concreta, no es necesario recabar todos los datos sobre ella, sino que basta con recurrir a los datos de los que cumplen su mismo perfil, esto es, de personas de su misma edad, su mismo nivel de estudios e incluso su mismo código postal.

2.3.3. Servidumbre maquínica

Conforme las personas nos sumergimos cada vez más en la vida *online* y conforme los dispositivos conectados en red se incorporan en nuestra cotidianidad y se integran en el marco de las interacciones diarias y corporales, nuestra percepción de lo social y de nosotros mismos se transforma de nuevas formas, de las cuales la vigilancia es solo un componente más.

Los imaginarios y prácticas de vigilancia vinculados a la vida cotidiana se diferencian solo en ciertos aspectos de aquellos que podrían verse en espacios con altos niveles de control, como los aeropuertos o los lugares de trabajo. Así, si bien solemos percibirlos como situaciones distintas, pueden identificarse multitud de puntos de encuentros: por ejemplo, un eventual acceso a nuestro correo electrónico se podría llevar a cabo por parte tanto de nuestro empleador, un agente de aduanas o un rastreador *web*. Los cambios aquí están más vinculados con aspectos de lo que conlleva la vida humana en la era digital, esto es, con cómo se alteran las vivencias subjetivas y la formación de las identidades a partir de dichos sistemas técnicos. Las incertidumbres de ser observado y observar a los demás, actualmente ampliadas digitalmente, impactan en las relaciones y obligaciones sociales de maneras muy diversas. Ocurre, por ejemplo, en las plataformas de redes sociales, que nos referimos a otros como “cuentas” sin muchas veces ser del todo conscientes de si detrás de ese “avatar” existe una persona encarnada, un grupo de personas organizadas, o un *bot* programado para dar determinadas respuestas o realizar ciertas interacciones.

En este contexto en el que nuestra comunicación en muchos casos se encuentra mediada por máquinas de las que formamos parte constitutiva (y no ya de las que nos limitamos a servirnos), nuestra relación con ellas puede llegar a definirse con Deleuze como de «servidumbre», tal y como explica Lazzarato (2008, p. 109): «Uno puede vivir sometido a “servidumbre” o puede estar “sujeto” a una máquina (técnica, social, comunicativa, etc.). Estamos bajo la servidumbre a una máquina en tanto constituimos una pieza, uno de los elementos que le permiten funcionar».

Es decir, nos encontramos al servicio de la máquina cuando somos entendidos, no ya como meros manipuladores de la misma, sino en la medida en que devenimos piezas de ella, objetos de acción de los que ella se beneficia, a los que ella responde. Este hecho resulta muy visible en, por ejemplo, las aplicaciones de citas, donde la fuente de producción radica en las personas que acceden a ella y ceden una ingente cantidad de información personal con el propósito de encontrar a otras personas afines a ellas. Sin embargo, en tanto sometidas a servidumbre, quienes participan en ellas son maquínicamente divididas en perfiles potenciales de mantenerse activas en la aplicación, ser posibles compradoras de supuestos beneficios en relación a su visibilidad para otras usuarias y vendidas en paquetes de datos para otras empresas publicitarias. Estas nuevas formas de operar las relaciones afectivas a través de la máquina han supuesto también un cambio en la forma habitual de establecer vínculos amorosos (Rosenfeld *et al.*, 2018).

Sobre esto, Lazzarato, (2008, pp. 114-115), también explica que en la servidumbre maquínica, fundimos nuestro cuerpo con la máquina, sin realizar una distinción entre lo “humano” y lo “no humano”, entre individuo y objeto, entre lo sensible y lo inteligible:

La *sujeción social* actúa sobre la dimensión molar del individuo (su dimensión social, sus roles, sus funciones, sus representaciones), mientras que la *servidumbre maquínica* actúa sobre la dimensión molecular, preindividual, infrasocial (los afectos, las sensaciones, los deseos, las relaciones aún no individualizadas, no asignables a un sujeto) (Lazzarato, 2008, p. 110).

Así, mientras que la sujeción social percibe a las personas y a los dispositivos como entidades separadas e independientes (el sujeto y el objeto), y establece entre ellas límites intransmisibles, la servidumbre maquínica, percibe a las personas y a las máquinas como «multiplicidades abiertas» (Lazzarato, 2008, p. 115). El ser humano y la máquina son agrupaciones de elementos, afectos, órganos, flujos, funciones que se ubican en el mismo plano y que no pueden contraponerse de acuerdo a dualismos como ser humano/objeto, humano/no humano, sensible/inteligible.

En línea con Félix Guattari (1980/1988), el autor italiano afirma que la máquina no solo se compone de cada una de sus partes, sino también de los elementos que la conforman, lo cual la hace portadora de un elemento de autoorganización, de retroalimentación y de autorreferencialidad incluso en su condición maquínica. Además, posee la capacidad de iniciar procesos de creación, de modo que, por más inusual que ello pueda resultar para la tradición del pensamiento occidental, la “subjetividad” se sitúa simultáneamente en el lado del sujeto y del objeto. De manera similar, para Raunig (2015/2023, p. 131):

La servidumbre maquina, que conduce los modos de subjetivación más allá de la sujeción social, es la cara oculta gubernamental incluso de la potencialidad de medios de comunicación avanzados. La de-pendencia de las máquinas se ve multiplicada en el continuo engancharse a las máquinas, en el quedarse colgado de las máquinas, en el estar enganchado a ellas. El gran arte de la servidumbre maquina entrelaza una vida *online* permanente con el imperativo del aprendizaje para toda la vida y la fusión indisoluble entre los negocios y los afectos.

Según este autor (2015/2023, p. 135), la concepción de la máquina que se infiltra en el ser humano resultaría incorrecta. En este sentido, apela al ejemplo de los marcapasos cardíacos o cerebrales, como algo más que dispositivos técnicos, ya que resultan componentes ajenos no humanos que transforman al ser humano en una máquina. Por otro lado, la ya mencionada pulsera electrónica resultaría más que un reemplazo de las paredes de la cárcel, y los chips para identificar a los animales superarían a las correas para perros de la sociedad de control: «En muchas situaciones no parece tanto que las máquinas estén penetrando en los seres humanos, sino más bien que los humanos se ven arrastrados “dentro de la máquina”» (Raunig, 2015/2023, p. 135).

Pero no solo existe una tendencia a entender al otro desde los datos que media una máquina. En el apartado anterior titulado *De la Digitalización a la Datificación* ya avanzaba el cambio que había supuesto el extendido uso de teléfonos, relojes y otro tipo de dispositivos conectados a Internet como nuevas “prótesis” de nuestros cuerpos en las que volcamos una información kinésica sobre nosotros que nos cuenta de maneras que hasta ahora solo se relacionaban con la cinemática y la eficiencia de los cuerpos en el entorno laboral (Mattelart y Vitalis, 2014/2015, pp. 55-58). Ello hace aflorar una tendencia a entendernos a nosotros mismos también como dato (López-Gabrielidis, 2020), y a explorar una forma de autoconocimiento en función de lo que una máquina indica que son los parámetros de “normalidad”: cuáles son, y lo más importante, cuáles deberían ser nuestras horas de sueño, el número de kilómetros recorridos diariamente, nuestra frecuencia cardíaca o la regularidad de nuestro ciclo menstrual.

Confesión maquina

Haggerty y Ericson sostienen que las fuerzas fluidas o “flujos” trabajan con conjuntos mutantes de elementos que se unen simplemente para operar sistemas de poder, como puede ser el resonado caso de Facebook y el Departamento de Seguridad Nacional de Estados Unidos. Los flujos de la agencia de vigilancia están asegurados por el deseo, que para estos autores es una «fuerza activa y positiva» y no

solo una «carencia» en la obra de Deleuze y Guattari (Haggerty y Ericson, 2000, p. 609).

En los ensamblajes de la vigilancia actuales confluirían todo tipo de deseos, en la medida en que “la vigilancia está impulsada por el deseo de unir sistemas, combinar prácticas y tecnologías e integrarlas en un todo más amplio” (Haggerty y Ericson, 2000, p. 610). Y no se trata de cuerpos interpretados de la manera tradicional, sino de una serie de flujos significativos, reunidos para que el cuerpo pueda ser conocido, o más bien, reducido a información, lo que para Mark Poster (1990, p. 93) resultaría en cómo nos “entienden” las empresas de *marketing* y los departamentos gubernamentales. Sobre esto, Lyon (2018, p. 120) argumenta que tanto Poster como Haggerty y Ericson no vaticinaron hasta qué punto la gente está ahora dispuesta a negociar con su doble de datos, y a aceptar los beneficios de conveniencia derivados de la pérdida de control sobre aquel.

Este autor continúa argumentando que Haggerty y Ericson apenas hicieron referencia a que el objetivo de asegurar el orden, la supervisión y la administración puede no completar el listado de anhelos vinculados a la vigilancia. El ya comentado “valor de ocio voyeurista”, reflejado en las fotografías de cámaras de videovigilancia o en programas de televisión que hacen uso de estos dispositivos para crear su contenido, señala otras dimensiones del deseo. Dichas dimensiones son a su vez visibles en otra obra de Deleuze y Guattari, *Anti-Edipo* (1972/1983), donde «el deseo es una máquina y el objeto del deseo es otra máquina conectada con ella» (p. 26).

Esto podría resultar, como propone Bernard Harcourt (2015), en una situación donde los usuarios son máquinas de deseos, vinculadas con otras máquinas de deseos —sus dispositivos, aplicaciones y plataformas—. La necesidad de revisar de manera constante si tenemos nuevos mensajes, así como las publicaciones en redes; dedicar gran parte de nuestro tiempo al uso de diferentes aplicaciones, así como tener problemas para liberarnos de la presión de estar constantemente en línea y siempre alertas a las notificaciones de nuestros dispositivos, todo ello es el signo de una cultura de máquinas deseantes. Para Deleuze y Guattari (citados en Harcourt, 2015, p. 51), la fuente de gran parte del deseo está tanto en este ámbito como en otros; «es el consumismo el que libera los flujos del deseo».

Así, todos esos dispositivos se vuelven cada vez más presentes en nuestra vida; los usuarios vivimos con ellos y los deseamos. Como continúa Harcourt, a las personas nos gusta tanto interactuar con los vídeos que publican las cuentas que seguimos, enviar mensajes de texto e interactuar en las diferentes redes sociales existentes, que permitimos y fomentamos vigilancias de todo tipo. «Solo queremos, solo necesitamos estar en línea, descargar esa aplicación, tener acceso a nuestro correo electrónico, descargar ese *selfie*» (Harcourt, 2015, p. 52). Pero si esto se explica por el deseo, entonces debe ser deseo

entendido como interés, en este caso el desencadenado por la asociación con el consumismo.

Sobre la necesidad de estar en línea, Raunig (2015/2023, p. 145) afirma que el aspecto menos perceptible de las redes sociales es el anhelo de interactuar públicamente, de “(com)-compartir” datos personales, de compartirse y partirse. Esta reciente ansia por la “autodisección” en las redes sociales se fundamenta en el anhelo de destacarse en la sociabilidad en línea, una imperiosa necesidad de visibilidad, que se encuentra vinculada a una aparente voluntariedad de pérdida de la privacidad.

Según este autor, la «confesión maquina» que se produce dentro de las redes sociales permanece en el comportamiento «entre el sí mismo que se autoidentifica y su verdad frente al muro opaco de un confesionario social» (2015/2023, p. 146). Para Raunig, Foucault anticipó de manera muy acertada el comportamiento de las redes sociales, en concreto Facebook:

Su verdad no está garantizada por la autoridad altanera del magisterio ni por la tradición que trasmite, sino por el vínculo, la pertenencia esencial en el discurso entre quien habla y aquello de lo que habla. En desquite, la instancia de dominación no está del lado del que habla [...] sino del que escucha y se calla; no del lado del que sabe y formula una respuesta, sino del que [...] no pasa por saber (Foucault, 1976, citado en Raunig, 2015/2023, p. 146).

Para Kirstie Ball (2009), la vigilancia ya de por sí expone a las personas de múltiples formas, sin embargo, en el universo de las redes sociales, la vida interior, o la interioridad, se muestra de formas que implican la actividad de los individuos. Y aunque se resignen a tal exposición, también pueden llegar a disfrutarla. Naturalmente, como indica Lyon (2018, p. 140) el entorno de “vigilancia blanda” del consumidor ya propicia la exposición por sí misma. Este tipo de vigilancia, tal como la caracterizaba Gary T. Marx (2007), es menos intrusiva, por lo que la entrega de datos —en el caso que ocupa al autor, biométricos— puede resultar menos polémica cuando se emplean lenguajes específicos y se cuenta con un ambiente cultural y mediático específico. Esto logra el cumplimiento mediante la persuasión, al enfatizar los intereses comunitarios, no individuales, y explorar a distancia en lugar de cruzar los límites corporales íntimos.

La aparente aspiración de ser visible puede estar relacionada también con cómo la tecnocultura contemporánea aprecia la generación de información eficiente, ágil y asequible, donde la responsabilidad se centra en que cada vez más ésta sea pública. Sobre esto, Dean (2002) sostiene que el capitalismo comunicativo actual y los convenios estatales generan las circunstancias que fomentan la revelación y la autorrevelación. El impulso de revelar está vinculado al deseo de vigilar, fortaleciendo la política de lo personal, o al menos la de la información personal. Con todo, Lyon (2018, p. 140)

encuentra otra posible explicación de por qué los usuarios de las redes sociales se sienten tan libres de permitir que sus datos personales circulen libremente en línea; y es que representa una consecuencia lógica de lo que Arlie Hochschild (2013) llama el “yo subcontratado”.

Esto es, cuando el yo se subcontrata de esta manera, el mercado interviene e incursiona en muchos aspectos de la vida íntima. Si la vida social ya se estructura en torno a estos servicios, entonces tiene sentido la aparición de aplicaciones y sitios donde también se ofrezcan dichos servicios. En general, si ya existen contextos en los que se comparten fácilmente detalles muy personales, en un contexto de mercado esto podría considerarse como la preparación del terreno para versiones en Internet del mismo tipo de espacios, mediados en este caso por corporaciones privadas con ánimo de lucro. La voluntad de desprenderse de datos personales se vuelve rutinaria en tales entornos.

Sin embargo, no debemos perder de vista el concepto de «integridad contextual» de Helen Nissenbaum (2004), ya que el contexto marca una diferencia en cómo se interpretan los usos institucionales de los datos personales. Lo mismo cabe matizar respecto de la posición social de cada uno, en términos de género o edad, y de cuánto tiempo se invierte en actividades en línea. En suma, las personas podemos tener un interés legítimo en compartir cierto tipo de datos personales con otras personas para establecer vínculos de confianza sin que por ello debamos renunciar a nuestro derecho a la privacidad.

2.3.4. Datos y metadatos

Venimos observando cómo la vigilancia está en constante evolución y cambia de diversas formas, algunas de las cuales modifican su naturaleza. Actualmente se recopilan y emplean diversos tipos de datos de nuevas formas, lo que provoca que podamos distinguir entre la vigilancia entendida con Kitchin (2014a, 2014b) como prácticas «dirigidas» y las nuevas formas de lo que se ha dado en llamar *dataveillance* (lo que podríamos traducir como vigilancia de datos).

El concepto de *dataveillance* fue acuñado por Roger Clarke (1988), para describir la vigilancia de las actividades de alguien mediante el estudio de su rastro de datos. Hoy en día, esto incluye no solo acciones como las compras con tarjeta de crédito o las solicitudes de seguros sociales, sino también las llamadas de teléfono, la captura de datos biométricos y el uso de Internet. Mediante la extracción de esta información se va conformando el cuerpo de nuestro doble de datos.

Pero, ¿cuáles son sus fuentes? Rob Kitchin (2014a, 2014b) distingue entre tres tipos de vigilancia: dirigida, automatizada y voluntaria. En la vigilancia dirigida, es un humano quien obtiene los datos, con ejemplos obvios como los sistemas de circuito cerrado de televisión o una agencia de seguridad que

busca registros de propiedad de vehículos. En el segundo, los datos se recopilan sin la intervención de un humano, como es el caso del registro rutinario de los rastros generados a partir de transacciones con el banco o establecimientos de consumo y comunicaciones, y sobre todo con el uso de teléfonos móviles. En tercer lugar, están los datos que son “voluntariamente” cedidos por el usuario, el cual proporciona dicha información en redes sociales y otras aplicaciones. Por supuesto, estos usuarios no necesariamente piensan en sus actividades en términos de proporcionar voluntariamente datos a terceros, pero esta es una forma precisa de entender la recopilación de datos de vigilancia en este contexto, por muchas comillas que este concepto necesite.

“Datos en bruto” como oxímoron

A menudo usamos el término “recopilación de datos” para referirnos a las prácticas de obtención de la información, sin embargo esta forma de expresarlo resulta algo engañosa, ya que parece sugerir que recopilar datos es ensamblar cosas que existen libres en la naturaleza. Pero los datos no son fenómenos naturales, es necesaria una mediación para extraerlos.

Como afirman Gitelman y Jackson (2013, pp. 2-3), los datos parecen existir antes que los hechos; son el punto de partida de lo que sabemos, de quiénes somos y de cómo nos comunicamos. Esta sensación compartida de empezar con los datos a menudo conduce a una suposición inadvertida de que los datos son transparentes, de que la información es evidente por sí misma, la materia fundamental de la verdad misma. Los datos se “recopilan”, “ingresan”, “compilan”, “almacenan”, “procesan”, “extraen” e “interpretan”. Explicado de esta forma parece que la interpretación resulta en último lugar, sin embargo, las autoras afirman que, hasta un cierto nivel se puede decir que la recopilación y gestión de datos presupone la interpretación de los mismos. Para ello citan a Lev Manovich cuando dice que «los datos no sólo existen» sino que hay que «generarlos» (Manovic, 2001, citado en Gitelman y Jackson, p. 3). Por tanto, los datos necesitan ser imaginados como datos para existir y funcionar como tales, y la imaginación de los datos implica una base interpretativa. Es por ello que estas autoras consideran que los datos en bruto son un oxímoron.

Ir más allá: metadatos

En línea con lo anterior, podemos añadir que nuestro doble de datos no solo se conforma a través de los textos, vídeos e imágenes que producimos conscientemente en uno u otro espacio de la red, y de cuya autoría podemos responder. Como afirma Zuboff (2019/2020, p. 256), también hemos de atender a lo que define como «texto en la sombra», que no es otra cosa que el conjunto de información que los

dispositivos que utilizamos añaden a nuestro contenido original —lo que la autora denomina «el primer texto»—. Ahora bien, un nombre que me resulta más adecuado para la comprensión de este “texto en la sombra” es el de “metadatos”, agudamente explicado por Edward Snowden (2019, p. 246) de la siguiente manera:

El prefijo de este término, meta-, que tradicionalmente se traduce como ‘por encima’ o ‘más allá’, se utiliza aquí en el sentido de ‘acerca de’: los metadatos son datos acerca de datos. Siendo más precisos, son datos que están hechos de datos: un grupo de etiquetas y marcadores que permiten que los datos sean útiles.

Una forma de entender los metadatos es definirlos como los “registros de actividad” que realizan nuestros dispositivos: la hora a la que realizas una llamada, a quién y cuánto dura, o cuánto tiempo estamos viendo un vídeo en redes sociales. Igualmente, este concepto abarca todo aquello que hacen nuestros dispositivos de forma mecánica: contar los pasos que damos, ubicar nuestra geolocalización o detectar nuestros latidos mientras dormimos. Estos hechos por sí solos pueden llegar a parecer inocuos, pero debemos tener en cuenta que los metadatos se generan de manera automática, por lo que apenas tenemos control sobre ellos. Son las máquinas las que se encargan de crearlos, recopilarlos y analizarlos. Como señala Snowden (2019, p. 247), «nuestros dispositivos están constantemente emitiendo comunicaciones en nuestro nombre, queramos o no».

Este autor insiste en que es cierto que la mayoría de nosotros interpretamos la vigilancia a gran escala atendiendo al contenido del mensaje que emitimos o recibimos. Recordemos cómo Shannon (1949) argumentaba que el contenido de los mensajes era irrelevante para la cuestión de la ingeniería del almacenamiento y la transmisión, por lo cual tampoco el contexto de divulgación y recepción de mensajes se consideraba digno de atención.

Al entender los metadatos como una cuestión meramente técnica, el contenido no tendría conexión con ellos. Amparándose en esta reduccionista concepción de la privacidad como exclusivamente relacionada con el contenido, Snowden señala que algunos portavoces de agencias de vigilancia estadounidenses intentaron argumentar que recopilar metadatos no constituía vigilancia. El hecho de que estas agencias de seguridad afirmasen tener poco interés en ese contenido hace que nuestra preocupación sobre la vigilancia que pueden ejercer sea menor (Snowden, 2019, p. 246). Sin embargo, continúa el alertador asilado en Rusia, el contenido de nuestra comunicaciones puede no llegar a exponernos tanto como los patrones de conducta que se pueden extraer de los metadatos que lo acompañan:

Este hecho es el que anula la afirmación de cualquier gobierno de que los metadatos, de algún modo, no son una ventana directa a la sustancia de una comunicación, separan el grano de la paja. Por este motivo, es mejor considerar los metadatos no como una especie de abstracción benigna, sino como la esencia misma del contenido: es precisamente la primera línea de información que busca quien te vigila (Snowden, 2019, p. 247).

Según Zuboff (2019/2020), otra de las excusas que se suele argumentar —en este caso las empresas que recopilan estos metadatos— tiene que ver con que «éstos son agregados en bloque para un gran número de usuarios individuales» (p. 331), hecho que provoca que a estas escalas los individuos no puedan ser identificados. Si llegados este punto de la lectura todavía no he sido suficientemente clara para ilustrar los daños de privacidad a escala colectiva que estas recopilaciones masivas individuales pueden provocar, añadiré que Zuboff (2019/2020, p. 782) desmonta exhaustivamente esta justificación a partir de la constatación de lo cada vez más sencillo que resulta para la «ciencia de la reidentificación» que comprueban que resulta sorprendentemente sencillo desanonimizar los metadatos.

Para Mattelart y Vitalis (2014/2015), la fiebre securitaria no hace sino aumentar la necesidad de conocimiento y anticipación que se extrae de la información y datos recopilados a través de la observación y la vigilancia: «Los atentados aparentan justificar un refuerzo securitario si bien éste ya existía de antes» (p. 131). De hecho, según Lyon (2015, p. 67), durante el 2013, la Casa Blanca afirmó que los métodos de rastreo de la NSA habían descubierto más de 50 complotos terroristas. Sin embargo, continúa el autor, este anuncio pronto quedó refutado y, tras un análisis independiente de la New America Foundation en enero de 2014 se demostró que de 225 casos de actividad terrorista que la NSA dijo fueron investigados, solo cuatro fueron el resultado del uso de metadatos y ninguno de ellos sirvió para prevenir ningún ataque. El informe concluía con que:

la vigilancia de los metadatos de los teléfonos estadounidenses no tuvo ningún impacto discernible en la prevención de actos de terrorismo y sólo el más marginal de los impactos en la prevención de actos de terrorismo. Prevenir actividades relacionadas con el terrorismo, como la recaudación de fondos para un grupo terrorista (Moskowitz, 2014, citado en Lyon, 2015, p. 67).

Para Véliz (2020/2021, p. 52), las actividades relacionadas con el terrorismo, por resultar poco habituales, suponen que sus labores de prevención a través de la vigilancia masiva resulten poco útiles, ya que recolectan más información irrelevante que significativa, añaden más ruido que claridad y

dificultan el trabajo de las agencias de seguridad.

Vigilancia maquínica

Si consideramos que habitamos en un mundo donde gran parte de nuestros datos personales son recolectados y examinados por máquinas (Véliz, 2024, p. 200), ello plantea el dilema de si resulta más beneficioso para la privacidad que sean los algoritmos quienes filtren en vez de que sean los seres humanos los que realicen dicha labor, bajo el argumento de que a nadie le inquietaría suponer que un algoritmo “conociera” información acerca de nuestra vida privada. Aunque esto también es analizado por Lessig en el Capítulo 11 de *El Código 2.0*, (pp. 340 y ss.), para esta autora, existe una percepción de que, en términos de privacidad, resulta más alarmante que un ser humano examine nuestra información personal a que un algoritmo lo haga, hecho que proviene de la creencia de que los algoritmos no son nuestros iguales:

Los algoritmos informáticos no se preocupan por los detalles íntimos de nuestra vida como lo haría un ser humano: no son seres sensibles y no comprenden la vida social como nosotros. Los algoritmos no juzgan; no se excitan al ver un cuerpo desnudo; no sienten repugnancia ni indignación; no se quedan mirando; no chismorrean; no se ríen de nuestras faltas. Y los algoritmos no son agentes morales; no son responsables ni autónomos (en el sentido filosóficamente rico de tener autonomía moral) (Véliz, 2024, p. 200).

Sin embargo, el hecho de que a través de una mediación maquínica de nuestra vigilancia no se vea comprometida nuestra intimidad y no suframos un juicio moral sobre nuestras acciones, no significa que ceder la toma de decisiones a un algoritmo no suponga un perjuicio sobre nuestra privacidad.

En primer lugar, nos enfrentamos a los riesgos derivados de la recopilación de datos, pues una vez que estos son recopilados pueden utilizarse contra nosotros, como ya hemos visto anteriormente. También existe la amenaza de que sean robados o tengan acceso a ellos personas u organismos que quieran causarnos un perjuicio. Por otro lado, tal y como dice Véliz (2024, p. 201) en última instancia las personas que lo encargaron, diseñaron e implementaron son las responsables de dicha recopilación de datos y de una hipotética violación de la privacidad de las personas afectadas, en el caso de que no llevarsen a cabo dicha compilación sin una razón justificada y el consentimiento expreso de las afectadas.

En segundo lugar, con la vigilancia maquínica nos enfrentamos al ya mencionado problema de la agregación, pues los algoritmos pueden inferir información sensible a partir de información no sensible. Si se recopilan nuestros datos y se deduce información sensible sobre nosotros, nuestro derecho a la

privacidad está siendo violado, como apuntamos, no por los algoritmos en sí, sino por las personas que acceden a esos datos o se encuentran en una posición en la que pueden acceder a ellos.

Si cuestionamos además con qué clase de datos — desfasados, sesgados, discriminatorios— se está “nutriendo” a estos algoritmos, el resultado de su toma de decisiones no puede ser otro que el de aumentar las desigualdades sociales (O'Neill, 2016/2017). Por otro lado, tal y como indica Paola Ricaurte (2023, p. 46):

la automatización de lo social a través del uso de tecnologías implica que la opresión pueda deslindarse de sus causas. Al automatizar las decisiones, a nivel estatal o corporativo, los resultados de esos modelos automatizados pueden ser atribuidos a la agencia maquínica y desligados de la agencia humana. Así, los actores sociales pueden deslindar su responsabilidad en la producción de la violencia estructural y la desigualdad resultante.

Uno de los ejemplos más terribles sobre la automatización de las decisiones humanas por medios algorítmicos lo encontramos el programa Lavender (Pascual, 2024), utilizado por el ejército israelí para detectar y bombardear posibles objetivos enemigos. Este sistema es el medio clave utilizado para efectuar bombardeos en la Franja de Gaza sin apenas comprobaciones exhaustivas de si los objetivos son o no civiles.

Lavender no es más que un modelo probabilístico que trabaja con estimaciones y, en consecuencia, comete errores. Según fuentes oficiales mencionadas en el informe en el que se basa el artículo (Pascual, 2024) no está claro qué criterios se utilizan para identificar a los objetivos, si bien menciona algunos generales como el cambio frecuente de teléfono o que sean de género masculino. Lavender tiene un margen de error del 10%, lo que ha llevado a la muerte de miles de palestinos sin vínculo con militantes. Además, se complementa con otros sistemas para rastrear y atacar a individuos marcados, procesando información de más de 2,3 millones de residentes en la Franja de Gaza.

Esto corrobora la masiva red de vigilancia digital a la que todos los gazatíes están expuestos. Quienes a su vez son calificados con una puntuación entre 1 y 100, de menor a mayor probabilidad estimada de que se relacionen con el brazo armado de Hamás o la Yihad Islámica; aquellos que obtienen las calificaciones más altas son asesinados junto a sus familiares y vecinos.

El otro punto sobre el que incide Véliz (2024, p. 201) tiene que ver con la falacia de que las empresas tecnológicas presentan sus tecnologías como “inteligentes” y “autónomas” cuando la mayoría de las veces son los seres humanos los que todavía están detrás de esa supuesta autonomía. Es decir, resulta

tan complicado y costoso construir sistemas que estén completamente controlados por “inteligencia artificial”, que las empresas tecnológicas terminan haciendo que los seres humanos realicen el trabajo complementando, entrenando o sustituyendo por completo los algoritmos.

En este caso, destaco cómo Verónica Smink (2023) recoge el hecho de que existe una «fuerza laboral oculta» (párr. 9) —como la definió la asociación no lucrativa Partnership on AI (PAI), que reúne a entidades académicas, de la sociedad civil, de los medios y de la industria en general que están involucradas con la Inteligencia Artificial— detrás de sistemas como ChatGPT. Se trata de trabajadores contratados por grandes corporaciones tecnológicas, en general en países pobres en el hemisferio Sur, para “entrenar” a estos sistemas. Estos individuos llevan a cabo una labor monótona pero vital para el correcto funcionamiento de este tipo de programas, al categorizar millones de datos e imágenes para enseñarle al *software* cómo proceder.

Estos profesionales, más conocidos como “etiquetadores de datos” (*data labelers* en inglés), identifican datos como textos, imágenes y vídeos, y señalan al *software* qué es qué, de manera que la máquina pueda comprender qué representa cada elemento y aprender en qué situación utilizarlo. En el sector tecnológico, a este tipo de labor se le denomina “enriquecimiento de datos”. Sin embargo, pese a ser una labor crucial para el progreso de la llamada “Inteligencia Artificial”, los enriquecedores de datos constituyen el elemento más débil —y peor pagado— en la cadena productiva de las grandes compañías tecnológicas. De acuerdo con el informe del periodista Billy Perrigo (citado en Smink, 2023), OpenAI tercerizó el trabajo de enriquecimiento de datos mediante una empresa de *outsourcing* llamada Sama, con base en San Francisco, que empleó a empleados en Kenia para llevar a cabo dicho proyecto.

Por todo ello podemos concluir este punto con dos afirmaciones: en primer lugar, que la vigilancia maquínica en muchas ocasiones no es tal, puesto que sigue necesitando una mediación humana para poder llevarse a cabo; y en segundo lugar, que donde no ocurre esto, dicha vigilancia maquínica se enfrenta a una serie de decisiones que favorecen la discriminación, al estar constituidas por datos sesgados, por lo que invalidan la presunción de que son menos perniciosas que la intervención humana.

2.3.5. Extractivismo de datos personales

¿Cómo entendemos nuestra relación con los datos y con cómo son captados por diferentes organizaciones a través de la vigilancia?

Según Kienscherf (2022, p. 20), muchos estudiosos de la comunicación, en particular aquellos de tradición marxista, sostienen que esta relación implica formas de trabajo que también están sujetas a

explotación. Otros investigadores, por su parte, entienden que los usuarios son fuentes de materia prima que se les extrae para convertirla algorítmicamente en perfiles predictivos. A este autor le surge entonces la siguiente pregunta de indudable pertinencia teórica: ¿este capital de vigilancia se valoriza a través de la explotación del trabajo de los usuarios de diversas plataformas o a través de la extracción de sus datos como materia prima?

Para resolverla conviene repasar el concepto de explotación del trabajo en la obra de Marx (1867/1975), quien explica que en los mercados competitivos la explotación del trabajo es la fuente de las ganancias para los capitalistas, ya que el valor de una mercancía se determina por el tiempo de trabajo socialmente necesario. A partir de aquí, la obtención de «plusvalor» o «plusvalía» por parte de los capitalistas deriva de la explotación que se da cuando los trabajadores son obligados a trabajar más tiempo o de forma más productiva de lo necesario para reproducir el valor de su fuerza laboral. La reinversión continua de, al menos, parte de la plusvalía obtenida es lo que define al capitalismo, a través de la acumulación capitalista. Esta acumulación depende de la mercantilización de la fuerza laboral y de la explotación de los trabajadores.

Ya hemos visto cómo dicha mercantilización de la fuerza laboral fue resultado de procesos históricos violentos designados por Marx como «acumulación primitiva», manifestada en el cercamiento de bienes comunes, la expropiación de tierras indígenas en las Américas y la expropiación de mano de obra africana, sin olvidar el añadido ya mencionado de Federici (2004/2010) sobre la «caza de brujas»:

Este proceso requirió la transformación del cuerpo en una máquina de trabajo y el sometimiento de las mujeres para la reproducción de la fuerza de trabajo. [...] La acumulación primitiva no fue, entonces, simplemente una acumulación y concentración de trabajadores explotables y capital. Fue *también una acumulación de diferencias y divisiones dentro de la clase trabajadora*, en la cual las jerarquías construidas a partir del género, así como las de “raza” y edad, se hicieron constitutivas de la dominación de clase y de la formación del proletariado moderno (p. 90).

Este traumático proceso trastocó los modos de vida tradicionales para servir a los imperativos de la acumulación capitalista. De hecho, para muchos autores, incluidos los citados Kienscherf (2022, p. 21) y Federici (2004/2010, p. 89), la acumulación primitiva sigue desempeñando un papel clave en la acumulación capitalista. Sin embargo, Kienscherf introduce aquí las muy estimables apreciaciones de Nancy Fraser sobre cómo es necesario desplazar el foco «de la historia principal de la explotación a la historia de fondo de la expropiación» (Fraser, 2014, p. 60). Según la filósofa estadounidense, debemos

entender el capitalismo como un orden social institucionalizado que delimita y depende de esferas externas, y que no solo suministra trabajadores y medios de producción por debajo del valor o “gratis”, ya que también contribuye finalmente a salvaguardarse a sí mismo de sus propias tendencias a la crisis, así como de la resistencia de la clase obrera.

Debemos atender también a que la actividad social y reproductiva es absolutamente necesaria para la existencia del trabajo asalariado, la acumulación de plusvalía y el funcionamiento del capitalismo como tal. El trabajo asalariado no podría existir sin el trabajo doméstico, la crianza de los hijos, la escolarización, el cuidado afectivo y una serie de otras actividades que ayudan a producir nuevas generaciones de trabajadores y a reponer las existentes, así como a mantener los vínculos sociales y los entendimientos compartidos (Fraser, 2014, p. 61).

Sobre esto, Kienscherf (2022, p. 21) observa cómo existe un número cada vez mayor de actividades socio-reproductivas que son externas a la acumulación capitalista pero que también son necesarias para ella. Ello incluye muchas formas de actividades sociales puramente recreativas que ahora ocurren en plataformas en línea donde se producen medios de producción gratuitos para las mercancías del llamado capitalismo de la vigilancia.

¿Son por tanto los argumentos de que estos capitalistas de la vigilancia obtienen sus ganancias de la extracción de “datos en bruto” más acertados que las teorizaciones de los académicos que tienden a estirar el concepto de explotación marxista para que se ajuste a las formas en que se crea valor digitalmente?

Como adelanté en el apartado “*Datos en bruto*” como *oxímoron*, el problema en esta lógica radica en que aceptarla significa interpretar los datos personales que los usuarios producen consciente o inconscientemente en el curso de sus interacciones en línea como materia prima, lo cual justificaría la apropiación de estos flujos de datos (Kienscherf, 2022, p. 22). Estos marcos discursivos reflejan las narrativas utilizadas para justificar y naturalizar rondas anteriores de acumulación primitiva en términos de derechos de propiedad exclusivos. El autor se apoya en las tesis de Julie Cohen (2019, pp. 48-49) para explicar que la expropiación de datos personales por parte del capital de la vigilancia depende de la idea de un «dominio público biopolítico» donde suministros casi inagotables de datos supuestamente en bruto y potencialmente valiosos están a disposición de las corporaciones.

En una línea similar, Zuboff (2019/2020) alerta de cómo los capitalistas de la vigilancia parten del supuesto de que los flujos de datos de los usuarios son meros productos de desecho para cuyo uso productivo los propios usuarios no están ni dispuestos ni capacitados, mientras que ellos sí tienen la

habilidad de convertir estos flujos superfluos de datos en mercancías valiosas.

Sin embargo, como ya hemos visto con Gitelman (2013), los datos no están esperando a ser descubiertos como si se diesen de forma natural, sino que son una abstracción registrada del mundo creada y valorizada por personas que usan la tecnología. En suma, las tesis que postulan la existencia de “datos en bruto” como un recurso natural ubicuo y gratuitamente disponibles para que los actores corporativos dotados de los medios tecnológicos para “cocinarlos” los aprovechen y conviertan en productos valiosos, no hacen sino facilitar y naturalizar procesos de expropiación a una escala inimaginable.

A todo ello añade Kienscherf la diferencia decisiva que existe entre la expropiación de datos y la de tierras u otros bienes similares. De este modo, rescatando un argumento clásico popularizado por autores como Boyle (2003, pp. 41-42, citado en Kienscherf, 2022, p. 22) o Lessig (2001/2009, pp. 294-296), Kienscherf subraya que, a diferencia de los recursos tangibles, como la tierra, el agua o el petróleo, los datos constituyen bienes no son rivales y no exclusivos. Esto significa que, una vez que se publica un conjunto de datos, este se vuelve accesible a un número potencialmente ilimitado de usuarios (pues la única información sobre la que se puede reclamar exclusividad es aquella que se mantiene en secreto), y además estos pueden utilizarlo de distintas maneras y al mismo tiempo para satisfacer sus necesidades (no hay rivalidad en su consumo y disfrute)

Además, Kienscherf (2022, p. 23) sugiere que los argumentos de que el capital de la vigilancia depende de la extracción de datos como materia prima asignan también un papel meramente pasivo a los usuarios y, por lo tanto, pasan por alto una diferencia crucial entre los medios masivos y las plataformas en línea, esto es, la participación activa de aquellos en la producción de contenido y tecnología. Por tanto, el autor subraya que quienes participan en plataformas digitales producen datos mientras reproducen, no solo su propia fuerza de trabajo y la de otras personas, sino también a sí mismos y a los demás como seres sociales.

De esta manera, las plataformas se convierten en la infraestructura central por medio de la cual los capitalistas de la vigilancia convierten las interacciones productivas, socio-reproductivas y recreativas de las personas en trabajo gratuito para su beneficio. Estas plataformas permiten canalizar actividades que ocurren fuera de la lógica de la acumulación capitalista, aunque son una condición para su reproducción, hacia procesos de valorización. Al participar en estas actividades a través de plataformas privadas, los usuarios producen datos que luego son expropiados mediante la vigilancia ubicua que en ellas opera. Sin embargo, a diferencia de otras formas de acumulación primitiva, la desposesión de los

usuarios de las plataformas no implica tanto una coerción directa, como la aceptación sin negociación de un consentimiento contractual de la expropiación de sus datos. Los usuarios de las plataformas, consciente o inconscientemente, de manera activa o pasiva, producen datos que son expropiados y, según Cohen (2019, p. 64) «entran en un proceso de producción industrial durante el cual se refinan para generar dobles de datos: plantillas de información».

A modo de conclusión, Kienscherf (2022, p. 23) afirma que existen dos fuentes de valor y plusvalía a través de la mercantilización de los datos personales: su producción de forma gratuita por parte de los usuarios y el valor agregado a través del cual estas plataformas convierten dichos datos en mercancías. En consecuencia, las plataformas convierten la actividad de sus usuarios en trabajo gratuito, pero se trataría más de una expropiación del trabajo que de una explotación del mismo. Sin embargo, esta forma de expropiación del trabajo, sostengo, puede explicarse mejor a través del concepto de “extractivismo de datos personales”, que utilizan autoras como Paola Ricaurte (2023, pp. 22-23):

En las comunidades ancladas al territorio se comprende bien el extractivismo no en términos abstractos, sino como experiencia de vida de un proceso de despojo que ha sido histórico y sistemático. El extractivismo en los territorios, aunque en primera instancia hace alusión al despojo de los recursos naturales, en última instancia significa sacar de su lugar, descolocar, privar a las comunidades de las formas de sostenimiento de la vida. Esas formas de sostenimiento de la vida incluyen formas de organización comunitaria, saberes ancestrales, tecnologías, cosmovisiones, espiritualidades, semillas originarias, prácticas para afianzar el tejido social, formas de construir el sentido de lo común e imaginarios de futuro. Por esta razón, es fundamental comprender el extractivismo como un proceso asociado con el despojo de los cuerpos-territorios tanto en su sentido material como inmaterial y relacional. Los bienes comunes amenazados no son solamente los que se toman de la tierra, la amenaza real es la imposibilidad de continuar la vida.

En esta tesis defiendo que, al extractivismo todavía imperante de materias primas para la elaboración del *hardware* que hace posible recopilar y almacenar nuestros datos que veíamos al principio, hoy se suma también un extractivismo de nuestros comportamientos y relaciones, los cuales son mediados a través de dichos dispositivos para entrenar un *software* orientado a nuestra vigilancia. Esta definición tan compleja y profunda de lo que supone el «extractivismo» como proceso «histórico y sistemático» es completada por Ricaurte (2023, pp. 32-33) con una puntualización referente a su deriva ligada a las tecnologías digitales y los datos personales:

La colonialidad de la tecnología asociada con la digitalización del mundo y la automatización de la sociedad (Stiegler, 2018) se manifiesta a través de procesos epistémicos que ejercen violencias estructurales a escala. Estos procesos comienzan con el extractivismo de los cuerpos-territorios, pero se encuentran asociados a procesos cognitivos que median nuestra relación con el mundo. Esos procesos son la dataficación, la conversión del mundo en datos que puedan procesarse para ser monetizados; la mediación algorítmica, para generar modelos que permitan la predicción del futuro a partir del análisis de los datos extraídos; y, por último, la automatización, que posibilita la toma de decisiones a partir de esos modelos (Ricaurte, 2022). Así se cierra el ciclo de la producción de un orden de conocimiento que se instaura como la versión legitimada algorítmicamente de la realidad.

2.4 Desimplantar Matrix de la matriz¹⁴

La digitalización y datificación de algunas de nuestras interacciones, tanto sociales como con nuestro propio cuerpo, en ocasiones interseccionan con otros ámbitos que en un primer momento no asociamos a esta esfera de la vigilancia maquínica y que, sin embargo, en la actualidad se pueden ver afectadas. El caso que presento a continuación permite dar buena cuenta de ello.

Para introducirlo debemos detenernos en una fecha y lugar concretos, el 24 de junio de 2022, día en el que el derecho al aborto en EEUU dejó de estar blindado constitucionalmente. Ese día, la Corte Suprema concluía en el caso «Dobbs contra Jackson Women's Health Organization», y por cinco votos contra cuatro, que la Constitución estadounidense no contempla este derecho. Ello revocaba la jurisprudencia previa de «Roe contra Wade» (1973), ratificada por «Planned Parenthood contra Casey» (1992), que dotaba a este derecho de amparo constitucional e impedía que cada Estado pudiera legislar a su conveniencia hasta su prohibición.

El camino hacia la conquista de este derecho, en el caso estadounidense, no fue una tarea sencilla. Para empezar, la sentencia de «Roe contra Wade» que fue publicada dos días después de que Nixon jurase su segundo mandato, contó con dos magistrados menos de los habituales prestando servicio para su ratificación, tal y como apunta Pérez Alonso (2023, p. 531). Junto a ello, y a diferencia de otras sentencias del mismo tribunal, la doctrina «Roe contra Wade» siempre estuvo envuelta en gran controversia y fue núcleo de una continua disputa política centrada en si los detractores a esta doctrina ostentaban o no la mayoría en la corte Suprema para conseguir su futura derogación.

Según Pérez Alonso (2023, pp. 534-535), el núcleo doctrinal de «Roe contra Wade» se encuentra en los apartados VIII y X: en el primero se ancla el aborto al derecho constitucional a la intimidad, cuyo reconocimiento se entiende implícito en la Decimocuarta Enmienda, aunque en este sentido debemos tener en cuenta el fundamento VIII de la sentencia (citado en Pérez Alonso, 2023, p. 534):

La Constitución [estadounidense] no menciona explícitamente ningún derecho a la intimidad. Sin embargo, en una serie de resoluciones que se remontan quizá a *Union Pacific R. Co v. Botsford*, 141 U.S. 250, 251 (1891) el Tribunal ha reconocido que el derecho a la intimidad personal, o a garantizar ciertas áreas o zonas de intimidad, existe bajo la Constitución. En diversos contextos, el Tribunal o algunos de sus jueces han encontrado al menos raíces de tal derecho en la Primera Enmienda [...] en la Cuarta y

¹⁴ Este apartado se basa en (y toma su título de) un capítulo escrito junto con Marina Gómez Alcalde (Solera y Gómez Alcalde, 2025) para el libro *Algoritarios II*, [pendiente de publicación].

Quinta Enmiendas [...] en la Novena Enmienda [...] o en el concepto de libertad garantizado en el primer párrafo de la Decimocuarta Enmienda constitucional [...]. Estas resoluciones dejan claro que sólo los derechos individuales que puedan considerarse «fundamentales» o «implícitos en el concepto de libertad ordenada» [...] se incluyen en esta garantía de intimidad personal [...]. Este derecho a la intimidad, ya encuentre su base en el concepto de libertad personal de la Decimocuarta Enmienda y en las restricciones a la acción estatal, como creemos lo está, o, como el juzgado de distrito concluyó, en los derechos que el pueblo conserva según la Novena Enmienda, es lo suficientemente amplio para abarcar la decisión de una mujer de terminar su embarazo.

Sin embargo, el derecho al aborto no era ni absoluto ni ilimitado, dado que en el apartado X se especificó una serie de plazos dentro del periodo de gestación —dividido en trimestres— según los cuales se regulaba la posibilidad o no de continuar con el mismo. Así, la libertad de elección pasaba de total durante el primer trimestre hasta llegar a ser suprimida en el tercero.

Con «Roe contra Wade» se intentó solucionar un asunto que provocaba sentimientos encontrados, lo que dio combustible efectivo a quienes acusaban al Tribunal Supremo estadounidense de ejercer un activismo judicial injustificado ya desde la etapa previa (1953-1969) del llamado Tribunal Warren (Lessig, 2006/2009, pp. 492-494). Lo que también provocó que los partidarios del derecho al aborto se organizaran de la misma manera que sus detractores, generando así dos potentes grupos de presión a favor y en contra de la resolución.

Si bien los casos surgidos a partir de 1973 no afectaron a la tipificación penal del derecho al aborto, sí es cierto que se fueron aprobando leyes que introducían requisitos procedimentales, financieros o técnicos para llevarlos a cabo, las cuales sí fueron avaladas constitucionalmente por el Tribunal Supremo de los EEUU (Lessig, 2006/2009, p. 221; Pérez Alonso, 2023, pp. 538-539). La sentencia más importante en este sentido fue la del citado «Planned Parenthood contra Casey» (1992), que finalmente ratificó el derecho al aborto aprobado con «Roe contra Wade», aunque eliminó la división en trimestres para adoptar un concepto de “viabilidad” del feto que abría la puerta a prohibir embarazos antes del segundo trimestre (Pérez Alonso, 2023, p. 547).

Durante los años que siguieron a «Planned Parenthood contra Casey» hubo cierta tregua sobre este tema dentro de los nombramientos (vitalicios) de los jueces del Tribunal Supremo por parte del Senado de EEUU. Sin embargo, la situación cambió radicalmente cuando falleció una de las juezas de corte progresista a menos de quince días de que iniciasen su año judicial 2020-2021 y a menos de mes y

medio de las elecciones presidenciales. En contra de la tradición establecida, el Partido Republicano nombró a una nueva jueza conservadora antes del cambio de gobierno, lo que constituyó una sólida mayoría, de al menos cinco jueces, contraria a «Roe contra Wade» (Pérez Alonso, 2023, pp. 549-550).

El caso que finalmente hizo caer dicha doctrina fue el citado «Dobbs contra Jackson», en el que la clínica reproductiva Jackson Women's Health Organization (que acabó obligada a cerrar en julio de 2022) impugnó la constitucionalidad de la *Gestational Age Act* de 2018 del Estado de Mississippi (Pérez Alonso, 2023, p. 551). Lo llamativo del asunto es que, pese a que en su recurso a las iniciales sentencias favorables a la clínica el Estado de Mississippi descartaba su vínculo con la derogación de las doctrinas que avalaban el derecho al aborto, el Supremo acabó poniéndola sobre la mesa en su escrito de formalización de mayo de 2021 (citado en Pérez Alonso, 2023, p. 552):

Roe y *Casey*, por tanto, están en contradicción con la respuesta directa y constitucionalmente fundamentada a la cuestión que se plantea. Por tanto, la pregunta pasa a ser si este Tribunal debe rectificar tales sentencias. Y debe. Los motivos para rectificar *Roe* y *Casey* son abrumadores. *Roe* y *Casey* son una equivocación manifiesta. La conclusión de que el aborto es un derecho constitucional carece de base en el texto, estructura, historia o tradición.

Ambas doctrinas fueron finalmente derogadas con dos justificaciones: por un lado, que en la Constitución estadounidense no se hace mención expresa ni al derecho al aborto ni incluso al de la intimidad en el que aquel está anclado; y por otro lado, que ya existían normas punitivistas en torno a la interrupción del embarazo en distintos Estados antes de la firma de la Constitución. Sin embargo, con respecto a estas justificaciones el (prolijo) voto particular discrepante redactado por los magistrados Breyer, Sotomayor y Kagan¹⁵ afirma lo siguiente:

Como cuestión inicial, nótese un error en la sentencia inmediatamente precedente. Allí nos referimos al “pueblo” que ratificó la Decimocuarta Enmienda [...]. Pero, por supuesto, el «pueblo» no ratificó la Decimocuarta Enmienda. Lo hicieron hombres. Así que quizá no sea tan sorprendente que [...] no estuviesen en perfecta sintonía con la importancia de los derechos reproductivos para la libertad de las mujeres o para su capacidad de participar como miembros iguales de nuestra Nación. [...] La ley tampoco protegía entonces (y no lo haría durante años) [...] los derechos reconocidos en los casos *Lawrence* y *Obergefell* a la intimidad y el matrimonio homosexual. No protegía el derecho reconocido en *Loving* a

¹⁵ Extraído de la sentencia completa en inglés disponible aquí: https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf

matrimonios interraciales. No protegía el derecho reconocido en *Griswold* al uso de anticonceptivos [...]. Tratándose de método constitucional, la adhesión de la mayoría a replicar en 2022 cada visión del significado de libertad sostenida en 1868 tiene muy poco de recomendable. Nuestra doctrina en esta esfera constitucional, como en la mayoría de esferas, ha procedido desde hace décadas de modo muy diferente. [...] En última instancia, afirma la mayoría, todo lo que debe alegar para derogar la jurisprudencia es esto: que cree que *Roe* y *Casey* eran «egregiamente erróneas». [...] La mayoría [...] siempre las ha despreciado y ahora posee los votos para desecharlas.

Tal y como apunta Silvia Federici (2020/2022), esta continua búsqueda de la criminalización del derecho al aborto en EEUU tiene como telón de fondo el valor económico de la reproducción que el desarrollo tecnológico del capitalismo no ha hecho sino agudizar. No en vano, aunque se predique la superfluidad de la fuerza de trabajo humana, ésta sigue siendo imprescindible para la acumulación de capital, sea como trabajadores, consumidores o soldados: «Controlar el cuerpo de la mujer es tan importante para la clase capitalista que, incluso en Estados Unidos, donde el aborto fue legalizado en la década de 1970, se sigue intentado revertir esta decisión» (Federici, 2020/2022, p. 38).

Hoy esta advertencia de Federici se ha cumplido, como aquella de Simone de Beauvoir que exhortaba a que no olvidemos que «basta una crisis política, económica o religiosa, para que los derechos de las mujeres vuelvan a ser cuestionados. Esos derechos nunca se dan por adquiridos. Debéis permanecer vigilantes durante toda vuestra vida». Como consecuencia, muchos Estados vieron el cielo abierto para intentar instaurar o endurecer la persecución al derecho al aborto, si bien al final de esta sección revisaré adónde han llegado en tal empeño:

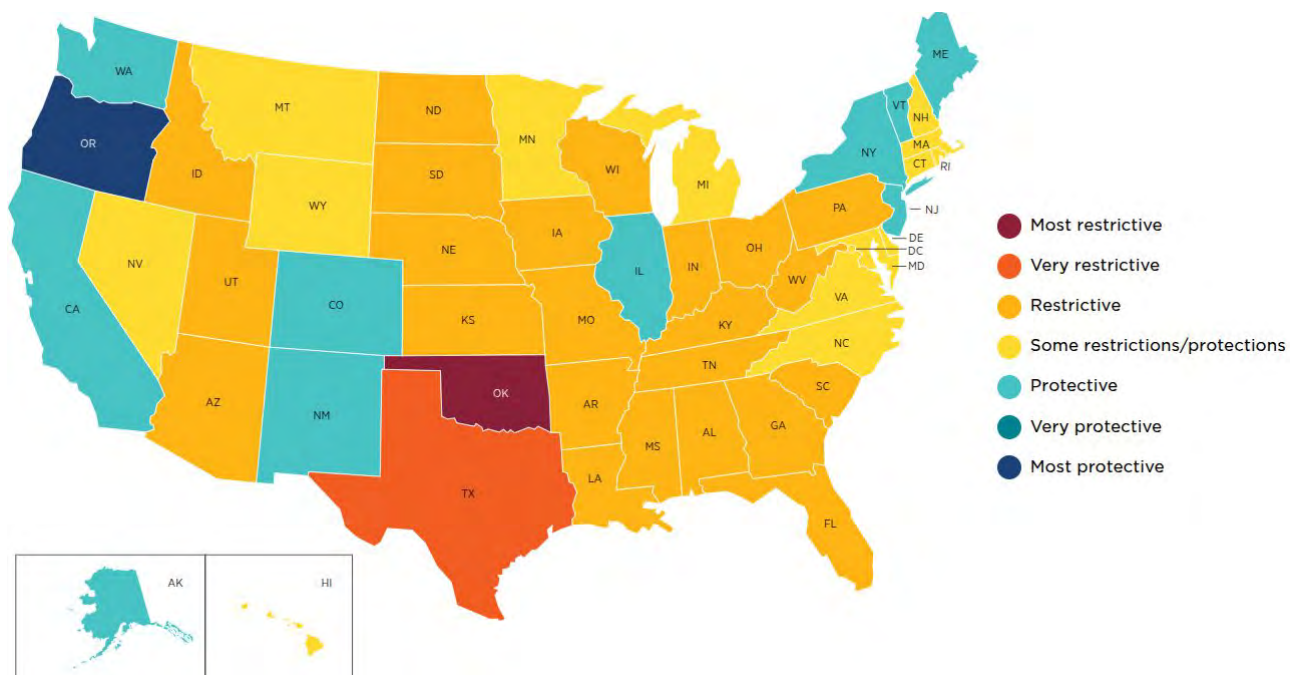


Figura 12. Mapa de las políticas sobre el aborto en EEUU a 9 de junio de 2022. Instituto Guttmacher¹⁶.

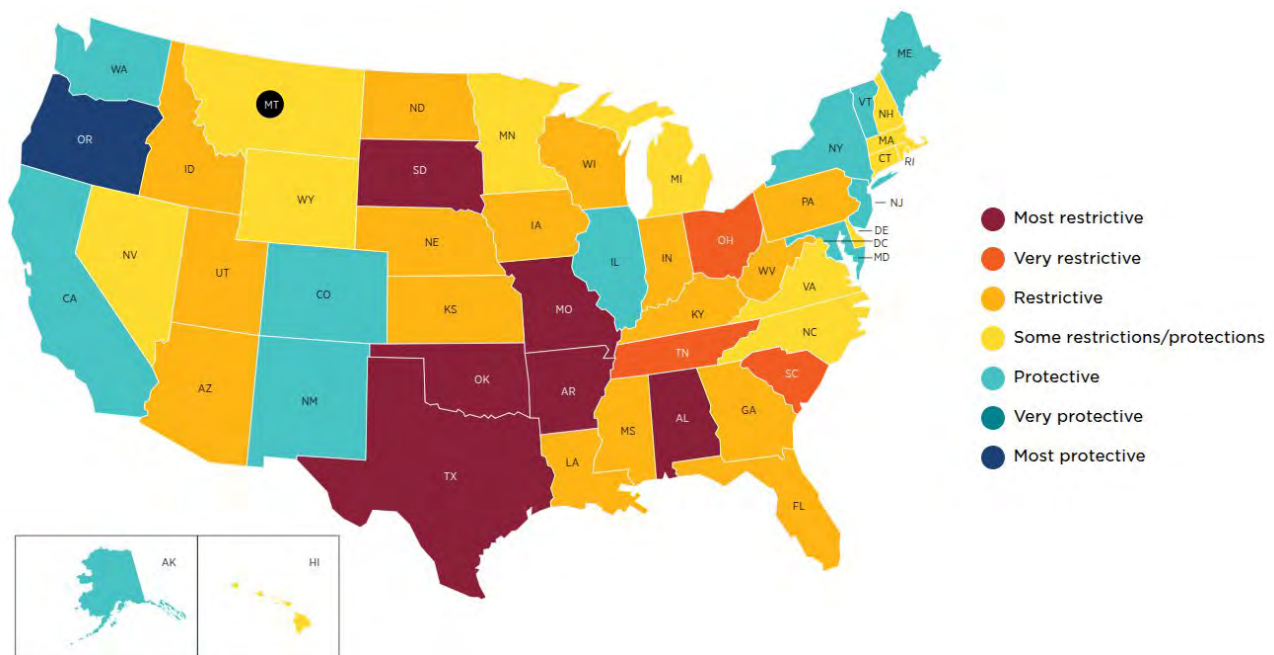


Figura 13. Mapa de las políticas sobre el aborto en EEUU *post* «Roe vs. Wade», a 24 de junio de 2022. Instituto Guttmacher¹⁷.

Sin embargo, el retroceso en algunos Estados, en materia de derechos reproductivos, presenta otro componente de cariz tecnológico. Si un año antes de la aprobación de «Roe contra Wade», integrantes del grupo Jane Collective (que ofrecía servicios de interrupción del embarazo en Illinois cuando éste

¹⁶ Véase: <https://web.archive.org/web/20220621193319/https://states.guttmacher.org/policies/> Para una información actualizada, véase: <https://states.guttmacher.org/policies/abortion-policies> Recuperado el: 17 de febrero de 2025.

¹⁷ Véase: <https://web.archive.org/web/20220626215311/https://states.guttmacher.org/policies/> Para una información actualizada, véase: <https://states.guttmacher.org/policies/abortion-policies> Recuperado el: 17 de febrero de 2025.

todavía era ilegal) tuvieron que destruir las tarjetas con la información personal de sus pacientes en la misma furgoneta de la policía que las llevaba detenidas a comisaría (Hill, 2022, párr. 1-2); 50 años más tarde surgía la duda de cómo se destruirían hoy dichas pruebas incriminatorias si éstas están dispersas por plataformas sociales y aplicaciones de control de ciclo menstrual, en un momento en que diferentes datos (y metadatos) sobre nuestro cuerpo pueden hacer saltar la alarma sobre una posible interrupción del embarazo ante las autoridades.

No estoy aquí promoviendo pronósticos distópicos. Bien al contrario, se trata de situaciones que han sucedido en lugares bastante lejanos de las fábricas de Rumanía de la época de los 80, donde médicos y enfermeros, acompañados por la policía, realizaban controles ginecológicos forzosos a las trabajadoras para dilucidar si se habían sometido a un proceso de interrupción del embarazo —el cual estaba prohibido en dicho país desde 1966—, sometiendo a aquellas que estuviesen embarazadas a un estricto control hasta su alumbramiento (Lersundi, 1987). Hablo, entre otros, del caso de Lattice Fisher, de Mississippi, quien en 2017 fue acusada de asesinato en segundo grado por haber dado a luz a una criatura sin vida en su casa y contar en su historial de navegación con consultas relativas a “Cómo inducir un aborto espontáneo” o “Cómo comprar en línea medicamentos para interrumpir el embarazo” (Zakrzewski *et al.*, 2022). O como el caso de Purvi Patel de Indiana, donde para intentar condenarla se hizo uso de mensajes de textos que ella había enviado a una amiga en los que aludía a la toma de pastillas abortivas en una etapa avanzada del embarazo (Bazelon, 2015).

A la luz (o más bien sombra) de precedentes como estos fue que, durante las deliberaciones del Supremo en 2022, comenzaron a proliferar en diferentes redes sociales publicaciones que combinaban las etiquetas *#roenade* y *#periodtrackingapps* (Gómez Alcalde, 2023), y que anticipaban las amenazas que este cambio legislativo podría acarrear también para quienes usan aplicaciones móviles orientadas al control de ciclo menstrual.

La cuestión es que estas aplicaciones de control de ciclo no se conforman con calcular con mayor o menor precisión nuestras fechas de ovulación y menstruación, sino que también recopilan datos fisiológicos y de comportamiento asociados a los síntomas de nuestro período, e incluso rastrean nuestros movimientos y hábitos de compra y navegación. El valor de la aplicación radica, por tanto, en el volumen de datos que se comparte con ella: a medida que sus usuarias se vuelven participantes activas en el proceso de producción, las líneas divisorias entre quién produce, consume y se beneficia de la información se desvanecen.

Así, ya en mayo Newman (2022) aludía a las guías sobre protección de la privacidad digital que la *Digital*

*Defense Fund*¹⁸ y la *Electronic Frontier Foundation*¹⁹ facilitaban a quienes buscaban datos o servicios relacionados con el aborto en EEUU ante la coyuntura de que éste dejase de ser un derecho constitucional. Otra gran aportación a esta alerta temprana la realizó la socióloga Gina Neff a través de un hilo de (todavía) Twitter inmediatamente posterior a la sentencia del Supremo donde exhortaba a borrar las aplicaciones de seguimiento de ciclo y daba una serie de información sobre lo que se podía hacer al respecto:



Figura 14.: Neff, Gina. [@ginasue]. (2022, 24 de junio). *Right now, and I mean this instant, delete every digital trace of any menstrual tracking. Please.* [Ahora mismo, y me refiero a este instante, borra todo rastro digital de cualquier aplicación de seguimiento menstrual. Por favor.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 15.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Now that I have your attention: we have work to do. A 🇺🇸* [Ahora que tengo vuestra atención: tenemos trabajo que hacer. Abro hilo][Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 16.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Americans lack fundamental privacy protections. Post-Roe makes that tragically clear. For many women, post-Roe privacy is more urgent. But privacy is even more important for ALL of us now.* [Los estadounidenses carecen de protecciones fundamentales para la privacidad. El caso Post-Roe lo deja trágicamente claro. Para muchas mujeres, la privacidad es más urgente después de Roe, pero ahora es aún más importante para TODOS nosotros.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

18 Véase: <https://digitaldefensefund.org/ddf-guides/abortion-privacy>

19 Véase: <https://ssd EFF.org/playlist/reproductive-healthcare-service-provider-seeker-or-advocate>

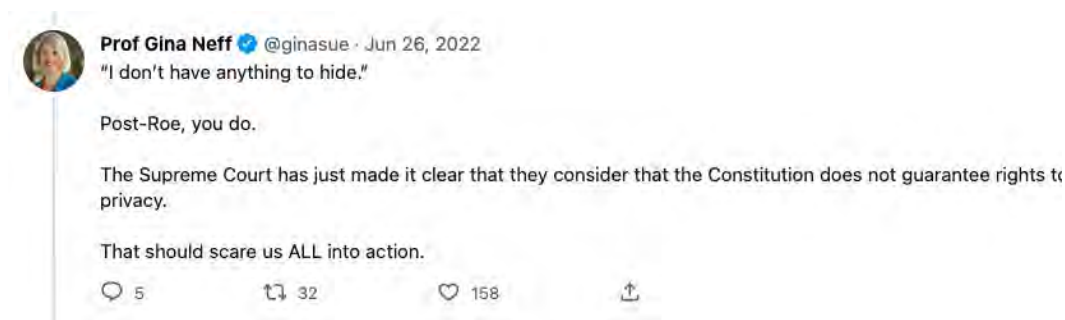


Figura 17.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *"I don't have anything to hide." Post-Roe, you do. The Supreme Court has just made it clear that they consider that the Constitution does not guarantee rights to privacy. That should scare us ALL into action.* [“No tengo nada que ocultar”. Después de Roe, sí lo tienes. La Corte Suprema acaba de dejar claro que considera que la Constitución no garantiza el derecho a la privacidad. Eso debería asustarnos a TODOS y hacernos actuar.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 18.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Here's what you can do: 1) Pay attention to your apps. They are an easy target, and they affect many of us. What are their data policies? How are companies protecting their users? What are their data retention policies? What do app companies do with law enforcement subpoenas?.* [Esto es lo que puede hacer: 1) Presta atención a tus aplicaciones. Son un blanco fácil y afectan a muchos de nosotros. ¿Cuáles son sus políticas de datos? ¿Cómo protegen las empresas a sus usuarios? ¿Cuáles son sus políticas de retención de datos? ¿Qué hacen las empresas de aplicaciones con las citaciones de las fuerzas de seguridad?] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

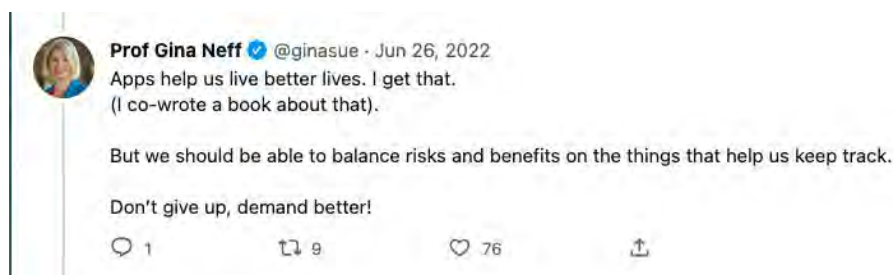


Figura 19.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Apps help us live better lives. I get that. (I co-wrote a book about that). But we should be able to balance risks and benefits on the things that help us keep track. Don't give up, demand better!* [Las aplicaciones nos ayudan a vivir mejor. Lo entiendo (he co-escrito un libro sobre ello), pero deberíamos poder sopesar los riesgos y los beneficios de las cosas que nos ayudan a llevar un registro. ¡No te rindas, exige algo mejor!] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 20.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Many apps collect data that can say intimate things about our health, but that data is not yet protected under US health privacy laws. Don't give up, demand a policy fix for this gap! And don't stop there.* [Muchas aplicaciones recopilan datos que pueden revelar información íntima sobre nuestra salud, pero esos datos aún no están protegidos por las leyes de privacidad de la salud de los EE. UU. No te rindas, exige una política que solucione esta brecha. Y no se detenga ahí.] [Tuit]. Recuperado de:

<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 21.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Law enforcement agencies have already targeted Google searches for "abortion pills", text messages, and DNA databases (Hello 23andMe! And http://Ancestry.com) in prosecuting women for abortions and miscarriages.* [Las agencias de aplicación de la ley ya han puesto el ojo en las búsquedas en Google de "pastillas abortivas", los mensajes de texto y las bases de datos de ADN (¡Hola 23andMe! Y http://Ancestry.com) para procesar a mujeres por abortos y pérdidas de embarazos espontáneos.] [Tuit]. Recuperado de:

<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

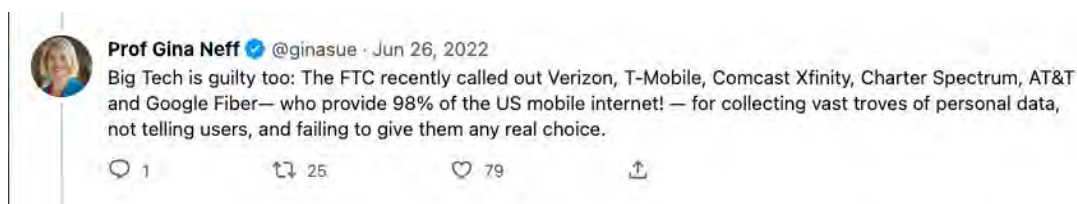


Figura 22.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Big Tech is guilty too: The FTC recently called out Verizon, T-Mobile, Comcast Xfinity, Charter Spectrum, AT&T and Google Fiber— who provide 98% of the US mobile internet! — for collecting vast troves of personal data, not telling users, and failing to give them any real choice.* [Las grandes tecnológicas también son culpables: la FTC recientemente denunció a Verizon, T-Mobile, Comcast Xfinity, Charter Spectrum, AT&T y Google Fiber (¡que proporcionan el 98% de Internet móvil en Estados Unidos!) por recopilar grandes cantidades de datos personales, no informar a los usuarios y no darles ninguna alternativa.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 23.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *So...* [Así...][Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 24.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *2) Up your personal privacy game. One place to start is @Info_Activism's "Security in a Box" https://securityinabox.org/en/ Protect your communications, your passwords, your devices, your files.* [2] Mejora tu privacidad personal. Un buen punto de partida es la sección "Security in a Box" de @Info_Activism

[https://securityinbox.org/en/ Protege tus comunicaciones, tus contraseñas, tus dispositivos, tus archivos.](https://securityinbox.org/en/Protege_tus_comunicaciones_tus_contraseñas_tus_dispositivos_tus_archivos) [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 25.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Loads of handy tips online for smarter personal information security to protect you and your loved ones. We should not stop there – demand better from the companies you use and from our law makers. We deserve privacy! But don't stop there.* [Hay muchos consejos útiles en línea para una seguridad de la información personal más inteligente que te protege a ti y a tus seres queridos. No deberíamos detenernos aquí: exijamos más a las empresas que utilizas y a nuestros legisladores. ¡Merecemos privacidad! Pero no nos detengamos ahí.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 26.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Life in post-Roe America will be harder for poor women, Black women, Hispanic women, immigrant women, underage women, raped women, women in crisis.... I could go on and on. Deleting an app doesn't fix that cold and cruel reality.* [La vida en Estados Unidos después de Roe será más difícil para las mujeres pobres, las mujeres negras, las mujeres hispanas, las mujeres inmigrantes, las mujeres menores de edad, las mujeres violadas, las mujeres en crisis... Podría seguir y seguir. Borrar una aplicación no soluciona esa fría y cruel realidad.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 27.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *3) Support the people and organizations supporting women.* [3) Apoya a las personas y organizaciones que apoyan a las mujeres.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

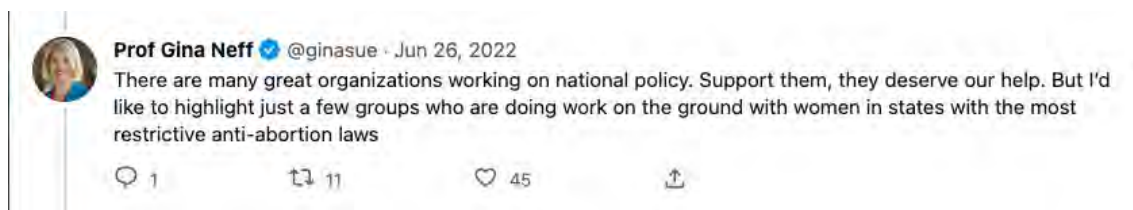


Figura 28.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *There are many great organizations working on national policy. Support them, they deserve our help. But I'd like to highlight just a few groups who are doing work on the ground with women in states with the most restrictive anti-abortion laws.* [Hay muchas organizaciones importantes que trabajan en la formulación de políticas nacionales. Apóyalas, merecen nuestra ayuda. Pero me gustaría destacar sólo algunos grupos que están trabajando sobre el terreno con mujeres en los estados con las leyes antiabortistas más restrictivas.] [Tuit]. Recuperado de:

<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 29.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Close to my Appalachian heart, Holler Health Justice, @HollerHealth a BIPOC- & queer-led racial, economic & reproductive justice nonprofit in West Virginia.* [Cerca de mis queridos Apalaches, Holler Health Justice, @HollerHealth, una organización sin fines de lucro de justicia racial, económica y reproductiva dirigida por personas BIPOC y queer en Virginia Occidental.][Tuit]. Recuperado de:

<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 30.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *The Kentucky Health Justice Network builds the power of Kentuckians to achieve reproductive justice through direct support, education and outreach.* <https://kentuckyhealthjusticenetwork.org>. [La Red de Justicia en Salud de Kentucky fortalece el poder de los habitantes de Kentucky para lograr la justicia reproductiva a través del apoyo directo, la educación y la divulgación. <https://kentuckyhealthjusticenetwork.org>][Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 31.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Texas Equal Access Fund @TEAFund, "making reproductive rights a reality", has been providing direct support in Texas. They are pausing their direct services for the moment, but are still very much in the fight for access to abortion for all.* [El Fondo de Acceso Igualitario de Texas @TEAFund, que "hace realidad los derechos reproductivos", ha estado brindando apoyo directo en Texas. Están suspendiendo sus servicios directos por el momento, pero siguen en plena lucha por el acceso al aborto para todas las personas.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 32.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *The Afiya Center @TheAfiyaCenter "Transforming the lives, health, and overall wellbeing of Black womxn and girls by providing refuge, education, and resources"* [El Centro Afiya @TheAfiyaCenter "Transforman la vida, la salud y el bienestar general de las mujeres y niñas negras brindándoles refugio, educación y recursos"] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 33.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *The Midwest Access Coalition @MidwestAccess helps people traveling to, from, and within the Midwest access a safe, legal abortion with support in travel coordination and costs, lodging, food, medicine, and emotional support.* [La Coalición de Acceso del Medio Oeste @MidwestAccess ayuda a las personas que viajan hacia, desde y dentro del Medio Oeste a acceder a un aborto legal y seguro con apoyo en la coordinación y los costes del viaje, alojamiento, comida, medicamentos y apoyo emocional.] [Tuit]. Recuperado de:
<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

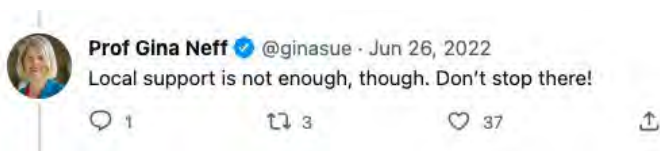


Figura 34.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Local support is not enough, though. Don't stop there!* [Sin embargo, el apoyo local no es suficiente. ¡No te quedes ahí!] [Tuit]. Recuperado de:
<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 35.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *4) Let's get our bodies back. There's work to be done and many more fights to fight for social and reproductive justice.* [4) Recuperemos nuestros cuerpos. Hay trabajo por hacer y muchas más luchas por librar por la justicia social y reproductiva.] [Tuit]. Recuperado de:
<https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 36.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Reproaction @reproaction leads bold action to increase access to abortion and advance reproductive justice.* [Reproaction @reproaction lidera acciones audaces para aumentar el acceso al aborto y promover la justicia reproductiva.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 76.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *Finally, this is not an abstract problem. Or even a technology problem (even though that's my lane, and what led to this tweet blowing up)...* [Por último, no se trata de un problema abstracto, ni siquiera de un problema tecnológico (aunque ese es mi tema y lo que provocó que este tuit se hiciera viral)...] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>



Figura 38.: Neff, Gina. [@ginasue]. (2022, 26 de junio). *5) Take care of each other. That is one of the most feminist and radical things that we can do. There's no app for that.* [5) Cuidarnos entre nosotras. Esa es una de las cosas más feministas y radicales que podemos hacer. No existe ninguna aplicación para eso.] [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

¿Cómo es posible que aplicaciones inicialmente consideradas inocuas y alejadas de la vigilancia digital en redes sociales debido a su orientación puramente personal, de pronto se conviertan en herramientas tan peligrosas que una experta del Oxford Internet Institute nos ruega que las eliminemos de nuestros dispositivos tan solos minutos después de conocerse el dictamen de «Dobbs contra Jackson»?

Lo cierto es, como apunta Newman (2022), que las aplicaciones de seguimiento del ciclo menstrual recopilan datos que pueden parecer benignos, pero que son claramente sensibles en el contexto de una posible penalización del aborto. De hecho, ya en 2021 la Comisión Federal de Comercio estadounidense sancionó a una empresa del sector, Flo Health, por compartir información sanitaria de sus usuarias con empresas de *marketing* y análisis, incluidas Facebook y Google (Federal Trade Comision, 2021).

Al hilo del esquema de cuatro reguladores —ley, norma social, mercado y arquitectura— (Lessig, 2006/2009, p. 207) que presenté en el apartado 1.1.4, subrayo que esta tensión entre la implantación de aplicaciones que registran, procesan y explotan nuestros datos corporales y sus riesgos para la privacidad se encuentra íntimamente relacionada con la legislación que cada país aprueba para proteger o atacar los derechos sexuales y reproductivos de su ciudadanía. Así, mientras que Francia blindo el derecho al aborto en su Constitución (Bassets, 2024), vemos cómo la sentencia del Supremo estadounidense amenazaba con retrotraer al Estado de Arizona a una ley de 1864 que castigaba severamente el aborto casi sin excepción (Beauregard, 2024). En definitiva, es a partir de esta intersección entre acecho legal y tecnológico a los cuerpos gestantes desde donde podemos abordar el conflicto al que nos enfrentamos día a día en relación a la salvaguarda de nuestros datos personales y de nuestras interacciones.

Ello me lleva a partir de la constatación del desarrollo de un significativo mercado de aplicaciones de control de ciclo, en gran medida justificado por un contexto de demanda de métodos anticonceptivos no médicos, especialmente entre jóvenes que ven estas alternativas como algo fiable, accesible y de coste mínimo (Ford *et al.*, 2021, p. 49). Dicha demanda contrasta con los estudios que alertan de su escasa fiabilidad médica (Eschler *et al.*, 2019), manifestada en problemas de precisión y eficacia, o directamente de sus malas prácticas en cuanto a la recopilación de datos personales, hasta el punto de que en algunos casos el seguimiento menstrual «provoca angustia y problemas de privacidad» (Levy y Romo, 2019, p. 7). En esta misma dirección apunta el hallazgo de que el 79% de las aplicaciones de salud disponibles a través de Google Play Store regularmente comparten los datos de las personas usuarias y están lejos de ser transparentes (Grundy *et al.*, 2019, p. 4).

Sin duda, a diferencia de los datos de localización, de rastreo del movimiento o de los marcapasos a los que aludía Raunig (2015/2023, p. 135), los ligados al ciclo menstrual todavía no pueden ser captados a través de dispositivos electrónicos de manera automática: No cabe hablar aquí de «servidumbre maquina». Somos nosotras quienes otorgamos esta información que, en última instancia, no podemos controlar, como tampoco podemos evitar sangrar de manera más o menos cíclica, al menos no sin recurrir a otras tecnologías o evidenciar que nuestro cuerpo está en otro estado, por ejemplo gestando o entrando en el climaterio. Y al exponer de este modo nuestros flujos orgánicos, quedamos transfiguradas en ese cuerpo descorporeizado, el ya nombrado “doble de datos” de pura virtualidad (Haggerty y Ericson, 2000, p. 611), a su vez sometido a normas cambiantes en función de la jurisdicción que habite.

Si a todo lo anterior agregamos que, en el caso que nos ocupa, actualmente no existe ni sanidad pública universal ni una ley federal de protección de datos en EEUU, la decisión del Supremo de sacar el aborto del amparo constitucional revela en toda su crudeza la actual intersección entre la falta de regulación de privacidad y el retroceso en derechos de salud sexual y reproductiva en algunos Estados.

Pero con lo que sí cuenta EEUU es con la *CLOUD Act (Clarifying Lawful Overseas Use of Data Act)*, una ley federal promulgada en 2018 que da carta blanca a sus autoridades para acceder indiscriminadamente a los datos almacenados en servidores de empresas de dicho país (correos electrónicos, mensajes de texto, *chats*, etc.) con independencia de su ubicación (Cordero, 2019). Para Peirano (2022) esta ley conlleva notables riesgos, dado que «aunque las comunicaciones están cifradas, la gestión incluye la clase de metadatos que genera cada transacción como, por ejemplo, la geolocalización de los miembros de un gobierno cada vez que se conectan» (p. 15).

Además, según un informe de 2021 del Consejo Internacional de Responsabilidad Digital (citado en Cadenas, 2022, párr. 9), en EEUU las *apps* de salud no tienen que cumplir las regulaciones estatales de la privacidad de los pacientes a las que sí están sujetos personal sanitario, hospitales, laboratorios y aseguradoras médicas. Para más *inri*, no hay ninguna normativa que defina qué se considera información sanitaria confidencial. En estas condiciones, Jimena Valdez (citada en Cadenas, 2022, párr. 8) asevera que, en caso de que se avance en la criminalización del aborto y las autoridades estatales comiencen a requerir datos incriminatorios a las plataformas digitales, sin duda éstas se los entregarán.

Cabe matizar, sin embargo, que este no es el caso de todo el territorio de EEUU, puesto que el Estado de California sí cuenta con una norma reguladora de los datos personales, la Ley de Derechos de Privacidad de California (CCPRA), en vigor desde enero de 2023. Esta normativa modifica la

precedente Ley de Privacidad de los Consumidores de California (CCPA) de 2018 en dos sentidos: de un lado, amplía los derechos de acceso y eliminación que ésta ya reconocía a la ciudadanía; de otro, añade nuevas categorías de información personal confidencial, como los datos sanitarios y las coordenadas de geolocalización, así como el derecho a corregir inexactitudes y a limitar el uso y la divulgación de información personal confidencial.

Con base en esta contextualización legal, para nuestro estudio comparativo sobre políticas de privacidad (PP) de las aplicaciones de control de ciclo (Solera y Gómez Alcalde, 2025) partimos de la selección que Gómez Alcalde (2023) había realizado sobre las seis aplicaciones más descargadas y mejor puntuadas en Google Play Store y App Store, tanto en la UE como en EEUU, y actualizamos el análisis de sus PP a fecha 27 de abril de 2024:

Aplicación	Desarrollador	País	PP actualizada	Enlace
 Mi Calendario Menstrual	Simple Design Ltd.	Reino Unido	30/08/23	https://web.archive.org/web/20240427092808/https://simpledesign.ltd/privacy/my_calendar.html
 Flo	Flo Health Inc.	Reino Unido	31/10/23	https://web.archive.org/web/20240427093241/https://flo.health/privacy-policy
 Clue	BioWink	Alemania	15/04/24	https://web.archive.org/web/20240427093249/https://hellocue.com/es/privacidad
 Meet You	Meet you Period tracker	Singapur	12/01/24	https://web.archive.org/web/20240427093315/https://www.meetyouintl.com/home/privacy.html
 Calendario Menstrual	Simpleinnnovation	EEUU	31/08/23	https://web.archive.org/web/20240427093336/https://simpleinnovation.us/my-calendar/privacy-policy
 Alerta de Período	GP Internacional LLC.	EEUU	s.f.	https://web.archive.org/web/20240427093558/https://gpapps.com/support/privacy-policy/

Tabla 1. Tabla descriptiva de las 6 *apps* de control de ciclo menstrual estudiadas. Fuente: Solera y Gómez Alcalde (2025)

Y para comprobar si dichas políticas variaban si residías en una u otra región simulamos nuestra ubicación en territorio estadounidense mediante Redes Privadas Virtuales (VPN, por sus siglas en inglés) y sistemas de ofuscación de IP como *Tor* (Solera, 2023, p. 129).

Tras ello, identificamos y sintetizamos en una tabla aquellas categorías de información potencialmente incriminatorias para las residentes de una jurisdicción donde el aborto está legalmente restringido o prohibido. En este sentido, decidimos obviar por redundantes aquellos datos que son consustanciales al empleo de estas aplicaciones, como las fechas de inicio y fin de periodo y la predicción de futuras fechas de ciclo.



Categorías	Mi calendario menstrual	Flo	Clue	Meet You	Calendario Menstrual	Alerta de Período
Rastreo de dirección IP (por la <i>app</i> o algún tercero)	V	V	V	V	X*	V
Rastreo de ubicación	X	V	X	X	X	X
Rastreo de historial de navegación	X	X	X	X	X	X
Comparte tus datos con terceros	X	V	V	V	V	V
Quedas sometida a las PP de terceros	X	V	V	V	V	V
Vende tus datos	X	X	X	X	X	?
Entrega tus datos ante requerimiento legal	V	V	V	V	V	V
Anonimiza tus datos	V	V	V	X	V	X
Puedes solicitar la eliminación de tus datos	V	V	V	V	V	V
Hay excepciones para eliminarlos	X	V	X	V	V	V
Puede mantener tus datos en sus servidores	X	V	X	V	?	?
Puede mantenerlos en servidores de terceros	X	?	?	V	?	?
Elimina por completo tus datos de sus servidores	V	X	V	X	?	?
Menciona dónde se encuentran sus servidores	X	V	V	V	X	X
Los datos se cifran en tránsito	V	V	V	X	V	V
Aplica cambios si la utilizas desde California	V	V	X	V	V	X
Aplica cambios si la utilizas desde la UE	V	V	V	V	V	X
Notifica cambios en su política de privacidad	V	V	V	V	X	X
Declara implementar SDKs y cuáles son	V	V	V	V	V	?
Permite conectar tus datos con otras personas	X	X	X	X	X	X

* Aunque no recoge la IP, sí la ID de publicidad del teléfono. Se trata de un identificador único y general para todas las aplicaciones del mismo dispositivo, por lo que este dato puede agregarse a otros para una posterior identificación.

Tabla 2. Tabla analítica de información recopilada por las 6 *apps* de control de ciclo menstrual estudiadas.

Fuente: Solera y Gómez Alcalde (2025)

Lo primero que llama la atención es que casi dos años después de la derogación de «Roe contra Wade» Flo continúe rastreando la ubicación de sus usuarias, por más que en paralelo haga disponible (no por defecto) un modo de uso anónimo y declare regirse por el RGPD, independientemente del país desde donde se acceda. Más llamativo aún resulta la constatación de que Flo se ha quedado sola en su geolocalización, toda vez que Clue, que compartía esta práctica al menos hasta julio de 2023 (Gómez Alcalde, 2023, p. 72), ya la ha desterrado de su PP. ¿Por qué motivo una *app* de ciclo menstrual recaba estos datos de ubicación? ¿Qué “valor añadido” le reporta ello a su clientela? A raíz del desamparo

constitucional del aborto que supone «Dobbs contra Jackson», lo cierto es que en EEUU (pero no solo allí) estas preguntas resultan cualquier cosa menos inocentes (hasta que se demuestre lo contrario).

Como puede adivinarse, la clave aquí reside en cómo semejante “geolocalización maquínica” puede poner en bandeja las (antaño onerosas) pruebas del “aborto interestatal”, esto es, de la posibilidad de que las gestantes de Estados que limitan el aborto viajen a otros que sí lo permitan para beneficiarse de sus derechos sin temor a ser procesadas por ello. Si bien en rigor no se trata de una cuestión nueva (pues ya se venía discutiendo al respecto, especialmente en los casos de menores de edad), la caída de la protección federal de «Roe contra Wade» ha animado a los Estados más represores a promover leyes (o interpretaciones de las mismas) que les permitan perseguir a quienes faciliten o reciban atención para abortar fuera de sus fronteras.

Según el seguimiento de la organización KFF (2025), a 22 de enero de este año existen cinco litigios contra tales regulaciones en tres Estados cuya conflictiva ubicación ilustro con la Figura 39: en Alabama, cuyas gestantes contaban con la opción (algo menos restrictiva) de la vecina Florida (Forouzan *et al.*, 2023, párr. 20), que hasta mayo de 2024 (cuando lo redujo a seis) concedía un plazo para abortar de 15 semanas; en Idaho, que ya antes de «Dobbs contra Jackson» estaba casi por entero rodeado de jurisdicciones más permisivas (véase Figura 12) y que ahora se enfrenta al reforzamiento generalizado de dichas protecciones; y en Tennessee, cuya prohibición total del aborto (sin siquiera excepción por riesgo vital de la madre, lo cual es actualmente objeto de otro litigio) se enfrenta al norte con su cercanía a la garantista Illinois y al este con su vecindad con Carolina del Norte y Virginia, cuyas restricciones al aborto no les impiden protegerlo dentro del primer mes y trimestre, respectivamente.

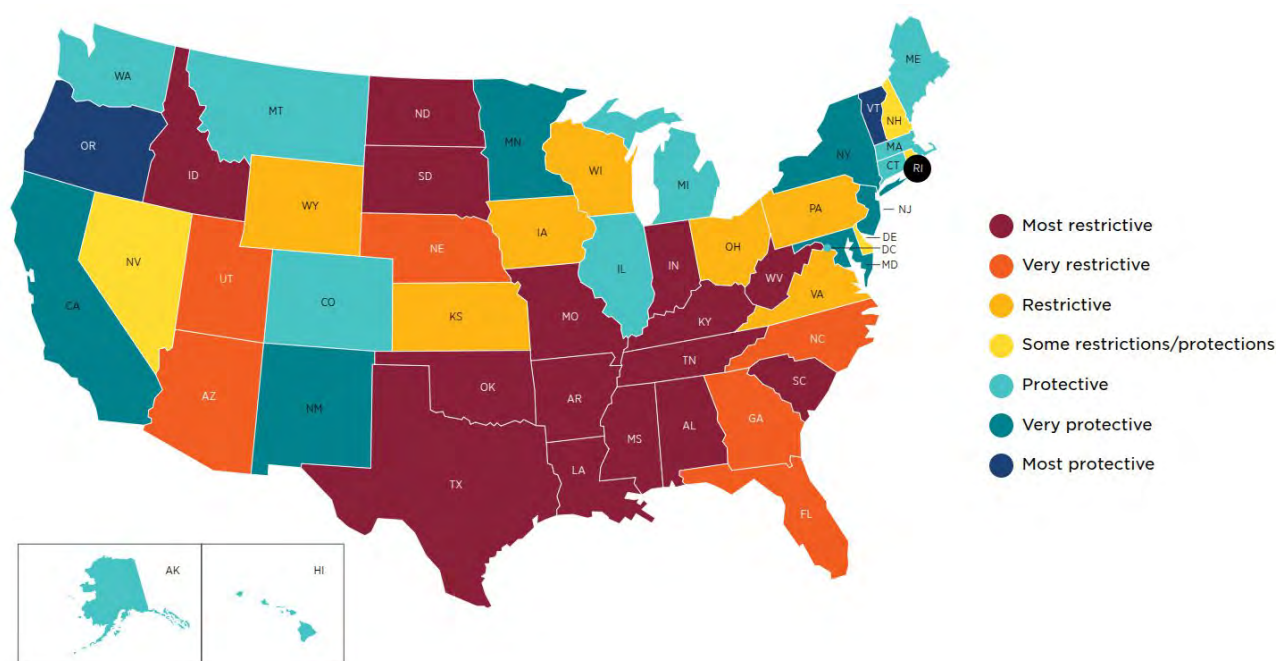


Figura 39. Mapa de las políticas sobre el aborto en EEUU *post* «Roe vs. Wade» a 25 de abril de 2024. Instituto Guttmacher²⁰.

Si a lo anterior sumamos la constatación de KFF (2025, párr. 1) de que entre 2020 y 2023 los abortos interestatales registrados en EEUU pasaron de suponer el 10% del total a casi el 20% resulta insoslayable el papel de “testigo de cargo” que podrían llegar a adquirir aquellas *apps* de ciclo menstrual que, como Flo, se prestan a recopilar unos datos tan codiciables por las acusaciones públicas, populares y particulares de aquellos Estados que logren imponer sus expansivas regulaciones antiabortistas.

Un segundo aspecto reseñable es la relevancia que para estas aplicaciones tienen los Equipos de Desarrollo de *Software* (SDK, por sus siglas en inglés), que permiten a empresas externas desarrollar servicios de ubicación, de traducción automática y similares que de otro modo deberían crearse desde cero por la compañía matriz. Ya desde su primer estudio al respecto, Gómez Alcalde (2023) detectó la necesidad de especificar en la tabla si las aplicaciones declaraban implementarlos, pues la facilidad que ofrecen para desarrollar de forma rápida y barata funcionalidades extra tiene como contrapartida su acceso amplio a los datos que recopilen las herramientas a las que complementan.

La gran amenaza radica en que, una vez que el desarrollador de SDK ha accedido a los datos, suele utilizarlos para fines ajenos al propósito original y venderlos a empresas de publicidad, *data brokers* e incluso agencias de espionaje (Ullah, 2020), en un proceso que «a menudo es tan complejo que es imposible saber, cómo y a quién se envían los datos recopilados por una sola aplicación» (Bax *et al.*, 2021, p.13). Este modelo de negocio infringe la privacidad de las *apps* donde se implementan, volviendo

²⁰ Véase: <https://web.archive.org/web/20240425064903/https://states.guttmacher.org/policies/> Para una información actualizada, véase: <https://states.guttmacher.org/policies/abortion-policies> Recuperado el: 17 de febrero de 2025.

inseguro su empleo incluso si la aplicación en cuestión cumpliera la normativa vigente. Un buen ejemplo lo encontramos en Clue, que pese a declarar su adhesión a «los más altos estándares de privacidad y seguridad» y ser la única *app* que afirma desvincular el perfil personal de los datos sanitarios y proteger sus contraseñas mediante funciones resumen (*hashing*, en inglés), admite un SDK que transfiere datos personales a EEUU.

El tercer aspecto que destaco es que tanto Alerta de Período como Meet You ofrecen entre sus servicios una «sección social» y una «comunidad abierta», respectivamente. En Meet You, para más “inri”, se arrojan los permisos de acceso a cámara, álbum de fotos o carpetas de almacenamiento sin que podamos siquiera garantizar que cumplen el compromiso de su PP de cifrar los datos antes de transmitirlos, al indicarse lo contrario en Google Play Store²¹

Por último, en el caso de Calendario Menstrual resulta preocupante que, si bien los datos se almacenan de modo predeterminado en el dispositivo de quien la usa, le da la opción de guardar una copia en los servidores de Google Cloud, quedando entonces sujetos a la PP de Google.

Llegados a este punto, puede ser tentador contemplar nuestro estudio como una suerte de relato de anticipación del «futuro terror» *made in USA* (Redondo, 2024) que cuando escribo estas líneas parecen empeñados en encarnar Donald Trump y Elon Musk. Algo de eso hay, sin duda, pero la investigación en la que embarqué a mi compañera Marina Gómez Alcalde desde las primeras filtraciones de la sentencia de «Dobbs contra Jackson» nunca ha desatendido las respuestas eminentemente políticas que el movimiento feminista de EEUU ha articulado para defender la salud sexual y reproductiva de las gestantes. En consecuencia, las últimas líneas de este apartado las consagraré a una valoración provisional del alcance de dichas resistencias, articulado en torno al citado esquema de cuatro reguladores de Lessig.

Antes de nada, conviene exponer algunos de los prejuicios que esta investigación nos ha permitido reconocer en nosotras mismas como habitantes en una España marcada desde hace más de una década por potentes movilizaciones feministas. Podría resumirlos en dos: por un lado, el prejuicio de que la ley de plazos que regula el aborto en España desde la Ley Orgánica 2/2010 es más amplia y garantista que la de EEUU (incluso antes de «Dobbs contra Jackson»); por otro, el prejuicio de que la ausencia de un sistema sanitario público y universal en EEUU supone un gravamen extralegal (de carácter eminentemente mercantil pero también arquitectónico por la distancia geográfica para acceder a cuidados asequibles) que coarta en buena medida el ejercicio efectivo de dicho derecho incluso en las

²¹ Véase: https://web.archive.org/web/20240425170818/https://play.google.com/store/apps/datasafety?id=com.meetyou.intl&hl=es_419&gl=US Consultado el 23 de abril de 2024

jurisdicciones más garantistas.

Respecto al primero, los datos de los mapas citados arriba evidencian lo restringido de las 14 semanas para el aborto libre (ampliable a 22 con permiso médico) que la legislación española ha mantenido desde 2010 hasta la reciente Ley 1/2023. Tal restricción contrasta con permisividad hasta la “viabilidad fetal” (entre 20 y 26 semanas) emanada de «Planned Parenthood contra Casey» y aún imperante en 23 de 50 Estados, a los que hay que añadir nueve (más Washington D.C.) que no aplican ninguna restricción por edad gestacional. Con todo, la ilustración más llamativa la proporciona la citada Florida, cuyas múltiples restricciones la situaban en los mapas como “*Very restrictive*” pero cuya protección del aborto de 1 semana más que España (15) hasta mayo de 2024 la convertían en destino privilegiado para miles de mujeres de los vecinos Estados de Alabama, Mississippi, Louisiana y Arkansas y aún seguía atrayendo a ella a miles de mujeres recibiendo a muchas mujeres los Estados vecinos de Alabama (Forouzan *et al.*, 2023, párr. 20-23).

Respecto al segundo prejuicio, los datos del Ministerio de Sanidad muestran que el 81,4% de las interrupciones voluntarias del embarazo realizadas en España en 2023 se derivaron a centros privados (Toro, 2024) pese a figurar legalmente como una prestación garantizada por el Sistema Nacional de Salud. Más inquietante aún resulta el dato de que varias comunidades autónomas nunca hayan informado de abortos en sus territorios (Toro, 2024, párr. 4, 6-7), lo cual ha dado pie a que el Tribunal Constitucional sentencie como vulneración de derechos fundamentales lo que podríamos denominar como “aborto interautonómico forzoso”, a raíz del caso de una mujer que tuvo que ir a abortar a Madrid después de que el Servicio Murciano de Salud se negara a practicárselo en esta comunidad autónoma (López Trujillo, 2023). Si a todo ello añadimos que los datos comparativos del Guttmacher Institute muestran que desde «Dobbs contra Jackson» cada vez son más los Estados (19) que sufragan con fondos públicos los abortos de familias vulnerables (a través del programa *Medicaid*) y/o que obligan a las aseguradoras a incluir este servicio en sus pólizas privadas de salud (13), el carácter diferencial de la existencia de sanidad pública universal en España para garantizar el ejercicio efectivo de este derecho respecto a EEUU no queda tanto reducido sino necesariamente matizado.

Para enmarcar estos primeros apuntes legales en una conclusión global sobre la actual situación de la interrupción voluntaria del embarazo en EEUU retomaré ahora con la Figura 39 el mapa más reciente que he recopilado del Guttmacher Institute:



Empezando por esta última situación, es evidente que si comparamos este último mapa con el de la Figura 12 encontramos el doble de Estados (12) que hoy sufren una prohibición prácticamente total del aborto, más otros cuatro que han reducido el plazo a seis semanas. Con todo, en casi un tercio de ellos (5) hay litigios pendientes de resolver (aunque sin medidas cautelares) que reclaman la inconstitucionalidad de tales regímenes. Y conviene recordar que muchos de los Estados más intransigentes son limítrofes con otros susceptibles de ofrecer la opción del “aborto interestatal”.

22 Véase: <https://web.archive.org/web/20250212064903/https://states.guttmacher.org/policies/> Para una información actualizada, véase: <https://states.guttmacher.org/policies/abortion-policies> Recuperado el: 18 de febrero de 2025.

investigaciones de autoridades de Estados restrictivos que afecten no solo a pacientes y profesionales clínicos, sino también a organizaciones activistas y proveedoras de tratamientos por telemedicina.

Retomando los cuatro reguladores citados, estos “avances legales” promovidos por la movilización en el terreno de las “normas sociales” pueden verse respaldados por unas “normas corporativas” vinculadas al “mercado” (una política de relaciones públicas) que incentiven la eliminación de las “políticas de privacidad” y, en última instancia, de la propia “arquitectura” de las *apps* de cualquier rastreo de ubicación. He aquí la tendencia que vimos que ha seguido Clue, pero a la que Flo sigue oponiéndose, con el consiguiente riesgo legal para sus usuarias. Más allá de la geolocalización, sin embargo, he podido constatar cómo, respecto a investigaciones anteriores (Gómez Alcalde, 2023 y Eticas Foundation, 2022), se han producido algunos cambios en las PP que apuntan al refuerzo de la privacidad de las personas usuarias. En ausencia de una nueva normativa que lo ordene (en el caso estadounidense, no así en la UE), no resulta aventurado plantear que las críticas de las feministas *post* «Roe contra Wade» han tenido un impacto en la toma de decisiones de estas empresas.

Sin embargo, sigue siendo alarmante el número de empresas ajenas, como las aludidas desarrolladoras de SDK, que se involucran en el funcionamiento de estas aplicaciones. Dicha alarma es aún mayor teniendo en cuenta la habitual remisión a las PP de dichas empresas por parte de las *apps* primarias, lo cual nos aboca a un bucle infinito por donde perdemos cualquier perspectiva de control sobre nuestra información. Esto nos lleva a preguntarnos si no existen demasiados participantes que puedan exponer los flujos de datos potencialmente incriminatorios que circulan por estas aplicaciones.

También subrayo la predisposición de estas *apps* a la violación del deber de custodia de nuestra información confidencial, sobre todo cuando hablamos de requerimientos no respaldados por procedimientos garantistas de la tutela judicial efectiva. Y es que a este respecto sí que hallamos unanimidad en estas empresas: si las autoridades estatales lo requieren, todas ellas faltarán a nuestra confianza y les entregarán información íntimamente vinculada con nuestros cuerpos. Ello nos recuerda la relevancia de las alternativas de seguridad en el plano tecnológico, que incluyen, cuando el borrado de las *apps* no sea asumible, las tácticas de ofuscación a las que dedico el *Capítulo 4*, las cuales generan ruido de fondo sobre nuestra actividad para distorsionarla y lograr así confundir a los traficantes de datos y devaluar su confianza.

Igualmente, podemos llegar a conclusiones similares si retomamos los consejos a los que apuntaba Gina Neff (2022) en sus tuits: en primer lugar prestar atención a las aplicaciones que utilizamos y a sus políticas de privacidad y exigir tanto a sus desarrolladores como a los legisladores una mayor protección

de nuestros datos personales, ello también implica tener una mejor percepción de cómo nuestra privacidad está relacionada con la de otras personas con las que estamos conectadas; en segundo lugar, dado que este no es un problema meramente abstracto o tecnológico el cual el borrado de una *app* concreta no va a solucionar, resulta importante ser consciente de que estas violaciones sistemáticas interseccionan también con aspectos como la raza, el origen, la edad o el nivel de ingresos económicos; por lo que, en última instancia, se torna fundamental dar soporte a organizaciones y grupos que brindan apoyo a personas que se encuentran en estas situaciones.

La diferencia apreciable entre unos Estado y otros, así como la evolución positiva de algunos de ellos hacia normas más proteccionistas sobre este derecho reflejan las resistencias que han generado el movimiento feminista también a escala legal con los distintos referéndums y normas impulsadas contra las consecuencias estatales de la sentencia de 2022. Lo que nos permite evocar la tremenda complejidad del panorama de los derechos reproductivos en el EEUU actualmente, gracias a un virtuoso vuelco a la situación desde una escala hasta ahora temida (la estatal), al estilo de cuando Deleuze (1990/1995, p. 278) en el comienzo del *Post-scriptum sobre la sociedad de control* indica que «No hay lugar para el temor, ni para la esperanza. Sólo Cabe buscar nuevas armas».

Llegados a este punto, conviene enfatizar que, aunque en este estudio nos centramos en la intersección entre el acecho legal y tecnológico a los cuerpos gestantes en EEUU, el hecho es que, sin un marco legislativo garantista, nada impide que este riesgo se extrapole a otros datos confidenciales y territorios. En este sentido, resulta esperanzador que hoy sean 24 los Estados donde el derecho al aborto está plenamente establecido. De ellos, nueve han suplido la súbita desprotección a escala federal incluyendo o reforzando la codificación de este derecho en sus respectivas Constituciones estatales (aunque Nevada está pendiente de ratificarla en 2026). Y no menos importante es el hecho de que cuatro Estados que venían de amplias prohibiciones (Utah, Wyoming, Wisconsin y Dakota del Norte) las tengan hoy suspendidas a la espera de la resolución de sendos litigios.

Con todo, el caso de Dakota del Norte nos brinda un inmejorable recordatorio (similar al del “aborto interautonómico forzoso” que se denunciaba en España) de que, para ser efectivos, los avances legales han de ir de la mano de los otros tres reguladores, muy especialmente de las “normas sociales”. Y es que se da la circunstancia de que el litigio que en septiembre de 2024 logró suspender cautelarmente la prohibición total promovida al poco de caer «Roe contra Wade» fue presentado por la única clínica abortiva que quedaba en el Estado y que en agosto de 2022 se había mudado a la vecina Minnesota. Así pues, por más que aquí el “aborto interestatal” sea plenamente factible, nos hallamos ante la recuperación formal de un derecho que sin embargo carece del fundamento material y, por extensión,

social para poder efectuarse.

Esta chocante situación me permite concluir enfatizando algo que hasta ahora apenas he explicitado: la singular trascendencia de las organizaciones en pro de los derechos sexuales y reproductivos para resistir los embates posteriores a «Dobbs contra Jackson» y, más allá, (re)conquistar viejos y nuevos derechos (cobertura financiera, aborto interestatal, reducción de plazos, eliminación del consentimiento paternal en caso de menores...). No en vano, en todos los Estados donde se ha logrado incluir o reforzar el derecho constitucional a la interrupción voluntaria del embarazo la iniciativa ha surgido de defensores de derechos civiles y reproductivos, los cuales han movilizado a centenares de miles de personas para, primero, reunir las firmas necesarias para convocar los referéndums preceptivos y, más tarde, captar los apoyos que permitieron ganar muchos de ellos (7 de ellos el mismo 5 de noviembre de 2024 en que Trump fue reelegido Presidente). Y otro tanto cabe decir de los Estados donde se está defendiendo el aborto interestatal o se han paralizado las prohibiciones totales (KFF, 2025).

Una inmejorable ilustración final de esta virtuosa combinación de las vías normativa y legal la representa Arizona, donde a raíz de la anulación de «Roe contra Wade» se intentó volver a una «ley draconiana» de 1864 (citado en Beauregard, 2024, párr. 7) que prohibía el aborto incluso en casos de violación e incesto. La intensa movilización social que denunció estos intentos, espoleada aún más si cabe por el respaldo del Supremo estatal a dicha norma decimonónica en abril de 2024, forzó primero a la Fiscalía General del Estado a prometer que no acataría la citada ley, y luego al Congreso estatal a promover su derogación para restituir otra de 2022 que limitaba el plazo para abortar a 15 semanas. Sin embargo, la culminación de esta transformación de la norma social en favor del derecho al aborto llegó el 5 de noviembre de 2024, cuando la coalición Arizona for Abortion Access logró un respaldo del 61,61% a una enmienda constitucional que devolvía el plazo legal a las 24-26 semanas de viabilidad fetal, plazo que quedaba a su vez amparado por la aprobación el año anterior de uno de los citados escudos legales para proteger a quienes acudieran a abortar desde otros Estados²³. Una vez superado de forma garantista este vaivén legal a lo largo de décadas e incluso siglos, queda pendiente para futuras investigaciones la incógnita de cómo casa el citado porcentaje de apoyo al derecho al aborto con la victoria el mismo día de Donald Trump con un 52,2% de los votos, 5,5 puntos más que Kamala Harris.

23 Véase: <https://web.archive.org/web/20250207060504/https://www.arizonaforabortionaccess.org/>

2.5. ¿Cómo respondemos al extractivismo de datos personales?

Al plantear la pregunta que da título a este epígrafe estoy adelantando que, efectivamente, hay formas de responder a este sistema y que las cuestiones que subyacen deben focalizarse en el cómo más que en su mera posibilidad, ya que, tal y como afirma Foucault (1978/1998, pp. 116-117):

donde hay poder hay resistencia, y no obstante (o mejor: por lo mismo), ésta nunca está en posición de exterioridad respecto del poder [...] más frecuentemente nos enfrentamos a puntos de resistencia móviles y transitorios, que introducen en una sociedad líneas divisorias que se desplazan rompiendo unidades y suscitando reagrupamientos, abriendo surcos en el interior de los propios individuos, cortándolos en trozos y remodelándolos, trazando en ellos, en su cuerpo y su alma, regiones irreducibles. Así como la red de las relaciones de poder concluye por construir un espeso tejido que atraviesa los aparatos y las instituciones sin localizarse exactamente en ellos, así también la formación del enjambre de los puntos de resistencia surca las estratificaciones sociales y las unidades individuales.

De hecho, asumir que la resignación es el estado de ánimo dominante o la única opción disponible es aceptar una visión sesgada de los sujetos, del poder y de cómo se relacionan. Para autores como Lyon (2018, p. 185), las visiones negativas y derrotistas, fruto de aceptar las representaciones del Gran Hermano, se alimentan de la percepción de los usuarios de Internet como meros “sujetos del poder”, lo cual resulta sencillo de aceptar si percibimos los imaginarios de vigilancia como espacios dominados por organizaciones remotas y fuera de nuestro control.

Si bien es cierto que en multitud de ocasiones somos partícipes de nuestra propia sumisión, el autor señala que incluso en esas situaciones se abren ventanas de oportunidad para cuestionar, negociar e incluso subvertir estas prácticas. Buena prueba de ello lo hemos visto en los citados cambios en la políticas de privacidad de las aplicaciones de control de ciclo hacia modelos más proteccionistas sin que una norma les haya obligado a ello. Esto no implica que la resistencia de las personas a este poder se pueda llevar a cabo con facilidad, sino que este poder se aplica sobre cuerpos que no están pasivamente sometidos a él.

Estudios como los llevados a cabo por Tiziano Bonini y Emiliano Treré (2024) muestran cómo en el día a día, las personas se cuestionan su relaciones laborales, políticas o de consumo mediadas a través de Internet, y cómo en ciertas situaciones se niegan a cooperar, limitan su exposición o modifican su manera de interaccionar con la plataforma o aplicación como forma de desafiar el extractivismo de

datos. Estas resistencias responden en muchas ocasiones, como también afirma Lyon (2007, p. 67), a su relación con otros movimientos como los de las libertades civiles, el feminismo, el antirracismo, etc.

Otros actos cotidianos de auto-protección —que también son señales de que somos conscientes de la vigilancia—, como poner la configuración de privacidad de nuestras redes sociales en los estándares más restrictivos, tapar la cámara del portátil con cinta adhesiva o rechazar sistemáticamente las *cookies* de los diferentes portales *web* que visitamos (al menos en regiones como la UE donde esa opción es legalmente imperativa), sin dejar de reflejar un posicionamiento frente al extractivismo de datos, tienen pocas probabilidades de producir un gran efecto sin un apoyo institucional. Si bien muchos medios alientan a los ciudadanos a protegerse, la cuestión más amplia y verdaderamente política es si los ciudadanos comunes y corrientes podemos o no desafiar a estas organizaciones extractivistas para que se preocupen adecuadamente por los datos personales que manejan.

Dado que parte de lo que podría considerarse vigilancia digital enfatiza sus estrategias en la lógica a gran escala de la tecnología y la economía política, con demasiada facilidad esto ensombrece el papel de las tácticas a la escala de la vida cotidiana que relata el filósofo francés Michel de Certeau (1990). Por ejemplo, algunos debates académicos sobre los usuarios de Internet han estado marcados con una visión abstracta, centrada y racional del yo. De este modo, tal y como indica Julie Cohen (2012), han perdido de vista el yo encarnado, social y creativo que realmente encuentra, usa y experimenta la información. Esto significa que debemos prestar más atención a la acción humana, si bien ésta se encuentra ahora cada vez más mediada por tecnologías digitales.

En pocas palabras, hoy en día la privacidad no se trata tanto de aquella propuesta de 1890 de un «derecho a ser dejado en paz», repasada en la sección 2.2.2, del abogado Samuel D. Warren y el juez Louis Brandeis, como de tratar de controlar los flujos de información personal, una situación en la que el contexto es crucial. Esto resuena con la insistencia de Certeau (1990, p. 255), que indicaba en el punto 1.3. cuando indica que no hay que tomar a la gente por idiota.

En otras palabras, resulta un error suponer que los usuarios, consumidores, o como quieran denominarlos, son cuerpos pasivos y que se guían voluntariamente por reglas establecidas. Debemos explorar, por tanto, las prácticas cotidianas para descubrir cómo operan realmente las personas y cómo se comportan frente a las estrategias del poder.

2.5.1. Modos de hacer

Marcado ineludiblemente por las revueltas de Mayo del 68, el historiador francés Michel de Certeau centró desde entonces sus estudios en la vida cotidiana, donde identificó una variedad de indicadores que señalaban, en una dimensión micro y dispersa, la resistencia y la creatividad de individuos comunes que se esforzaban por mantener una libertad que siempre les resultaba temporal. En esta línea, en 1974 publicó *La Culture au pluriel*, donde argumenta que los mecanismos disciplinarios de aislamiento social son crecientemente cuestionados por acciones diarias que desmontan los cálculos de la planificación autoritaria, y esto ocurre en diferentes ámbitos como el urbano, en los medios, el educativo y el laboral entre otros.

De esta manera, frente a una «cultura en singular» que aspira a enterrar bajo un prisma unificador las continuas divergencias culturales que no se ajustan al signo del poder, la cultura “en plural” «apela incesante a un combate», (Certeau, 1974/1993, p. 213), ocupando en el día a día los espacios por los que pueden surgir voces y creaciones que subviertan la cultura hegemónica.

En 1980, Certeau replanteó estas problemáticas en el primer volumen de *L'invention du quotidien*, titulado *Arts de faire*. En este texto, el escritor condensa su investigación previamente aludida en el concepto de «antidisciplina» (Certeau, 1990, p. XL), que conlleva cambiar el enfoque del disciplinamiento (Foucault, 1975/2022) hacia unos usos cotidianos plenamente identificados como producción, como la *poïesis* (creación, invención) que busca subvertir el disciplinamiento.

El término *arts de faire* — traducido por Jordi Claramonte (Certeau, 2001) como “modos de hacer” — es propuesto por el historiador francés para englobar las prácticas de “consumo” que, pese a trabajar «con un vocabulario y una sintaxis recibidos» (Certeau, 1990, p. XXXVIII), revelan una «invención de lo cotidiano» cuya caracterización formal remite a dos ejes teóricos: de una parte, las combinaciones operativas que, en clave de “uso”, se ponen en marcha en estas prácticas; y de la otra, la perspectiva polemológica que da cuenta de «las operaciones casi microbianas que proliferan en el interior de las estructuras tecnocráticas, cuyo funcionamiento desvían mediante una multitud de “tácticas” articuladas sobre los “detalles” de lo cotidiano» (Certeau, 1990, p. XL).

Estrategias y tácticas

Para analizar el conflicto relacionado con el citado “consumo”, el escritor galo hace una distinción fundamental entre estrategia y táctica. La primera sería aquel «cálculo (o manipulación) de las relaciones de fuerzas» (Certeau, 1990, p. 59) que deriva de la posibilidad de aislar a una determinada instancia

dotada de voluntad y poder en un lugar propio, desde donde delimita e interactúa con una “exterioridad”. Tal instauración de un lugar propio supone «una victoria del lugar sobre el tiempo» que permite desplegar una práctica panóptica, un intento de controlar el tiempo mediante la pre-visión del espacio que, a su vez, da lugar a un tipo de saber definido como la «capacidad de transformar las incertidumbres históricas en espacios legibles» (Certeau, 1990, p. 60). Para este autor, el escenario de la estrategia es por tanto el ámbito del poder.

En contraste con ésta, la táctica sería ese otro cálculo de fuerzas que, no teniendo más lugar que aquel ocupado por el primero, no puede permitirse situarlo “en su punto de mira” ni retirarse de su vigilancia. Ante ello, «ciega y perspicaz como se está en un cuerpo a cuerpo sin distancia» (Certeau, 1990, p. 62), la táctica privilegia el tiempo, pertrechándose para aprovechar las ocasiones mediante golpes furtivos asestados en un lugar y/o tiempo vedados y/o con instrumentos no reglamentarios. En este sentido, Certeau caracterizó las tácticas como el ámbito de los débiles, al entenderlas, no como un subconjunto de la estrategia, sino más bien como una adaptación a entornos que han sido creados por las estrategias de los poderosos. Al uso de la táctica se le atribuye una ausencia de poder, por lo que se acentúa la diseminación camuflada a través de los lugares de dominio y, sobre todo, la tenacidad. Con esto Michel de Certeau llega a una síntesis de los modos de hacer como:

Un estilo de intercambios sociales, un estilo de invenciones técnicas y un estilo de resistencia moral, es decir, una economía del ‘don’ (generosidades *à charge de revanche*), una estética de ‘golpes’ (operaciones de artistas) y una ética de la tenacidad (mil maneras de negarle al orden establecido el estatuto de ley, de sentido o de fatalidad) (Certeau, 1990, p. 46).

Para ilustrar esta diferencia, el autor alude a las estrategias de planificación urbana y las tácticas utilizadas por sus habitantes para eludirlas. El autor emplea el tránsito de los viandante en la ciudad como un modelo de táctica, ya que los arquitectos de los espacios urbanos no pueden predecir por completo todas las maneras en que las personas se desplazarán por sus calles. De hecho, si las vías se proyectan sin tener en cuenta las necesidades de los transeúntes, surgirán atajos y caminos alternativos a través de áreas que no se proyectaron para ser transitadas a pie. El peatón transita a través de un espacio concebido por arquitectos urbanos, en un terreno que sin serle propio debe habitar. Es en este territorio donde el peatón debe elaborar tácticas para ajustar o contrarrestar las trayectorias estratégicamente (pre)concebidas por el planificador urbano para cubrir sus necesidades.

Por tanto, actuar de manera estratégica implicaría disponer de una amplia disponibilidad de tiempo,

dinero y experiencia, y tener la capacidad de confiar en planes de largo alcance. En cambio, actuar tácticamente implicaría tener escasa disponibilidad dinero y experiencia. Sin embargo, en cuanto al concepto de tiempo, Certeau identifica aquí la importancia de la “memoria” en la táctica como elemento clave, la cual lejos de suponer un lugar propio, se trata de un recabado de saberes y conocimientos colectivos transmitidos a través de la experiencia, por lo que el tiempo de ejecución lo divide en el momento de la acción rápida nutrida por una memoria de largo recorrido:

Una duración se introduce así en la correlación de fuerzas y va a cambiarla. La *metis*, en efecto, apuesta por un tiempo acumulado, que le resulta favorable, contra una composición de lugar que le es desfavorable. Pero su memoria permanece escondida (carente de lugar identificable) hasta el instante en que se revela, en el “momento oportuno” [...]. El relámpago (*éclair*) de esta memoria brilla en la *ocasión*, [en la que] concentra el *máximo* de saber en el *mínimo* de tiempo (Certeau, 1990, pp. 125-126).

2.5.2. Formas de resistencia al extractivismo de datos

Si bien las interacciones sociales se han podido ver modificadas cuando son mediadas por máquinas, éstas últimas tampoco han resultado imperturbables a su aplicación cotidiana. Un claro ejemplo lo encontramos en el origen del *hashtag* de Twitter, surgido el 23 de agosto de 2007 de la propuesta de un usuario de esta plataforma, Chris Messina, cofundador de las “desconferencias” *BarCamp* sobre tecnologías y datos abiertos. Messina lanzó al final de su tercera edición de 2007 un tuit con la sugerencia original de agrupar temáticamente los hasta entonces dispersos mensajes de Twitter sirviéndose del símbolo del *hash* “#”. Al poco tiempo decidió ampliar la propuesta hacia la idea de mejorar la contextualización, el filtrado de contenido y la serendipia exploratoria en el seno de Twitter (Messina, 2007a).

Tras presentar su idea en las oficinas de la empresa sin éxito, Messina continuó fomentando el uso de los *hashtags* entre sus conocidos hasta que ese mismo año acabaron extendiéndose para agrupar publicaciones y coordinar esfuerzos en torno a desastres como los incendios de San Diego: *#sandiegofire* (Messina, 2007b). No fue hasta dos años después que Twitter finalmente implementó los hipervínculos a los *hashtags* para facilitar y extender su uso, para acabar en 2010 añadiendo el espacio de los *trending topics* en su página principal.

Esta anécdota nos ayuda a ejemplificar una forma en que la tecnología, en lugar de ser adoptada tal y como ha sido construida, se ve adaptada a los deseos y necesidades de las personas que se sirven de ella. Sin embargo, en otras ocasiones los usuarios de plataformas mediadas por algoritmos inalterables y

opacos buscan formas alternativas de paliar los efectos negativos que sufren por habitar un lugar que no les es propio. Se trata de pequeños actos de resistencia que, según Bonini y Treré (2024, p. 159):

En todas estas grandes narrativas sobre la condición actual de las democracias capitalistas cada vez más mediatizadas, hay algo aparentemente minúsculo y mundano que escapa a las amplias mallas de las teorías del capitalismo comunicativo o de plataforma. Lo que escapa a su mirada son los miles de actos microscópicos de resistencia a la fuerza narrativa del capitalismo de plataforma, que se materializan en la apropiación, por parte de la gente común, los trabajadores y los activistas, de las herramientas de la comunicación en red primero, y de los algoritmos después, para ponerlas al servicio no de un *ethos* neoliberal sino de una agenda cooperativa y solidaria.

Para estos autores (Bonini y Treré, 2024, p. 22), estas formas de resistencia son entendidas como un fenómeno dinámico que puede adoptar muchas formas y ocurrir en varios niveles. Podría, de esta manera, haber actos de resistencia que sean reconocidos como tales solo por quienes los realizan; exclusivamente por quienes los reciben; reconocidos solo por un observador externo o por las tres partes citadas.

Otro autor que ha estudiado formas de resistencia cotidiana es el antropólogo y politólogo James C. Scott quien intentó dar respuesta en su obra *Weapons of the Weak* (1985), a cuestiones sobre qué hacen los campesinos (en el caso de Scott, estudió a campesinos de Malasia) frente a acciones manifiestamente injustas, encontrando en su investigación una serie de formas cotidianas, ordinarias y eminentemente prácticas de actuar y responder, que el autor recogió bajo el concepto de “armas de los débiles”.

Esta idea es recuperada tanto por Bonini y Treré (2024, pp. 22, 25-27) como por Brunton y Nissenbaum (2015, pp. 55-58), para trasladarla a los entornos digitales altamente vigilados, salvando siempre las distancias, ya que, tal y como afirman particularmente Brunton y Nissenbaum (2015, p. 57) «la amplitud de los recursos disponibles para unos y otros —las estructuras e infraestructuras— y los mecanismos de coerción y control a los que se enfrentan no permiten comparaciones simples», pero que aún así ayudan a pensar en las formas de resistencia en lo digital, como el concepto de ofuscación de estos autores que expliqué en el punto 1.1.5, entendido como una serie de métodos expresivos y funcionales de protesta y evasión que son accesibles a una variedad de actores, pero que son particularmente importantes para aquellos que carecen de acceso a otros métodos o desean complementarlos, por lo que se torna muy viable para estos autores asumir el concepto de “arma de los débiles” de Scott para referirnos a ellos (Brunton y Nissenbaum, 2015, p. 58).

Por otro lado, Baaz *et al.* (2016, p. 142) definieron la resistencia de manera sintética como «(i) un acto, (ii) realizado por alguien que defiende una posición subalterna o alguien que actúa en nombre y/o en solidaridad con alguien en una posición subalterna, y (iii) (la mayoría de las veces) en respuesta al poder».

Considero importante afinar aquí que, tal y como señalan Bonini y Treré (2024, p. 176), entre aquellas personas sometidas a una continua datificación de su vida diaria, hay un tipo de “resistencia” que apenas puede considerarse como tal y que se ejerce para perseguir pequeñas ganancias marginales sin ningún propósito de trasgredir este ecosistema altamente vigilado y, por ello, apenas comienzan una resistencia orientada a engañar al sistema, aspirando al mayor beneficio posible sin ninguna intención de cambiarlo realmente. En contraste, existen otras personas, especialmente aquellas económicamente dependientes de las plataformas para ganarse la vida, que se dan cuenta de que este ecosistema vuelve sus vidas precarias e impredecibles y entonces comienzan a organizarse, protestar y finalmente imaginar soluciones alternativas, por lo que ante, la duda de a si las prácticas cotidianas son resistentes por sí mismas resulta esencial tener presente la perspectiva polemológica de Michel de Certeau.

A continuación presento breves ejemplos de estas dinámicas en áreas como el consumo, el trabajo mediado por plataformas digitales —como es el caso de los *riders*—, así como casos de resistencia y tácticas de apropiación algorítmica llevadas a cabo por personas unidas por su admiración por un género o artista concretos, como muestra de prácticas cotidianas, algunas con un sentido más político que otras, que generan cambios en el sistema extractivista de datos.

El intercambio de tarjetas de fidelidad de los supermercados

Previamente a la expansión de la llamada economía de plataforma (Joyce *et al.*, 2022), encontramos ejemplos de estas resistencias en la ofuscación de la identidad de los consumidores a través del intercambio de tarjetas de fidelización de los supermercados con el fin de interferir en el análisis de patrones de compra. A este respecto, Brunton y Nissenbaum (2015, pp. 28-29) enfatizan cómo las tiendas de alimentación llevan mucho tiempo a la vanguardia en lo que se refiere a la recopilación de datos a través de sus tarjetas de fidelización, mediante cuyo uso los consumidores obtienen ciertos descuentos o beneficios y los supermercados registran sus hábitos de compra, incluidos metadatos acerca de qué días, a qué horas y qué categoría de productos adquieren.

De esta manera, Brunton y Nissenbaum (2015, p. 28) señalan que los primeros programas de fidelización se utilizaban para atraer a clientes habituales, que se aprovechaban así de descuentos vedados a quienes no usaban las tarjetas al tiempo que se prestaban a una recopilación de datos

utilizada para el envío de *marketing directo* y publicidad postal más personalizada. A tal punto llegaría esta recopilación que en poco tiempo la gran mayoría de estos establecimientos externalizaba el negocio del análisis de datos a empresas como ACNielsen. Sea como fuere, aunque estas prácticas se percibían en sus inicios como aisladas e inofensivas, una serie de incidentes alteraron la percepción de su finalidad, de inocua y útil a algo más siniestra.

Una de ellas tuvo lugar en 1999, donde una persona tuvo un accidente dentro de una cadena de supermercados en Los Ángeles, por lo que le interpuso una demanda. Como respuesta, los abogados del establecimiento amenazaron con revelar al tribunal el historial de compras de alcohol de la víctima para salir impunes (Brunton y Nissenbaum, 2015, p. 28). Una sucesión de casos similares en los años siguientes alimentó la sospecha de que las supuestamente inocuas tarjetas de fidelización estaban sirviendo para fines que iban más allá de la concesión de descuentos. Es por ello que, poco después de su introducción, se desarrollaron redes de intercambio de tarjetas en las que la gente las compartía para ocultar datos sobre sus patrones de compra. Desplegadas inicialmente a través de reuniones físicas organizadas *ad hoc*, más tarde se sirvieron de listas de correo y redes sociales para ampliar estos intercambios entre personas que vivían cada vez más lejos unas de otras. Este intercambio de tarjetas de fidelización constituiría un tipo de ofuscación de la identidad como una actividad de grupo, dado que cuanto mayor sea el número de personas dispuestas a compartir sus tarjetas, y cuanto más lejos viajen éstas, menos fiables serán los datos recopilados, mientras que los consumidores pueden seguir disfrutando de los descuentos ofrecidos.

Resistencia en la economía de plataforma

Avanzando hacia la resistencia dentro del poder de las plataformas, Bonini y Treré (2024, p. 24) indican a que existe una variante que apunta a los propios algoritmos, entendidos como herramientas mediante las que ciudadanos, trabajadores, artistas, académicos críticos y activistas ejercen sus acciones de protesta. A partir de las dificultades que dichos colectivos enfrentan cotidianamente mientras lidian con decisiones opacas tomadas por éstos, las prácticas ciudadanas que despliegan para reapropriarse de los mismos a través de la creatividad y el ingenio, pueden interpretarse como formas de resistencia a través de los algoritmos.

Bonini y Treré (2024, p. 74) mencionan que los disturbios, las huelgas y las protestas son una continuación de las luchas pasadas y representan sólo las manifestaciones más obvias del disenso y el descontento que ha animado a los trabajadores de las distintas plataformas en los últimos años. Los cortes de tráfico en la ciudad, los piquetes frente a las sedes corporativas del sector y los disturbios

estallan cuando la ira y el descontento alcanzan picos insoportables. Sin embargo, para estos autores, estas formas de resistencia pública al poder de las plataformas son sólo la punta del iceberg, en la medida en que, según ellos, la mayoría de trabajadores de esta industria no quiere destruir el trabajo que les permite (mal)ganarse la vida, sólo quiere mejorar sus condiciones. Este tipo de resistencia cotidiana (Scott, 1985), describiría todas las formas de disenso que no son tan dramáticas y visibles como los disturbios y las revoluciones. Las conductas de resistencia cotidianas de los grupos subalternos (por ejemplo, la lentitud, la huida, el sarcasmo, la pasividad, la pereza, los malentendidos, la deslealtad, la calumnia, la evasión o el robo) suelen estar ocultas o disfrazadas.

Aunque Bonini y Treré apuntan que no deberíamos romantizar estas formas de microresistencia, tampoco deberíamos subestimarlas (2024, p. 25), ya que su objetivo no suele ser subvertir o cuestionar el poder de las plataformas, como ocurre con otras formas de resistencia. A menudo, encuentran un intento de obtener alguna pequeña ventaja personal o colectiva, de ahorrar tiempo y dinero, de obtener victorias temporales o de poner “un palo en las ruedas” de las plataformas.

Así, estos autores (Bonini y Treré, 2024, p. 83) destacan que, por ejemplo, en China y la India algunos repartidores se han registrado en plataformas de entrega de alimentos a la vez como repartidores y como clientes. Cuando los pedidos disminuyen o cuando un repartidor quiere aumentar su *ranking*, a veces recurren a una práctica que los repartidores chinos llaman *shuadan*, un verbo chino que significa “crear pedidos falsos artificialmente”. De este modo, dichos trabajadores emplean su cuenta de cliente para realizar un pedido que es asignado a su cuenta de repartidor, para después rechazarlo y, o bien quedarse con la comida sin pagar, o bien no cogerla y simplemente aumentar su número de repartos para escalar en la posición algorítmica que llevará a que les asignen más pedidos en el futuro.

Por otra parte, y entendiendo que los trabajadores de las plataformas no son usuarios pasivos de éstas, Bonini y Treré (2024, p. 91) recogen ejemplos de cómo han comenzado a cuestionar la posibilidades que ofrecen. De esta manera, los repartidores con mayor conocimiento en tecnología han creado aplicaciones no autorizadas que permiten funciones no permitidas por las aplicaciones originales, forzando ilegalmente sus límites tecnológicos. Por ejemplo, en Indonesia, donde la mayoría de los repartidores trabajan para una plataforma denominada Gojek, la investigadora Rida Qadri descubrió que:

en los últimos seis años, ha surgido un floreciente mercado subterráneo de aplicaciones para Gojek de terceros no autorizadas. Cada aplicación *tnyul* (no autorizada) debe su nombre a un espíritu infantil del folclore indonesio que ayuda a su amo humano a ganar

dinero robando y responde a necesidades específicas de los repartidores para ayudar a que sus trabajos sean menos miserables (Qadri, 2021, citado en Bonini y Treré, 2024, p. 91).

De hecho, continúan comentando que desde que Gojek se creó en 2015, los conductores con más conocimientos en tecnología comenzaron a ayudar a otros colegas a resolver problemas técnicos creados por la aplicación. Con el tiempo, pequeñas tareas de soporte técnico, como restablecer los valores de fábrica o reiniciar y reparar el GPS, dieron lugar a esta variedad de aplicaciones no oficiales para las necesidades de diferentes conductores. Algunas de estas innovaciones ilegales introducidas por los mensajeros indonesios fueron incluso copiadas por la propia Gojek. De este modo, esta empresa mejoró su servicio al apropiarse de la innovación generalizada que surgía “desde abajo” y, finalmente, ahorró recursos en investigación y desarrollo. Por contraparte, los conductores de Gojek pudieron obligar a la plataforma a revisar sus posibilidades y, por lo tanto, a mejorar sus propias condiciones de trabajo.

Data fandom y Fan activism

Los fans del K-pop son famosos por su increíble capacidad de movilización, incluyendo la compra de grandes anuncios en Times Square (Herman, 2018) o por conseguir en poco tiempo que sus bandas favoritas alcancen el número 1 en las listas (Blake, 2021). Se trata de un *fandom* muy bien organizado a escala mundial que realiza diferentes estrategias. Entre ellas destacan los *sumseuming*, que significa “reproducción continua las 24 horas del día, los 7 días de la semana, mientras uno respira” y es una palabra utilizada en el *argot* de los fans de grupos coreanos para referirse a la reproducción repetida de un artista para aumentar sus cifras de las listas de plataformas como Spotify (Kang, 2020).

Sobre este *fandom*, Bonini y Treré (2024, p. 107) relatan también cómo los fans de BTS (un grupo de música coreano) en EEUU crearon cuentas falsas para reproducir la música de la banda en servicios de *streaming* y distribuyeron el acceso a estas en otros países a través de las redes sociales. Los destinatarios transmitieron la música de BTS de forma continua en múltiples dispositivos a través de redes privadas virtuales (VPN, por sus siglas en inglés), las cuales pueden ofuscar las ubicaciones redirigiendo el tráfico de los usuarios a través de múltiples servidores globales. Algunos fans incluso llegaron a organizar donaciones para que otros pudieran pagar por cuentas de *streaming premium*. Este tipo de acción en red infló artificialmente el consumo del álbum de BTS en EEUU y engañó a los algoritmos de Spotify, que interpretaron el gran aumento de *clicks* como una tendencia musical en rápido ascenso que merecía una mayor visibilidad. A su vez, los algoritmos de Spotify incluyeron automáticamente las canciones de BTS en un mayor número de listas de reproducción generadas por algoritmos, convirtiéndose así en aliados

involuntarios de la estrategia diseñada por los fans de BTS.

Qian Zhang y Keith Negus (2020) sostienen que estas prácticas son el resultado de un tipo particular de fandom: el “*fandom* de datos”. Este tipo de fans adoptan estrategias individuales y colectivas para «intervenir deliberadamente e influir en los datos estadísticos, sonoros y semánticos recopilados y reportados en las plataformas digitales y las redes sociales» (Zhang y Negus, 2020, p. 494). Esto es debido a que se han dado cuenta de cómo son relevantes para la industria musical, en tanto son entendidos como datos, por lo que se apropian de este conocimiento para beneficiar a sus músicos favoritos y mejorar sus métricas y número de reproducciones.

Otro caso que merece ser relatado es uno reciente protagonizado por el *fandom* de Taylor Swift, denominado *swifties*. Así, cuando a principios de 2024 se produjo la difusión de imágenes sexualmente explícitas de la cantante estadounidense creadas con modelos generativos, las denominadas *deepfakes* pornográficas (Brascia, 2024), dichas *swifties* respondieron utilizando tácticas de *fake seeding* (siembra de archivos falsos). Para ello, lanzaron su propia campaña coordinada para enterrar el material pornográfico, inundando la red de contenidos nombrados y etiquetados con los términos de búsqueda “*taylor swift ai*” o “*taylor swift deepfake*” que no se correspondían con lo buscado (Peirano, 2024).

Por otro lado, además de organizarse para apoyar a sus ídolos, los mismos *fandoms* del K-pop también establecen tácticas con fines activistas, en lo que Jenkins (2012, párr. 10) define como *fan activism* (activismo fan), esto es:

formas de compromiso cívico y participación política que surgen desde dentro de la propia cultura fan, a menudo en respuesta a los intereses compartidos de los fans, a menudo llevadas a cabo a través de la infraestructura de las prácticas y relaciones de los fans existentes, y a menudo enmarcadas a través de metáforas extraídas de la cultura popular y participativa.

En este sentido, resultó muy mediático el modo en que en 2020 los fans del K-pop sabotearon un mitin de Trump al solicitar entradas de forma masiva para luego no acudir al evento. Fruto de esta acción, los organizadores de la campaña cancelaron los eventos planeados fuera de dicho mitin debido a que se esperaba una multitud desbordante que después no se materializó (Lorenz *et al.*, 2020).

En otra ocasión, este *fandom* recibió también una gran cobertura mediática por sus habilidades algorítmicas al servicio de causas de justicia social. Este episodio nos devuelve al año 2020 en EEUU, cuando al calor de las protestas en respuesta a la muerte de George Floyd a manos de la policía en

Minneapolis y de la posterior amenaza del presidente Trump de emplear al ejército contra los manifestantes, el Departamento de Policía de Dallas pidió a la población que enviara videos de los manifestantes a través de una aplicación dedicada a ello. Bonini y Treré (2024, p. 153) relatan cómo fans del K-pop inundaron esta aplicación con contenido relacionado con este género musical que suponía la violación del *copyright*. Como resultado de esta paradójica saturación de la aplicación con contenido ilícito, el Departamento de Policía tuvo que eliminarla.

Este fandom también ha sido responsable de “secuestrar” *hashtags* promocionados por la derecha radical como #MAGA, #BlueLivesMatter y #whitelivesmatter, al inundarlos con clips de grupos de K-pop, *memes* y contenido similar para acallar las voces racistas y ofensivas (Bonini y Treré, 2024, p. 153).

En definitiva, a través de su compromiso constante con la arquitectura del ecosistema de las redes sociales, estos grupos de fans, han desarrollado una fuerte conciencia algorítmica y un refinado conocimiento tecnológico que usan para el beneficio de sus ídolos y para luchar por diferentes causas sociales.

2.5.3. Tácticas de resistencia contra el extractivismo de datos personales

Con demasiada frecuencia, relata Lyon (2022, p. 154) la informática y el diseño de *software*, ahora profundamente relacionados con la creación de algoritmos, se enseñan y se entienden como prácticas alejadas del mundo real. Los estudiantes disocian su programación de las “aplicaciones” reales y se desvinculan de cualquier sensación de que su trabajo implique política. Ante ello, Lyon defiende que las cuestiones relacionadas con la ética de los datos personales deben colocarse en el centro desde los planteamientos iniciales de estas tecnologías.

En esta línea, cabe recalcar que el extractivismo de datos se caracteriza por su dependencia de la colaboración de las personas, las cuales dan a las plataformas lo que quieren y permiten que su éxito se expanda cuanto más tiempo pasan en sus aplicaciones. Pero hemos visto cómo aquellos que participan en las plataformas también pueden hacerlo por motivos de resistencia: a través de tácticas subversivas en contraposición a estrategias de vigilancia, este mismo escepticismo y resistencia podrían orientar enfoques más críticos de la vigilancia en general. Como indica Lyon (2022, p. 159), todos estamos implicados en esta vigilancia; pero también podríamos estar implicados en su reformulación.

Dado que Internet es tan importante hoy en día, es esencial que las prácticas emergentes en ella se vean como lo que son, no sólo las cuestiones de recopilación y análisis de información de vigilancia se

refieren principalmente a Internet, sino que los debates relacionados con ellas se llevan a cabo con frecuencia en él. La mayor parte de lo que se discute sobre la cultura de la vigilancia se relaciona de algún modo con Internet, no sólo con la vigilancia de la seguridad nacional, sino también con las redes sociales, el Internet de las cosas y las formas en que nuestros dispositivos y entornos están cada vez más interconectados y, por supuesto, registran y comparten datos personales.

En este sentido, de nuevo los contextos se revelan como cruciales. Por lo que las ideas de Nissenbaum sobre la “integridad contextual” resultan muy fructíferas en este campo, al informar y dar lugar a una serie de prácticas que intentan abordar de manera más directa cómo los usuarios comunes de Internet entienden las cuestiones del manejo de la información personal.

A lo largo de estas páginas hemos visto cómo la vigilancia es vista como una sombra de las estrategias de poder dominantes, hoy ampliamente entendidas como capitalismo de vigilancia. Esas actividades incluyen el control de la población, la gestión de las ciudades, la securitización de los sistemas de transporte y comunicación, todas las cuales son, en el sentido de Michel de Certeau (1990), “estrategias” de poder. En su estimulante análisis, recurrir a la vida cotidiana es emprender una exploración orientada a encontrar “tácticas” de poder que contrastan con los códigos dominantes de control y eficiencia y, a veces, los cuestionan. Al tratar de entender cuáles podrían ser algunas de esas tácticas, mediante la exploración de imaginarios y prácticas, descubrimos nuevos tipos de creatividad a medida que las personas identifican y buscan significados que son importantes para ellas.

No obstante, en este punto estimo crucial retomar el hilo que Florencio Cabello (2019, p. 35) rescata de la obra *Textual Poachers* (cazadores furtivos, en castellano) del anteriormente citado Henry Jenkins (1992) para reflexionar acerca de los límites de las tácticas de Certeau y, sobre todo, para trascenderlos:

La orientación de la crítica del autor estadounidense se identifica ya desde el título del apartado donde desarrolla su argumentación sobre dicho límite: «*What do poachers keep?*» —«¿Qué guardan los cazadores furtivos?». Y es que Jenkins difiere de Michel de Certeau cuando este afirma que «la lectura no posee garantías contra el desgaste del tiempo (uno se olvida y olvida) y no conserva (o lo hace mal) aquello que adquiere». Centrándose en los aficionados televisivos, el teórico de Atlanta repondrá que «los fans logran guardar aquello que producen con los materiales que ‘cazan furtivamente’ de la cultura masiva [...] Los fans poseen [...] una cultura específica construida a partir de la materia prima semiótica que les proporcionan los media, [la cual] desafía las reclamaciones de la industria mediática de ostentar *copyrights* sobre las narrativas populares» (Jenkins, 1992, p. 44).

A raíz de esto Cabello se cuestiona cómo imaginar dentro de las estructuras comunicativas y tecnológicas predominantes un ámbito donde esta producción cultural “furtiva” pudiera persistir y, más allá, reinventarse. Tras examinar las dos referencias lingüística (los usos) y polemológica (las tácticas) que Michel de Certeau utiliza para definir los modos de hacer, Cabello (2019, p. 37) sugiere el procomún como una tercera referencia que ayuda a completar esta caracterización, ampliando las cuestiones sobre permanencia, legado y materialidad presentes en el análisis de Jenkins.

Para ello propone aproximarnos al procomún teniendo en cuenta su opuesto —los cercamientos— que, tal y como Antonio Lafuente señala, nos revela lo común invisibilizado, que a menudo pasa desapercibido y se asume sin cuestionamiento. Recordemos simplemente cómo en el apartado 2.1.1. veíamos que el proceso de «acumulación primitiva» surgido de la expropiación de las tierras comunales del campesinado europeo que analiza Marx, pero también de la gran caza de brujas examinada por Silvia Federici, dio paso al nacimiento del proletariado industrial (con su correlato indisociable de degradación de las mujeres). En consonancia con ello, Emmanuel Rodríguez y Raúl Sánchez Cedillo vinculan dichas tierras comunales con la contemporánea concepción de un procomún basado en la «inteligencia colectiva» (que emparentan con la noción marxiana de *general intellect*) para así denunciar una nueva campaña «de expropiación y subordinación a la producción bajo mando de esas nuevas tierras comunes» (Rodríguez y Sánchez Cedillo, citados en Cabello, 2019, p. 38) bajo la forma de «cercamientos de la inteligencia colectiva», a su vez emparentados con la citada noción de «acumulación primitiva».

A partir de aquí, ¿de qué modo podemos definir el procomún para entenderlo como esos “lugares comunes” donde preservar y recrear el legado ético y estético de golpes tácticos carentes de un lugar propio?

Una referencia clave la ofrece Yochai Benkler (citado en Cabello, 2019, p. 40), quien define el procomún como «una específica forma institucional de estructurar el derecho de acceso, uso y control de los recursos» que se opone a la propiedad porque no asigna tales derechos de forma exclusiva sino que los abre de forma igualitaria a una colectividad más o menos definida, la cual «puede usar o disponer de los recursos regidos por el procomún, de acuerdo con unas normas que pueden ir desde el “todo vale” a reglas formales escrupulosamente articuladas que se aplican de modo efectivo». En pocas palabras, el autor plantea que el procomún implica «libertad para operar bajo restricciones simétricas, disponible para una clase de usuarios abierta o indefinida» (Benkler, 2014, p. 70).

En esta línea, Antonio Lafuente, enfatiza que el procomún no debe entenderse como una forma

(menos) particular de propiedad, pues se aleja de tales nociones económicas para adentrarse en las concepciones antropológicas sobre las comunidades: «De la ética de los valores hemos de transitar a la de las capacidades si queremos entender cómo es la dinámica de producción del procomún, pues *un bien común no es más que una estrategia exitosa de construcción de capacidades para un colectivo humano*» (Lafuente, 2007, citado en Cabello, 2019, p. 42).

Más recientemente, Luis Lloredo Alix (2020) ha ofrecido un lúcido recorrido crítico por distintas concepciones (teológica, económica, jurídica y comunalista) de los «bienes comunes» para concluir defendiendo una «concepción política» basada en la propuesta de Peter Linebaugh (2008/2013, pp. 62-63) del «*commoning*» como acción, como «hacer común»:

[L]o común es más bien un proceso o punto de llegada, el fruto de una actividad política de cooperación, y no un punto de partida o un presupuesto identitario —un sujeto: la comunidad— respecto del cual puedan predicarse una serie de propiedades —unos objetos: los bienes comunes—. [R]equiere imbuir de co-participación todos los niveles, desde la producción hasta la toma de decisiones colectivas, desde lo rural a lo urbano, desde el mundo agrario al industrial, desde las tareas de cuidado hasta el trabajo cognitivo (Lloredo Alix, 2020, pp. 230-231).

Pues bien, si de abordar la co-participación en el campo de la comunicación se trata, Cabello (2019, p. 11) propone hacerlo aterrizando las prácticas e instituciones del procomún en la estructura de tres «capas» (física, lógica y de contenidos) con la que Benkler (2006/2015, p. 445) dota de «coherencia como un problema único» a los conflictos en cada uno de esos tres niveles de «la batalla por la ecología institucional del entorno digital»:

La capa física se refiere a los artilugios materiales usados para conectar a los seres humanos entre sí, incluyendo ordenadores, teléfonos, dispositivos móviles, cables, enlaces inalámbricos y similares. La capa de contenido [...] incluye tanto los enunciados mismos como los mecanismos de filtrado, acreditación e interpretación, en la medida en que estos se basan en la comunicación humana y no en el procesamiento mecánico. La capa lógica representa los algoritmos, estándares y formas de traducir el significado humano a algo que las máquinas puedan transmitir, almacenar o computar, y de ahí a algo que las máquinas procesen con vistas a una comunicación significativa para los seres humanos. [...] En cada una de estas capas hemos visto el surgimiento de funcionalidades técnicas y prácticas orientadas a su uso según un modelo no privativo que haría el acceso más barato y menos

susceptible de control por parte de un solo actor o conjunto de actores.

Orientadas de este modo hacia su preservación y recreación en el procomún, las tácticas que detallaré a continuación resultan relevantes no solo para las personas que las ponen en práctica para hacer frente al poder maquínico sino también para el resto de nosotros. Y ello porque representan la evidencia de que es posible transformar nuestra relación con las plataformas mediadas por algoritmos, bien a través del reforzamiento de nuestro marco jurídico, bien mediante la acción directa y expresiva que busca hacer inservible el extractivismo de datos, bien por medio de la búsqueda e implementación de alternativas democráticas consagradas a «eliminar la extracción financiera [...] para librarse de la perversa incentivación que empuja a una organización a tomar las decisiones incorrectas» (Rieback, 2021, párr. 9).

3. Tácticas de litigación colectiva por la privacidad en la UE: NOYB y el marco europeo de protección de datos personales

3.1. Breve recorrido sobre la legislación en la UE en materia de protección de datos

El derecho a la protección de datos y el derecho a la vida privada están estrechamente relacionados, pero son diferentes. En varios sentidos, la protección de datos es menos amplia que la privacidad de los mismos. La privacidad de los datos se refiere a proteger la información de ser vista por personas no autorizadas, especialmente en situaciones donde la protección de los datos no es suficiente, como en casos de intrusión a la privacidad física o cuando los datos se vuelven anónimos. Pero a veces la protección de datos puede cubrir más aspectos que la privacidad informativa, como cuando se comparten datos personales a propósito.

Valga esta introducción para constatar que en el ámbito jurídico el derecho al respeto a la vida privada y el derecho a la protección de los datos personales, aun estando relacionados, en ocasiones cuentan con regulaciones distintas. El derecho a la privacidad, también conocido como el respeto a la vida privada, es un derecho fundamental protegido en la legislación internacional desde su aparición inicial en la Declaración Universal de Derechos Humanos (DUDH) en 1948. Poco tiempo después de aprobar esta declaración, este derecho también fue reconocido en el Convenio Europeo de Derechos Humanos (CEDH), un tratado firmado por 12 Estados en 1950 con carácter vinculante.

Tanto la DUDH como el CEDH se adoptaron antes de que el uso del ordenador e Internet se volvieran populares y la información comenzara a digitalizarse. Para proteger nuestra información personal en esta nueva esfera, desde entonces se han ido aprobando nuevas reglas conocidas en algunas jurisdicciones como «privacidad de la información» y en otras como el «derecho a la autodeterminación en materia de información» (Consejo de Europa *et al.*, 2019, p. 21).

Así, la protección de datos en Europa empezó en los años 70 del siglo XX, cuando algunos países adoptaron leyes especiales para regular cómo se tratan los datos personales por parte del gobierno y las grandes empresas (Consejo de Europa *et al.*, 2019, p. 21). Tras esto, se crearon en toda Europa normas de protección de datos cuya importancia se hizo cada vez más importante, más allá del derecho a la privacidad.

En nuestros días, en las leyes de la Unión Europea (UE) la protección de datos se considera un derecho fundamental aparte del derecho a la privacidad. Así, por ejemplo, el Artículo 8 de la Carta de Derechos de la UE reconoce el derecho a la protección de datos personales y destaca los valores fundamentales relacionados con este derecho. De esta manera, establece que tus datos personales solo pueden usarse

con fines honestos y específicos, siendo necesario para ello contar con tu consentimiento o tener una razón legal válida para ello. Junto a esto, las personas deben poder ver y corregir su información personal, y esta corrección debe ser supervisada por una autoridad neutral.

En términos de legislación, es importante tener en cuenta que el Derecho de la UE se compone del Derecho primario y el Derecho derivado. Los Tratados, específicamente el Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), han sido ratificados por todos los países miembros y representan el “Derecho fundamental de la UE”. Las normativas, directrices y resoluciones emanadas de él son implementadas por las entidades autorizadas para ello en los Tratados, y conforman el “Derecho derivado de la UE”. Dentro de este, hallamos diferencias entre los Reglamentos y las Directivas, pues aquellos son directa e inmediatamente aplicables a todos los Estados miembros (como el conocido RGPD, Reglamento General de Protección de Datos), mientras que las Directivas necesitan ajustarse a cada Estado miembro a través de una transposición normativa nacional.

Finalmente, es importante resaltar el papel que desempeñan las Sentencias del Tribunal de Justicia de la Unión Europea (TJUE), dado que este tribunal tiene la autoridad para decidir si un país de la Unión ha cumplido con sus responsabilidades según las leyes de protección de datos. También tiene la tarea de interpretar las leyes de la UE para asegurar que se apliquen de manera efectiva y consistente en todos los países miembros. De hecho, desde que se creó la Directiva sobre Protección de Datos en 1995, se ha acumulado una gran cantidad de decisiones judiciales que explican qué significan los principios de protección de datos y el alcance del citado Artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea. En este sentido, las decisiones legales anteriores a la aprobación del RGPD siguen siendo vinculantes para entender y usar las reglas de privacidad de la UE, en la medida en que los principios básicos de la antigua ley de privacidad se han mantenido en la nueva.

A continuación, me dispongo a realizar un breve repaso por la evolución histórica de la legislación en materia de protección de datos en la UE, la cual sintetizo en el siguiente esquema:

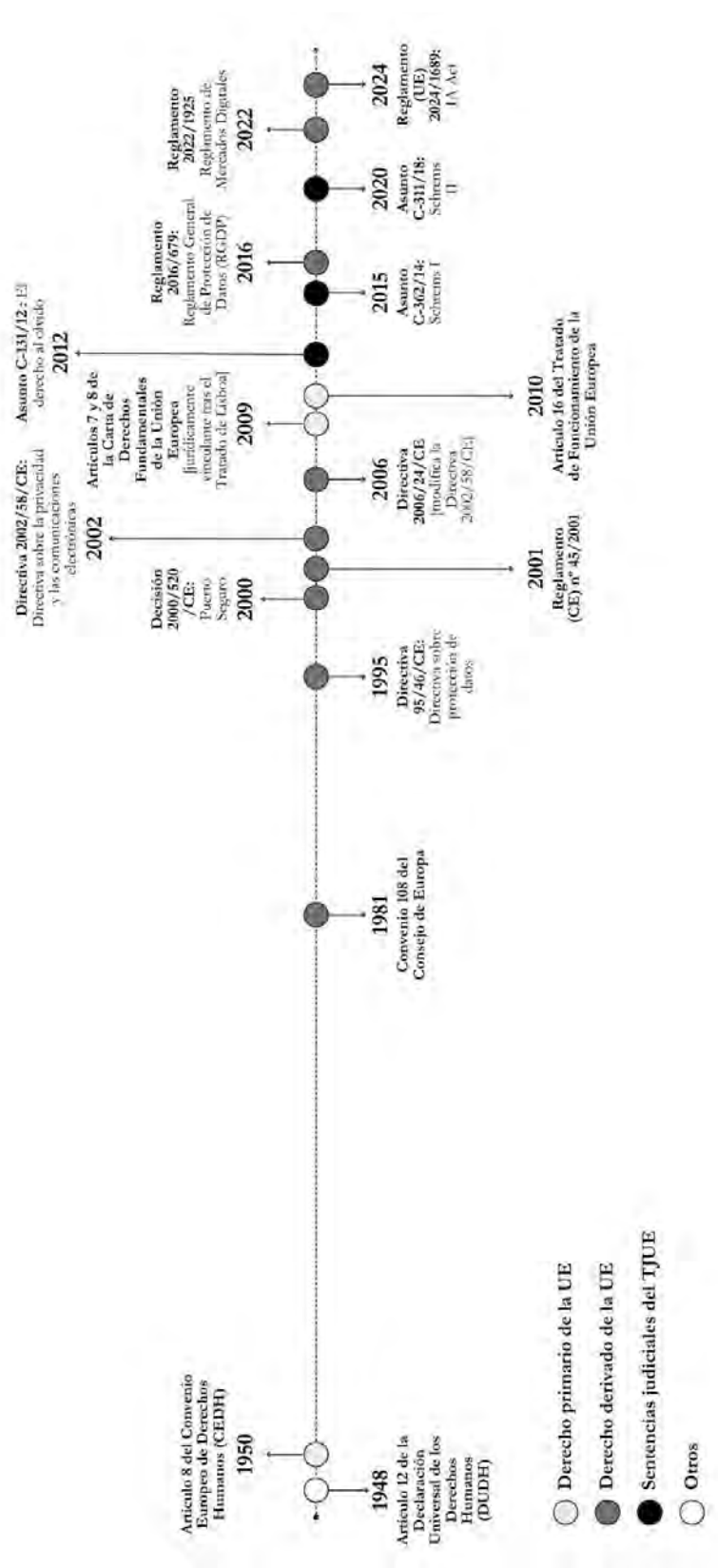


Figura 41. Evolución histórica de la legislación en materia de protección de datos en la UE. Fuente: Elaboración propia.

3.1.1. La Declaración Universal de los Derechos Humanos

Más allá de la UE, la primera vez que se definió en un documento internacional el derecho a salvaguardar nuestro espacio privado ante la intromisión de terceros, en particular del Estado, fue en 1948 en el artículo 12 de la Declaración Universal de Derechos Humanos, en relación al respeto de la vida privada y familiar:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (DUDH, 1948, Artículo 12).

3.1.2. El Convenio Europeo de Derechos Humanos

Si bien la DUDH no es una declaración vinculante, posee un papel significativo como pilar del derecho internacional en lo que respecta a los derechos humanos y ha impactado en la evolución de otras leyes de derechos humanos en Europa. Como avancé arriba, ello se ve reflejado en el Convenio Europeo de Derechos Humanos (CEDH) que, tras aprobarse en 1950, entró en vigor en 1953. En este caso, los países miembros sí que se obligan a cumplir el contenido de este tratado, incorporándolo y aplicándolo en su legislación nacional. Para garantizar que tal compromiso se lleva a cabo, en el año 1959 se creó en Estrasburgo el Tribunal Europeo de Derechos Humanos (TEDH).

En lo que respecta al derecho a la protección de datos, si atendemos al Consejo de Europa *et al.* (2019, p. 24), el CEDH va más allá de la DUDH al ampararlo explícitamente en su articulado, incluyendo los límites al mismo:

Derecho al respeto a la vida privada y familiar:

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás (Convenio Europeo de Derechos Humanos, 1953, Artículo 8).

3.1.3. El Convenio 108

El desarrollo de la tecnología de la información a partir de los años 60 del siglo XX provocó una acuciante necesidad por desarrollar regulaciones cada vez más precisas para proteger la privacidad y salvaguardar los datos personales. Dicho desarrollo culminó en 1981 con el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Este Convenio, según el Consejo de Europa *et al.* (2019, pp. 28-30), se aplica tanto al sector público como al privado y afecta también a las autoridades judiciales y los cuerpos de seguridad. El Convenio salvaguarda a las personas físicas frente a posibles abusos que pueden ocurrir en el manejo de sus datos personales, y simultáneamente persigue regular los flujos internacionales de datos personales. En relación al manejo de información personal, los principios fijados en el Convenio hacen referencia, especialmente, a la recolección y el tratamiento automático de datos de forma lícita y leal, con objetivos legítimos determinados. Esto implica que los datos no deben emplearse con objetivos distintos a estos y que tampoco deben ser almacenados por un periodo mayor al requerido en su inicio. También hace referencia a la calidad de los datos, los cuales deben ser apropiados, relevantes y precisos, y a que su acopio no debe ser desmesurado. A su vez, prohíbe el tratamiento de manera generalista de datos considerados sensibles.

Este Convenio también reconoce los derechos de las personas al conocimiento y rectificación de sus datos personales, al tiempo que regula el libre intercambio de información personal entre sus firmantes (todos los Estados miembros de la UE y, desde 1999, también la propia UE) e impone ciertas restricciones al tránsito de los datos en Estados donde la legislación no prevea una protección similar. Aunque el Convenio 108 como tal no está sujeto al control judicial del TEDH, a lo largo de los años este órgano se ha regido por el Convenio contextualizándolo dentro del Artículo 8 del CEDH.

Este tratado ha sufrido dos modificaciones a lo largo del tiempo: en 2001, estableció un Protocolo Adicional al Convenio 108 que atiende a los flujos de datos hacia terceros países, señalando la necesidad de establecer autoridades nacionales encargadas de la salvaguarda de esta información; y en 2018, lo sometió a un proceso de modernización con la adopción del Protocolo CETS n°223, que mantiene el carácter universal y adaptable del Convenio y fortalece su capacidad como herramienta universal para regular la protección de datos, incrementando las obligaciones de las entidades encargadas de su tratamiento. Para combatir el aumento de las prácticas de perfilado a partir de los datos extraídos de Internet, el Convenio también garantiza el derecho de las personas a no ser objeto de decisiones basadas exclusivamente en el tratamiento automatizado sin considerar sus propias opiniones.

3.1.4. La Directiva 95/46/CE: Directiva sobre protección de datos

Antes del RGPD, el principal instrumento jurídico dentro de la UE en esta materia era la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva sobre protección de datos). El origen de esta Directiva radicaba en la necesidad de armonizar las diferentes leyes que habían ido surgiendo por parte de los países miembros para generar un elevado estándar proteccionista relativo a la libre circulación de los datos que se producía.

Esta directiva ampliaba los principios de protección de datos de las citadas leyes estatales y del Convenio 108 y añadía instrumentos de protección, concretamente, la Directiva del control independiente. Sin embargo, los límites de esta directiva radicaron en su modelo legislativo, puesto que al no ser de aplicación directa, su objetivo armonizador fracasó al trasponerse de forma diferente en cada país, con diferentes interpretaciones, normas, mecanismos de control y aplicación, así como con sanciones dispares. A su vez, la evolución de las tecnologías de la información hizo que la Directiva quedara desfasada en diversas cuestiones, por lo que fue necesaria su posterior modificación en 2016.

3.1.5. Decisión 2000/520/CE: Puerto Seguro

Entre esta Directiva y el RGPD se aprobaron otras normas que complementaban a la primera, entre las que conviene que me detenga en primer lugar en la Decisión 2000/520/CE, a saber, la Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

Esta decisión estaba destinada a regular la transferencia de los datos personales de los ciudadanos de la UE con terceros países, transferencia que solo podía llevarse a cabo si se garantizaba un nivel de protección adecuado. Para el caso de la transferencia de datos con EEUU, dado que éste no cumplía los requisitos, se especificaron una serie de cuestiones que delimitaban dicha transferencia a que las entidades cumpliesen una serie de cuestiones enmarcadas en lo que denominaron “Puerto Seguro” (*Safe Harbour*).

De esta manera, como indica Pérez Yélamo (2024, p. 9), bajo el acuerdo de Puerto Seguro las corporaciones que deciden adherirse debían dar respuesta a una serie de principios fundamentales: la notificación de la recopilación y tratamiento que se va a hacer de sus datos así como el acceso a los

mismos; la posibilidad de no participar de los procesos de recopilación de datos y evitar su transferencia a terceros; la obligación, en el caso de que sí acepten dicha transferencia, de que los terceros que reciben los datos se adhieran también a lo establecido en el acuerdo de Puerto Seguro; y el deber de establecer medidas para proteger los datos, así como para recopilar solamente los necesarios para el propósito inicial. Finalmente, las empresas debían implementar un mecanismo que asegurase el cumplimiento de estos principios y demostrase que sus políticas de privacidad se ajustaban a este acuerdo.

3.1.6. El Reglamento (CE) nº 45/2001

Por otro lado, el Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, establecía una protección al tratamiento de datos personales por parte de las instituciones y organismos supranacionales de la UE. Además, esta directiva estableció una autoridad de control independiente, el Supervisor Europeo de Protección de Datos (SEPD), con competencias de control y con la obligación de vigilar el tratamiento de datos personales en las instituciones y organismos de la UE, así como de conocer e investigar las reclamaciones por presuntas violaciones de las normas de protección de datos. Tras la aprobación del RGPD este Reglamento fue derogado.

3.1.7. La Directiva 2002/58/CE

Otra cuestión que la UE consideró necesaria regular fue la protección de datos en el ámbito de las comunicaciones electrónicas, dado que, debido a la evolución de Internet y los dispositivos tanto móviles como fijos, resultaba crucial asegurar el resguardo de los derechos de sus usuarios a la privacidad y la confidencialidad. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), definía una serie de reglas acerca de la protección de la información personal en estas redes, así como de la comunicación de violaciones a la privacidad de las comunicaciones.

En términos de seguridad, los administradores de servicios de comunicaciones electrónicas debían, entre otros aspectos, asegurar que el acceso a la información personal se restringía únicamente a individuos autorizados y tomar acciones para prevenir que los datos personales no fuesen eliminados, perdidos o deteriorados de manera accidental. Cuando se presentase un riesgo concreto de infracción a

la seguridad de la red pública de comunicaciones, los operadores tenían la obligación de comunicar a los usuarios sobre dicho riesgo, además de alertar sobre un incumplimiento de la seguridad. Por último, la privacidad de las comunicaciones les obligaba, inicialmente, a abstenerse de la escucha, grabación, almacenamiento u otros métodos de intervención o supervisión de las comunicaciones y los metadatos. La Directiva también prohibía las comunicaciones no solicitadas (*spam*) y establecía normas acerca del almacenamiento de *cookies* en ordenadores y otros dispositivos.

3.1.8. La Directiva 2006/24/CE

La referida Directiva 2002/58/CE sufrió una polémica modificación por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Justificada por los problemas de seguridad apremiantes supuestamente identificados después de los ataques terroristas del 11 de marzo en Madrid en 2004 y del 7 de julio en Londres en 2005, esta norma exigía que los proveedores de servicios de Internet conservaran entre 6 meses y 2 años una plétora de datos (y metadatos) relativos al origen, destino, fecha, hora, duración, tipo de servicio y equipo usado en las comunicaciones telefónicas y por Internet (excluyendo solamente los vinculados al contenido de las mismas). Semejante carta blanca a la vigilancia preventiva indiscriminada motivó sendas cuestiones prejudiciales de altos tribunales de Austria e Irlanda ante el TJUE, el cual acabó invalidando la Directiva e 8 de abril de 2014 (STJUE de 8 de abril de 2014, C-293/12 y C-594/12, § 58-59), en una sentencia (que podríamos denominar “la primera sentencia de la “era post-Snowden” en la UE) que contenía rotundos argumentos como estos:

58. En efecto, por una parte, la Directiva 2006/24 afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales. [...]

59. Por otra parte, aun cuando la Directiva pretende contribuir a la lucha contra la delincuencia grave, no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública y, en particular, la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus

datos, a la prevención, detección o enjuiciamiento de delitos graves.

3.1.9. La Carta de Derechos Fundamentales de la Unión Europea

Otro hito reseñable en materia de protección de datos viene cuando la Carta de Derechos Fundamentales de la Unión Europea (en adelante La Carta) aprobada en el 2000 se convierte en un escrito jurídicamente vinculante como Derecho primario de la UE tras la (bastante accidentada) entrada en vigor del Tratado de Lisboa en 2009. Esta Carta abarca todos los derechos civiles, políticos, económicos y sociales de los ciudadanos de Europa, y representa la conjunción de las tradiciones constitucionales y responsabilidades internacionales que pertenecen a todos los Estados miembros. Las libertades mencionadas en el documento se agrupan en seis apartados: dignidad, derechos, equidad, solidaridad, ciudadanía y justicia. Para el caso que nos ocupa nos interesan dos artículos, el 7 y el 8, dado que esta Carta eleva la protección de datos a un derecho fundamental en la UE:

Artículo 7: Respeto de la vida privada y familiar: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8: Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente (Carta de Derechos Fundamentales de la Unión Europea, 2000, Artículos 7 y 8)

3.1.10. El Tratado de Funcionamiento de la Unión Europea

Este derecho se contempla también específicamente en el Artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) de 2010, en la sección relacionada con los principios fundamentales de la UE. Dicho artículo también establece una nueva base legal que concede a la UE el poder de legislar en relación a la protección de datos:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea (TFUE, 2010, Artículo 16).

Este es un progreso significativo, ya que las regulaciones de protección de datos de la UE anteriores se fundamentaron inicialmente en la base legal del mercado interno y en la necesidad de armonizar las leyes nacionales para no restringir el libre flujo de datos en la Unión Europea. El artículo 16 del TFUE sirvió de base jurídica para la reforma integral que aconteció con el RGPD.

3.1.11. Asunto C-131/12 : El derecho al olvido

Antes de la redacción final del RGPD hubo una serie de resoluciones judiciales del TJUE que supusieron cambios en la normativa de protección de datos. Entre la multitud de ellas recogidas por el Consejo de Europa *et al.* (2019) destaco, en primer lugar, la Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 en el asunto Google Spain, S.L., Google Inc. Contra la Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (Asunto C-131/12).

Este caso parte del citado Mario Costeja, quien tras la digitalización e indexación en Google de la edición impresa de 1998 del diario *La Vanguardia* comprobó que en sus resultados de búsqueda se hacía referencia a una antigua deuda suya ya saldada. Al ver afectada su imagen pública por dicha información, en 2009 el demandante solicitó al medio de comunicación que eliminase dichos enlaces, petición que fue denegada alegando el derecho a la información del medio en cuestión. Tras este intento, el afectado dirigió sus esfuerzos por corregir los resultados de búsqueda en Google, solicitando que no se indexasen los enlaces a esas noticias. Dado que la empresa estadounidense también se negó, comenzó una disputa judicial a la que se sumó la AEPD y que finalizó en 2014 con la sentencia del TJUE en la que aclaraba en su punto 3 que:

Los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas *web*, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas *web*, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita (STJUE de 13 de mayo de 2014, C-131/12, § 3).

Es tras este caso que se generalizó el derecho de los ciudadanos de la UE a solicitar la supresión de los enlaces a sus datos personales en los motores de búsqueda, lo cual trasladaba a los motores de búsqueda cierta responsabilidad en la preservación de los derechos de protección de datos de la ciudadanía.

3.1.12. Asunto C-362/14: Schrems I

Como apunté arriba al hilo de la invalidación de la Directiva 2006/24/CE, las revelaciones de Snowden en 2013 dejaron claramente en entredicho la seguridad de los datos personales europeos en manos de EEUU que recogía la Decisión 2000/520/CE. Al no revocar la UE por sí misma los acuerdos de *Safe Harbour* con EEUU, esta violación de derechos tuvo que ser denunciada por un joven estudiante de Derecho austríaco, Max Schrems. En calidad de usuario de Facebook, Schrems interpuso un litigio contra la filial europea de Facebook Inc. (radicada en Irlanda) ante la Autoridad de Protección de Datos irlandesa alegando que dicha compañía no aseguraba la protección de sus datos personales ante una posible intervención de las autoridades de EEUU justificada en supuestas razones de seguridad nacional (Cabezudo Vidal, 2023, p. 96).

Tras el rechazo inicial de la agencia irlandesa a admitir a trámite la demanda, finalmente el 6 de octubre de 2015 el TJUE zanjó la cuestión en su Sentencia denominada Maximilian Schrems contra Data Protection Commissioner. Petición de decisión prejudicial planteada por la High Court (Irlanda), (C-362). Conocida popularmente como la sentencia del Caso Schrems I, este dictamen del TJUE invalidaba la Decisión 2000/520/CE y, con ella, tumbaba los acuerdos de Puerto Seguro vigentes hasta entonces entre la UE y EEUU.

Como indica Pérez Yélamo (2023, p. 11), con esta decisión las compañías estadounidenses se vieron

privadas de un marco que supervisase su recepción de información personal desde la UE. Ante ello, la Comisión Europea se apresuró a negociar con el Departamento de Comercio estadounidense una respuesta a la sentencia del TJUE a la mayor brevedad, la cual se materializó en la instauración del llamado Escudo de Privacidad entre la UE y EEUU mediante la Decisión de Ejecución 2016/1250 emitida por la Comisión el 12 de julio de 2016.

3.1.13. Reglamento (CE) 2016/679: Reglamento General de Protección de Datos

Iniciados en 2009 y avivados por las citadas revelaciones de Edward Snowden, los intensos debates, sobre la necesidad de actualizar la normativa de protección de datos en la UE culminaron el 14 de abril de 2016 con la adopción del Reglamento General de Protección de Datos (RGPD). Tras un periodo de transición de dos años, finalmente esta normativa entró en vigor el 25 de mayo de 2018, y de esta manera quedó derogada la Directiva 95/46/CE.

Con este reglamento se adecuó decididamente la legislación europea a la salvaguarda de los derechos fundamentales en materia de protección de datos en la era digital. En este sentido, el RGPD introduce disposiciones nuevas acerca de la obligatoriedad por parte de las organizaciones de aplicar por defecto esta protección desde el diseño de sus servicios, de nombrar un delegado de protección de datos —si superan cierto tamaño—, y de respetar la portabilidad de dichos datos y de actuar de manera proactiva. Por otro lado, Pérez Yélamo (2023, p. 14) enfatiza la relevancia que adquiere en el RGPD la noción del consentimiento (al modo del lema feminista “Solo sí es sí”):

[E]l consentimiento debe ser explícito, informado, y a través de una afirmativa por parte del usuario. Los derechos de acceso, rectificación, supresión y la portabilidad de datos están claramente estipulados en los artículos 15 al 22, proporcionando un mayor control de los usuarios sobre sus datos personales. Además, en el artículo 25 se exige que la protección de datos sea una consideración central al inicio del desarrollo de un producto o servicio. Sobre las transferencias internacionales de datos se dedican los artículos 44 y sus subsiguientes, estableciendo que solo podrán llevarse a cabo lícitamente cuando cumplan los requisitos del propio reglamento y no comprometan la protección de las personas físicas.

Como he mencionado anteriormente, a diferencia de las Directivas, los Reglamentos deben aplicarse directamente en la legislación estatal sin necesidad de realizar una transposición, por lo que el RGPD ha venido a subsanar los inconvenientes derivados de la Directiva anterior, ofreciendo una normativa coherente y armonizada para todo el territorio de la UE.

3.1.14. Asunto C-311/18: Schrems II

La anteriormente mencionada Decisión de Ejecución 2016/1250 buscaba subsanar la derogación del *Safe Harbour* que el asunto Schrems I había propiciado. Según Pérez Yélamo (2023, p. 11), la nueva Decisión, también conocida como “Escudo de la privacidad”, exigía a las compañías adoptar normas más estrictas para garantizar transferencias de datos transparentes y seguras, restringía el acceso del gobierno de EEUU a dichas transferencias si no mediaban razones claras y precisas para ellas, y proporcionaba a los ciudadanos europeos la figura del Defensor del Pueblo, asignado para colaborar en la denuncia de posibles actos de vigilancia nacional ilegal. Esto último se incluye en los anexos III y VI de la decisión, donde se especifica un compromiso con la salvaguarda de los datos al sugerir una figura autónoma de los servicios de seguridad para preservar la privacidad de los ciudadanos.

Sin embargo, lejos de solventar el problema, este “escudo” vuelve a ponerse en entredicho en 2018, cuando Schrems regresa a los tribunales de Irlanda y el caso vuelve a ser examinado por el TJUE, a través del Asunto C-311/18, también conocido como Schrems II. Finalmente el 16 de julio de 2020 el TJUE decretó la invalidez de la segunda resolución de adecuación de la Comisión respecto a la transferencia de información personales a EEUU y reiteró su doctrina en relación con los estándares europeos de protección de datos.

Es interesante destacar aquí que, en paralelo a este dilatado litigio, fue aprobado e implantado el RGPD, el cual tuvo un importante papel a la hora de dictar la resolución, sobre todo las cuestiones relativas al consentimiento para la cesión de los datos:

el TJUE constató que la cesión de datos personales a Facebook Inc. no podía ampararse en el consentimiento explícito de los afectados, pues dicha transferencia se realizó sobre la base de cláusulas tipo, que no incorporan un consentimiento indubitado y específico para cada uno de los datos transferidos (Cabezudo Vidal, 2023, p. 120).

3.1.15. Reglamento (UE) 2022/1925: Reglamento de Mercados Digitales

Otro Reglamento que conviene citar aquí es el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, aprobado el 14 de septiembre de 2022, y en vigor desde mayo de 2023, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828, conocido como Reglamento o Ley de Mercados Digitales. Su propósito es asegurar un sector digital competitivo y equitativo, que facilite el desarrollo de las empresas digitales innovadoras y asegure la protección de los usuarios.

Este Reglamento introduce el concepto (algo eufemístico) de los “*gatekeepers*”, traducido como “guardianes de acceso”, y los define como aquellas grandes empresas tecnológicas que gestionan uno o varios servicios básicos de plataforma. Al ofrecer servicios fundamentales de plataforma, actúan como esenciales puertas de enlace para que las compañías alcancen a los usuarios finales. A su vez recogen y administran grandes volúmenes de información de usuarios, regulan el acceso a servicios populares y potencialmente esenciales, y tienen la capacidad de usar su posición para erradicar la competencia y restringir la innovación.

Para que navegadores *web*, redes sociales, asistentes de voz, motores de búsqueda, sistemas operativos y plataformas de video sean considerados “guardianes de acceso” se tienen en cuenta su volumen de mercado, la cantidad de datos que recopilan y el impacto que producen tanto en el mercado como en los consumidores europeos. Más concretamente, existen tres criterios de carácter cuantitativo para entender una corporación como guardián de acceso:

- i) cuando la empresa alcance un determinado volumen de negocios anual en el Espacio Económico Europeo y preste un servicio básico de plataforma en al menos tres Estados miembros de la UE; ii) cuando la empresa preste un servicio básico de plataforma a más de 45 millones de usuarios finales activos mensuales establecidos o situados en la UE y a más de diez mil usuarios profesionales activos anuales establecidos en la UE; y iii) cuando la empresa haya cumplido el segundo criterio durante los tres últimos años (Comisión Europea, 2023, párr. 15).

Siguiendo estos criterios, la Comisión designó en septiembre de 2023 a los seis primeros: Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft, y en total se consideran 22 los servicios que prestan. Tras esto se les otorgó un plazo de seis meses para el cumplimiento de las siguientes obligaciones establecidas en el Reglamento:

Ejemplo de lo que deberán hacer: las plataformas guardianas de acceso deberán

- permitir que terceras partes interactúen con los servicios propios del guardián de acceso en algunas situaciones concretas
- permitir que sus empresas usuarias accedan a los datos que generan al utilizar la plataforma del guardián de acceso
- ofrecer a las empresas que se anuncian en su plataforma las herramientas y la información

necesarias para que anunciantes y editores lleven a cabo su propia verificación independiente de los anuncios alojados por el guardián de acceso

- permitir que sus empresas usuarias promocionen sus ofertas y celebren contratos con sus clientes fuera de la plataforma del guardián de acceso

Ejemplo de lo que no podrán hacer: las plataformas guardianas de acceso ya no podrán

- clasificar más favorablemente sus propios servicios y productos que productos o servicios similares ofrecidos por terceros a través de la plataforma del guardián de acceso

- impedir que los consumidores se pongan en contacto con las empresas fuera de la plataforma del guardián de acceso

- impedir que los usuarios desinstalen programas o aplicaciones preinstaladas si así lo desean

- rastrear a los usuarios finales al margen del servicio de plataforma básica de los guardianes de acceso con fines de publicidad personalizada, sin que se haya concedido el consentimiento efectivo (Comisión Europea, s.f., párr. 17-26).

3.1.16. Reglamento 2024/1689: *AI Act*

Por último, quisiera finalizar este repaso con la reciente aprobación el 13 de junio de 2024 del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que también se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828, también conocido como Reglamento de Inteligencia Artificial o *AI Act*. Tal y como recoge el propio Reglamento:

El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial (en lo sucesivo, «sistemas de IA») en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de

protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación. El presente Reglamento garantiza la libre circulación transfronteriza de mercancías y servicios basados en la IA, con lo que impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente (Reglamento (UE) 2024/1689, 2024, (1)).

En materia de protección de datos, este Reglamento establece prohibiciones para la «compilación de bases de datos de reconocimiento facial mediante el raspado no selectivo de imágenes faciales de Internet o de grabaciones de CCTV» (EU Artificial Intelligence Act, 2024a, p. 2) así como la «identificación biométrica remota (RBI) “en tiempo real” en espacios de acceso público para las fuerzas de seguridad» (EU Artificial Intelligence Act, 2024a, p. 2) salvo contadas excepciones. A su vez, consideran Sistemas de IA de alto riesgos a aquellos que realizan perfilados de personas, esto es, «el tratamiento automatizado de datos personales para evaluar diversos aspectos de la vida de una persona, como su rendimiento laboral, su situación económica, su salud, sus preferencias, sus intereses, su fiabilidad, su comportamiento, su ubicación o sus movimientos» (EU Artificial Intelligence Act, 2024a, p. 3).

Dentro de él, encontramos también un artículo especialmente dedicado al tratamiento de datos, cuya fecha de entrada en vigor está prevista para el 2 de agosto de 2026 ((EU Artificial Intelligence Act, 2024b). Se trata del Artículo 59, relativo al tratamiento posterior de datos personales para el desarrollo de determinados sistemas de IA de interés público en el espacio aislado de regulación de la IA. En este artículo se establecen las condiciones para el uso de datos personales en el entrenamiento y prueba de determinados sistemas de IA, siempre bajo el fin de salvaguardar intereses públicos, cuando dichos datos no sean anónimos, sintéticos o de carácter no personal y cuando existen mecanismos de supervisión que eviten riesgos elevados sobre los derechos y libertades de las interesadas.

3.2. NOYB (None of Your Business)

3.2.1. Quiénes son

NOYB se define²⁴ como una ONG financiada mediante donaciones con sede en Viena (Austria) que trabaja para hacer cumplir la legislación sobre protección de datos, en particular el RGPD y la Directiva sobre privacidad en las comunicaciones electrónicas. Su nombre, sugerido por un usuario de Twitter, proviene de la abreviatura de *“None of your business”* (“No es asunto tuyo”).

Esta ONG fue fundada a comienzos de 2018 por Max Schrems, abogado y activista de la privacidad, el cual había litigado con éxito numerosos casos en el área de la privacidad y la protección de datos, entre los que destacan los ya mencionados contra Facebook y el Acuerdo de Puerto Seguro entre la UE y EEUU. Schrems confiesa en el primer informe anual de la organización (NOYB, 2020, p. 3) haber trabajado sobre la idea de crear una ONG profesional de cumplimiento de la privacidad (similar a las organizaciones de derechos del consumidor) que presentara casos contra grandes corporaciones en nombre de los usuarios, motivado por la cercana entrada en vigor del RGPD, el 25 de mayo de 2018, que incluía en su Artículo 80 la clave para su forma de trabajo:

Representación de los interesados

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.
2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con

²⁴ Véase: <https://noyb.eu/es/quienes-somos>

arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.
(Reglamento (UE) 2016/679, 2016, Artículo 80)

De este modo, gracias a que con el RGPD las posibles infracciones a la privacidad y a los derechos digitales de los ciudadanos realizadas por empresas y corporaciones pueden ser sancionadas a escala europea, facilitando así procedimientos mucho más eficaces y litigios estratégicos y recursos colectivos, NOYB se enfoca desde el principio en este tipo de casos.

En coherencia con lo anterior, este grupo no participa de manera directa en asuntos de supervisión gubernamental, ya que entienden que éstos son frecuentemente tratados por ONG ya establecidas o agrupaciones políticas locales. Adicionalmente, los equipos de supervisión gubernamental nacionales cuentan con una mayor capacidad para cuestionar las infracciones, ya que usualmente la supervisión gubernamental no puede ser cubierta a nivel europeo, sino en los tribunales nacionales correspondientes al gobierno en cuestión. Con todo, NOYB afirma simultáneamente que colabora con agrupaciones de este sector en este tipo de tareas.

De acuerdo con la legislación europea, son las Autoridades de Protección de Datos (APD) las que tienen el deber de garantizar el cumplimiento de nuestros derechos en cada país miembro de la UE. Sin embargo, NOYB es consciente de que hay motivos jurídicos, políticos y estratégicos (como la escasez de recursos) que restringen el anhelo y la habilidad de las APD para desempeñar su labor. Ante ello, y sin buscar sustituir ni eludir a dichas APD, NOYB se posiciona como una entidad no gubernamental que aborda asuntos relevantes que competen a las APD, garantizando el cumplimiento de la ley en tribunales civiles o mediante negociaciones directas con las compañías para paliar los posibles daños que estén produciendo antes de abrir una reclamación contra ellas.

La organización pudo fundarse gracias a una campaña de microfinanciación colectiva en Kickstarter que finalizó en enero de 2018, en la cual recaudaron 307.439€²⁵ gracias a las aportaciones de más de 2.500 personas (NOYB, 2020, p. 3). De esta manera, y antes de la entrada en vigor del RGPD, sus dos primeros abogados ya habían empezado a trabajar en una serie de posibles demandas. Las primeras fueron presentadas el mismo 25 de mayo, poco después de medianoche, contra Google, WhatsApp, Instagram y Facebook por el “consentimiento forzado” que ejercían. Con ellas NOYB (2020, p. 3) buscaba enviar una señal clara: «el *laissez-faire* en materia de privacidad había terminado».

Dentro de los principios generales²⁶ de la organización destacan, en primer lugar, su independencia y

25 Véase: <https://web.archive.org/web/20180203113909/https://noyb.eu>

26 Véase: <https://noyb.eu/es/nuestros-principios-generales>

neutralidad, es decir, se trata de una organización independiente e imparcial financiada mediante donaciones; en segundo lugar, la firme creencia de que los Derechos Digitales son Derechos Humanos, amparándose en la Carta de los Derechos Fundamentales, el Convenio Europeo de Derechos Humanos y la Declaración Universal de los Derechos Humanos; finalmente, NOYB también centra sus esfuerzos en la privacidad y la protección de datos dentro del sector privado y siempre con una visión paneuropea e intercultural.

A título organizativo, la ONG declara constituirse (NOYB, 2024a, p. 5) a través de una Asamblea General formada por miembros individuales distinguidos que están profundamente comprometidos con la privacidad, el RGPD y la aplicación de los derechos fundamentales. Junto a ellos, figuran representantes de sus aliados institucionales, como el Ayuntamiento de Viena y la Cámara de Trabajo de Austria, entre otros.

La Asamblea General, que trabaja sin ninguna remuneración, se reúne una vez cada dos años y nombra al Comité Ejecutivo, el cual se reúne trimestralmente para establecer los objetivos a largo plazo y revisar las operaciones de la organización. Según los estatutos de la organización, todos los miembros del Comité Ejecutivo también prestan servicios de forma estrictamente *pro bono*. Además de Schrems, la Junta Directiva está formada por Christof Tschohl, abogado y experto en privacidad y Petra Leupold, abogada y experta en derechos del consumidor.

A partir de aquí, la oficina jurídica de NOYB está compuesto por un equipo paneuropeo de 23 abogados y expertos. De esta manera, además de Schrems, la oficina la componen seis abogados/as de protección de datos, cuatro abogados/as en prácticas, tres desarrolladores y un técnico informático, además de un director de oficina, un director de operaciones, un gerente de proyectos, un encargado de recursos colectivos, una asistente de oficina, una responsable de creación de contenido y un responsable de relaciones públicas²⁷. Además de responder a las consultas iniciales y ayudar a sus miembros, la tarea principal de esta oficina es trabajar en los proyectos de cumplimiento y participar en la investigación necesaria para litigios estratégicos.

Es interesante indicar aquí que desde octubre de 2018, este grupo ofrece prácticas jurídicas para graduados universitarios en Derecho con un fuerte interés en la privacidad, los cuales pueden adquirir experiencia en investigación jurídica y redacción de reclamaciones sobre privacidad. Esta oficina también trabaja en la ejemplar base de datos pública sobre las reclamaciones en torno al RGPD, el GDPRhub, y en su boletín semanal, el GDPRtoday (NOYB, 2024a, p. 8). Además, este equipo se

²⁷ Véase: <https://noyb.eu/en/our-team-members-and-partners-0> Recuperado el 9 de enero de 2025

comunica por correo electrónico para consultas generales en inglés y alemán. También pueden responder consultas legales específicas en francés, italiano, holandés, español, catalán y griego.

3.2.2. Cómo trabajan

Según sus informes anuales (NOYB, 2024a, pp. 10-11), así como el apartado “cómo trabajamos” de su página *web*²⁸, NOYB busca fortalecer el derecho a la privacidad a través de «litigios estratégicos» y específicos contra corporaciones en función de la legislación vigente en la UE.

En términos prácticos, este carácter «estratégico» implica para NOYB examinar los posibles casos de manera minuciosa y priorizar aquéllos donde se ha producido una violación a la privacidad. De esta manera, detectan las posibles flaquezas legales y litigan empleando el enfoque más efectivo y el método más eficiente para cada caso, siempre con el objetivo de generar el máximo impacto. Así, NOYB interpone reclamaciones contra las compañías ante las entidades encargadas de la protección de datos (las mencionadas APD) de la UE o los llevan directamente a los tribunales competentes. En su enfoque de litigación, distinguen entre casos que buscan establecer estándares o normas cohesionadas y las que denominan como acciones coercitivas.

El sentido de los casos de establecimiento de estándares radica en que, dado que el RGPD es una normativa relativamente reciente, existen todavía muchos aspectos que no están claros o son objeto de controversia. Al desarrollar casos complicados enfocados en estas cuestiones inciertas, NOYB busca obtener una resolución de los tribunales superiores o las entidades de privacidad de la UE, como son el TJUE o el CEPD, que posteriormente establecerán el estándar para interpretaciones futuras del RGPD.

Por su parte, las acciones coercitivas se emplean en esas otras situaciones donde la legislación sí es bastante evidente, y donde el problema radica entonces en que algunas compañías simplemente no la respetan. El propósito de tales acciones de NOYB no es, pues, alcanzar una resolución del TJUE o el CEPD, sino asegurar que las autoridades nacionales de protección de datos apliquen la ley vigente para frenar las actividades ilícitas de dichas compañías. Para generar un impacto aún más significativo, NOYB destaca por su ambicioso despliegue de procedimientos a gran escala por los que presenta reclamaciones en diversos países de manera simultánea. Dos ejemplos que utilizan para explicar estas medidas, las cuales desarrollaré con mayor profundidad más adelante, son las 101 reclamaciones de NOYB contra transacciones ilícitas de datos a los EEUU o sus reclamaciones en masa contra anuncios de *cookies* fraudulentos.

²⁸ Véase: <https://noyb.eu/es/como-trabajamos>

Además de estas medidas, la ONG austriaca también hace uso de las relaciones públicas y de propuestas de los medios para respaldar el derecho a la privacidad sin necesidad de hacer uso de los tribunales. A su vez, fomenta un entendimiento compartido del RGPD y ofrece una plataforma de información denominada GDPRhub, que compila las resoluciones y la bibliografía legal relacionada con el RGPD. Por otro lado, NOYB también colabora con otras entidades para potenciar el efecto del RGPD, evitando así estructuras paralelas.

Para desempeñar su labor, este grupo aprovecha tanto la información que les facilitan sus miembros y patrocinadores como la que les llega a través de los denunciantes o el público general, a la que se suma la que detecta su equipo legal en función de diversos factores.

En primer lugar, NOYB busca que el caso en el que se va a involucrar tenga un gran impacto directo en la mayor cantidad de personas posibles, centrándose por ejemplo en toda una industria o en una práctica común en diferentes industrias y Estados. De esta manera, persiguen el objetivo de ampliar sus proyectos para aumentar aún más su repercusión y fomentar así el cumplimiento general a través de lo que denominan como «efecto indirecto» (NOYB, 2024a, p. 11).

En segundo lugar, la ONG elige casos en los que preliminarmente entiende que, dado que la infracción es obvia o la ley es muy clara al respecto, tiene altas posibilidades de éxito. Esto lo justifica afirmando que, dado que su financiación proviene en gran medida de donaciones, debe asignar sus fondos a aquellos asuntos con mayor tasa de éxito. Ello no quita que NOYB también asuma que en los casos en que buscan establecer un estándar porque la normativa no es tan clara, sí les merece la pena «correr el riesgo» (NOYB, 2024a, p. 11).

En tercer lugar, para la selección de casos, NOYB también tiene en cuenta todos los factores que pueden influir en el mismo, evaluando el calendario, la jurisdicción, los costes, los hechos, los denunciantes, los reguladores y que haya un «alto coeficiente de insumo/producción» (NOYB, 2024a, p. 11), todo ello con el fin de optimizar sus recursos. A su vez, la organización monitorea las acciones de las APD y los tribunales con el fin de beneficiarse de las condiciones más ventajosas, como pueden ser las tasas judiciales, el tiempo promedio de tramitación, experiencias previas y cuestiones similares. Por último, NOYB se cerciora de que sus casos estén limitados y bien definidos, de modo que, aunque una corporación viole casi todos los artículos del RGPD, sus acciones solo se centran en la parte más relevante.

De esta manera, NOYB procede a través de reclamaciones presentadas ante una autoridad nacional de protección de datos, encargada de hacer cumplir el RGPD. Cuando una APD recibe una de estas

reclamaciones, tiene la obligación de investigar y tomar una resolución en un periodo razonable. De manera frecuente, varias APD deben colaborar para tomar una decisión conforme al RGPD, por ejemplo, si el usuario perjudicado y la compañía involucrada no están en el mismo país. Si la APD no se pronuncia en el plazo establecido o si el interesado no está de acuerdo con el razonamiento jurídico, la decisión puede recurrirse ante los tribunales competentes.

Como apunté arriba, también es posible que la organización emprenda directamente demandas judiciales contra una empresa, las cuales, aun siendo más costosas que las reclamaciones, suelen ser más relevantes. Otra ventaja de este tipo de demandas es que no se someten a un procedimiento transfronterizo, tal y como sucedería con una reclamación contra una compañía ubicada en un Estado miembro distinto. Otra forma de disputa es el procedimiento de apelación de una reclamación, esto es, una acción legal que se dirige contra la decisión de una autoridad nacional con la que no están de acuerdo. Ante ello, el tribunal en cuestión tiene la facultad de enviar el caso a la siguiente instancia, hasta el Tribunal Supremo, que es responsable de resolver temas esenciales de interpretación jurídica.

3.2.3. Proyectos

Entre los diferentes proyectos en los que esta organización se involucra, reflejados en una sección específica de su *web*²⁹ podemos distinguir 14 temas diferentes, así como otros casos reseñables, como el reciente litigio conocido como “*pay or okay*”, los cuales merece la pena explicar brevemente:

Transferencia de datos entre la UE y EEUU

Aunque el primer caso de Max Schrems contra el llamado *Safe Harbor* es anterior a la constitución de NOYB como ONG, éste ha sido uno de los pilares fundacionales de la organización. Además, durante el llamado Schrems II, la organización brindó apoyo al abogado en su nuevo litigio contra Facebook y el llamado “escudo de privacidad” (NOYB, 2021, p. 10).

Tras la invalidación de este “escudo” en 2020, el grupo de abogados presentó 101 reclamaciones modelo contra empresas que seguían transfiriendo datos a EEUU³⁰. Cabe destacar entre ellas el caso C029-11 Tele2 Sverige AB³¹, en el que la autoridad sueca de protección de datos (IMY) emitió resoluciones contra cuatro empresas e impuso una multa de 12 millones de coronas suecas (1 millón de euros) al proveedor de telecomunicaciones Tele2, y de 300.000 coronas suecas al minorista en línea CDON, por utilizar Google Analytics en su página web (NOYB, 2023c).

29 Véase: <https://noyb.eu/en/projects>

30 Véase: <https://noyb.eu/en/project/eu-us-transfers> Recuperado el 9 de enero de 2025.

31 Véase: <https://noyb.eu/en/project/data-transfers/c029-11> Recuperado el 9 de enero de 2025.

Pero además de estas medidas coercitivas, NOYB también ha realizado esfuerzos por proporcionar información sobre cómo cumplir la sentencia a las empresas de la UE, al tiempo que asesoraba a los usuarios sobre sus opciones para detener las transferencias de datos a los EEUU.

Tanto Schrems como su equipo se encuentran preparados para impugnar cualquier nuevo acuerdo de transferencia de datos entre la UE y los EEUU que no se base en ningún cambio sustancial de las leyes y prácticas estadounidenses. Frente a ello, en una carta abierta sobre el futuro de las transferencias de datos entre la UE y EEUU NOYB (2022b) aboga por una solución a largo plazo basada en un acuerdo entre países democráticos que limite la vigilancia de las personas, sin importar su ciudadanía, a menos que se cumplan umbrales comunes (como una causa probable y una aprobación judicial).

Elaboración de perfiles y toma de decisiones automatizada

La toma de decisiones automatizada (ADM, por sus siglas en inglés) consiste en que sean las máquinas, sin intervención humana, las encargadas de resolver un asunto en función de datos factuales recopilados y de perfiles creados digitalmente (dobles de datos). Tanto en el sector público como en el privado, el uso indiscriminado de este tipo de decisiones basadas en última instancia en la programación (humana) de algoritmos afecta a la vida de las personas, independientemente de si no son convocadas a una entrevista laboral, reciben una calificación crediticia deficiente o están expuestas a precios personalizados (habitualmente al alza). Los principales problemas que surgen de su empleo incluyen el sesgo discriminatorio, así como la falta de responsabilidad y transparencia respecto a las causas de una decisión y la falta de posibilidad para explicar el fundamento en el que un algoritmo tomó una u otra decisión.

El artículo 22 del RGPD indica que los usuarios tienen derecho a no ser objeto de una decisión basada únicamente en procedimientos automatizados. A su vez, también tenemos derecho a expresar nuestro punto de vista, impugnar la decisión automatizada y recibir una intervención humana:

Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está

autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. (Reglamento (UE) 2016/679, 2016, Artículo 12)

Dentro de este marco, NOYB ha presentado varias reclamaciones contra gigantes tecnológicos, como Amazon y Airbnb, que no cumplieran con los derechos de los usuarios previstos en el RGPD. A su vez la organización ha emprendido investigaciones sobre cómo funcionan las ADM y la elaboración de perfiles, qué datos se utilizan y cuál es el origen de los mismos. De esta manera, en el momento en que escribo estas líneas NOYB ha interpuesto un total de cinco reclamaciones vinculadas a esta temática³².

Seguimiento en línea y móvil

El rastreador móvil o ID es un identificador único y general para todas las aplicaciones del mismo dispositivo. Se trata de una serie de números única que funcionan de manera similar a la IP, por lo que facilitan a proveedores de dispositivos móviles como Google y Apple, así como a terceros, la identificación de un usuario en las diversas aplicaciones que tenga instaladas en su terminal, y ayuda a conocer su comportamiento en línea y móvil, incluso si se desconoce la identidad de la persona usuaria en primera instancia. Dichos rastreadores suelen estar preinstalados en nuestro dispositivo, por lo que no se pueden eliminar, ni existe un método para interrumpir un seguimiento en el futuro.

Tal y como recalca NOYB³³, además de las normas aplicables en virtud del RGPD, el seguimiento está regulado estrictamente por el artículo 5(3) de la Directiva sobre privacidad y comunicaciones

32 Véase: <https://noyb.eu/en/project/profiling-automated-decision-making> Recuperado el 8 de enero de 2025.

33 Véase: <https://noyb.eu/en/project/advertising-ids>

electrónicas:

Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado (Directiva 2002/58/CE, 2002, Artículo 5(3)).

Por tanto, el almacenamiento de información o la obtención de acceso a información ya almacenada en el terminal del usuario solo está permitido mediante su consentimiento previo. En otras palabras, si una empresa no obtiene un consentimiento válido (denominado “*opt-in*” en inglés) antes de generar el ID de seguimiento, está actuando ilegalmente. Ante ello, y con el fin de eliminar los identificadores de seguimiento ocultos del entorno móvil, NOYB ha presentado varias reclamaciones en virtud de la Directiva sobre privacidad electrónica contra líderes del mercado tecnológico como Apple y Google, pero también contra empresas como MyFitnessPal, Fnac, Microsoft o Pinterest. Estas reclamaciones han alcanzado incluso a la propia Fundación Mozilla, denunciada por activar por defecto en el navegador Firefox una función llamada “atribución de preservación” de la privacidad, que sirve para rastrear las interacciones de los usuarios que luego se envían a los sitios *web* de forma agregada³⁴.

Dentro de esta categoría cabe reseñar también la multa de 5,8 millones de euros que NOYB consiguió que la Autoridad Noruega de Protección de Datos impusiera en 2020 a la aplicación de citas Grindr por recopilar y compartir datos personales sensibles de sus usuarios con terceros comerciales, los cuales podían volver a compartir de nuevo dicha información con otras empresas con el fin de realizar publicidad dirigida (NOYB, 2023d).

³⁴ Véase: <https://noyb.eu/en/project/online-mobile-tracking/c089> Recuperado el 8 de enero de 2025.

Identificación y autenticación

Dentro de esta categoría el grupo de abogados aglutina los casos relacionados con la sistemática tendencia de algunas empresas de solicitar excesivos datos personales alegando que son necesarios para fines de autenticación, cuando su verdadero objetivo es frustrar a los usuarios cuando desean ejercer sus derechos a través de los mecanismos disponibles. Ya que en muchos casos, los responsables exigen documentos de identificación, cuando solo a través de los datos de acceso a una cuenta sería suficiente para verificar al usuario en cuestión.

De esta manera, las reclamaciones de NOYB persiguen detener las comprobaciones rutinarias de identidad innecesarias y garantizar la seguridad de los datos mediante la solicitud de adaptación a formas de autenticación más sólidas y pertinentes. En esta línea, en Italia presentaron hasta 5 reclamaciones³⁵ dirigidas contra sitios *web* y *databrokers* que no atendían correctamente las solicitudes de acceso utilizando *cookies* como factor de autenticación y que llegaban a mostrar actitudes obstructivas que iban desde negar el derecho de acceso hasta exigir información adicional innecesaria para autenticar al usuario. En esta línea destaco de nuevo el caso de la aplicación Grindr, denunciada esta vez frente a la Autoridad de Protección de Datos de Austria por solicitar a un usuario que quiso ejercer su derecho de acceso (amparado por el Artículo 15 del RGPD) un *selfie* en el que apareciera un pasaporte y un papel con su dirección de correo electrónico, lo cual constituye una falta al reglamento.

Seguridad de los datos

Con el fin de minimizar los peligros de interceptación de información, el RGPD requiere que las compañías establezcan medidas de seguridad apropiadas, a través de diferentes puntos como el considerando 83, «donde se establece que el cifrado es una de las medidas posibles que pueden emplear tanto responsables como encargados del tratamiento para mitigar el riesgo» (AEPD, 2019, párr. 2), así como los artículos 6, apartado 4, letra e); el Artículo 32, apartado 1, letra a) y finalmente el Artículo 34, apartado 3, letra a) (AEPD, 2019). Si estos criterios no se respetan, se infringe la privacidad e integridad de nuestras comunicaciones. Aunque la mayoría de las compañías se encuentra en la “misma línea” que los usuarios en cuanto a la seguridad de sus sistemas, persisten fallos evidentes, ya sea debido a la negligencia o a la reducción de costes. Con el fin de satisfacer las exigencias de seguridad del RGPD, NOYB ha interpuesto una serie de reclamaciones a empresas como Amazon y Giropay, o incluso al Parlamento Europeo por una violación de la seguridad de los datos personales que contravenía varios Artículos del RGPD³⁶.

35 Véase: <https://noyb.eu/en/project/dating-apps> Recuperado el 8 de enero de 2025.

36 Véase: <https://noyb.eu/en/project/data-security/c086-01> y <https://noyb.eu/en/project/data-security/c086-02>

Calificación crediticia

Las agencias de calificación crediticia otorgan a las personas una puntuación de solvencia de cara a evaluar los riesgos de prestarles dinero o de extenderles un servicio de pago aplazado. En consecuencia, una puntuación crediticia bajo hace que a una persona le resulte más difícil participar en determinadas transaccionales en la sociedad (por ejemplo, obtener un contrato de telefonía móvil, un préstamo o un seguro).

Las empresas de evaluación crediticia manejan los datos de millones de clientes, por lo que resulta esencial que cumplan con el RGPD y respeten los derechos de los usuarios. La evaluación crediticia se gestiona de forma muy diferente en el seno de la UE, siguiendo a menudo las tradiciones nacionales en lugar de las nuevas normas del RGPD. Es por ello que dentro de este proyecto³⁷ NOYB busque limitar el uso de datos personales para calificación crediticia, así como acotar el intercambio de datos a gran escala entre terceros y agencias de calificación crediticia. A partir de aquí, la ONG trabaja para garantizar que los sistemas sean transparentes, conduzcan a resultados precisos y que los consumidores estén debidamente informados sobre el hecho de que las puntuaciones son generadas o intercambiadas entre diferentes empresas, fortaleciendo sus derechos de eliminación, acceso y rectificación amparados por el RGPD.

Derechos de los titulares de los datos

Dentro de esta categoría se aglutinan aquellas reclamaciones a empresas que no cumplen con los derechos otorgados por el RGPD a los ciudadanos de la UE, entendidos como “titulares de datos”, en lo relativo al acceso, rectificación, supresión, oposición o portabilidad, entre otros. Con estas acciones, NOYB persigue varios propósitos: alentar a los usuarios a ejercer su derecho fundamental a la privacidad, proporcionando información sobre cómo hacerlo; obtener una comprensión más profunda del procesamiento y uso de datos por parte de diferentes industrias mediante la presentación de solicitudes de acceso; y garantizar que las empresas respeten los derechos de los interesados y cumplan consistentemente con las solicitudes de los usuarios. A lo largo de los años, NOYB ha interpuesto 33 reclamaciones a diferentes empresas entre las que destaco a Microsoft, Google, Netflix, DAZN, Spotify, Amazon o Apple³⁸.

Recuperado el 8 de enero de 2025.

37 Véase: <https://noyb.eu/en/project/credit-scoring> Recuperado el 8 de enero de 2025.

38 Véase: <https://noyb.eu/en/project/right-rectification-art-16-gdpr> Recuperado el 8 de enero de 2025.

Consentimiento forzado y omisión del consentimiento

Según el RGPD, el consentimiento debe cumplir distintos requisitos para ser jurídicamente vinculante: debe darse libremente, de forma específica, informada e inequívoca. Según su Artículo 7:

Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato. (Reglamento (UE) 2016/679, 2016, Artículo 7)

Por tanto, el consentimiento debe solicitarse de forma transparente y justa y debe poder retirarse en cualquier momento, por lo que, básicamente, se necesita un consentimiento informado de “sí/no” o de “inclusión voluntaria”. Esto hace que haya una cantidad significativamente menor de personas que den su consentimiento, por lo que muchas empresas intentan eludirlo. De esta manera, compañías con gran cuota de mercado tienen la posibilidad de obligar a sus clientes a aceptar casi cualquier forma de procesamiento de datos, dándoles solo una oportunidad: o lo aceptan todo o no usan más ese servicio.

Sin embargo, a través de las diferentes reclamaciones llevadas a cabo por NOYB a este respecto consiguieron que se revertisen estas medidas y se garantizase que el Artículo 7 se cumpla y se aplique.

Destaco a modo de ejemplo las cuatro reclamaciones interpuestas el 25 de mayo de 2018³⁹ ante la CNIL francesa y la Autoridad Europea de Protección de Datos contra Google, Facebook, Instagram y Whatsapp, en las cuales consiguieron el reconocimiento de que estas empresas obligaban a sus usuarios a aceptar tanto sus políticas de privacidad como sus términos en su totalidad para poder seguir utilizando sus servicios.

Así, la primera decisión a este respecto por parte de la CNIL impuso el 21 de enero de 2019 una multa récord de 50 millones de euros a Google por falta de información facilitada a los interesados y falta de fundamentos jurídicos válidos para las operaciones de tratamiento relacionadas con la publicidad dirigida (NOYB, 2020, p. 10).

En los casos contra Facebook, Instagram y Whatsapp, hubo que esperar cuatro años y medio para que el CEPD considerara ilegal la supuesta “evasión” del RGPD por parte de Meta y le prohibiera utilizar datos personales con fines publicitarios, decisión vinculante que tuvo que aplicar la APD de Irlanda por la mencionada ubicación allí de la sede europea de la compañía. A principios de enero de 2023, el mismo CPD irlandés emitió tres decisiones finales sobre Facebook, Instagram y WhatsApp, imponiendo una multa de 390 millones de euros a Facebook e Instagram y de 5,5 millones a WhatsApp. Sin embargo, tanto Meta como NOYB decidieron recurrir estas decisiones en 2023 en tribunales nacionales de Alemania, Austria, Bélgica e Irlanda, así como a escala europea (NOYB, 2023a, p. 18).

Microsegmentación política, manipulación y seguimiento

Desde el esclarecimiento del caso Cambridge Analytica y la divulgación de informes acerca de gobiernos extranjeros que buscaban impactar en las democracias a través de la manipulación de datos personales para influir en las opiniones políticas de los usuarios, NOYB tiene un compromiso con respecto a la protección de datos de categorías especiales, como las opiniones políticas, para impedir que partidos políticos, plataformas y anunciantes se dirijan a los usuarios en función de las mismas. De esta manera ha interpuesto hasta diez reclamaciones a diferentes agentes entre las que destacan las vinculadas a las elecciones alemanas de 2021 (aún sin resolver pasados los siguientes comicios federales del pasado 23 de febrero de 2025), dirigidas contra partidos alemanes que van desde Alternativa para Alemania (AfD) y la Unión Cristiana Democrática (CDU) al Partido Socialdemócrata (SPD), los Verdes y Die Linke,⁴⁰.

39 Véase: <https://noyb.eu/en/project/forced-consent-dpas-austria-belgium-france-germany-and-ireland>

40 Véase: <https://noyb.eu/en/snap-election-faster-german-dpas-microtargeting-continues-influence-voters> Recuperado el 26 de febrero de 2025.

Procedimientos administrativos nacionales e inactividad de las APD

Si bien es cierto que según el RGPD las personas físicas pueden hacer valer su derecho a la privacidad ante una autoridad de protección de datos local, la realidad es que, según este grupo de abogados, a menudo las APD no investigan adecuadamente, tienen dificultades para avanzar en sus casos dentro del plazo estipulado o incluso los desestiman sin fundamento jurídico. Es por ello que NOYB dedica también sus esfuerzos a impugnar las decisiones de las autoridades de protección de datos cuando aquellas denuncias legítimas y bien fundamentadas son desestimadas o rechazadas de entrada sin la debida consideración.

Publicidad en línea

La publicidad en línea genera una serie de inquietudes vinculadas a la privacidad, dado que la publicidad personalizada frecuentemente conlleva el seguimiento de un usuario a través de múltiples páginas *web*, lo que puede provocar sospechas respecto la posible creación de perfiles. La recolección y almacenamiento de información personal puede, finalmente, provocar infracciones de datos derivados de nuestra carencia de control sobre dicha recolección y utilización para propósitos de publicidad. Es por ello que NOYB plantea una serie de reclamaciones que buscan restablecer el equilibrio entre las campañas de *marketing* y el derecho a la protección de datos. Entre ellas destacan las presentadas (y aún no resueltas) contra Google o Xandr (perteneciente a Microsoft), respectivamente por enviar correos electrónicos de *marketing* a través de Gmail sin consentimiento y sin comunicar la identidad del remitente, y por una falta de precisión y minimización en el tratamiento de los datos personales⁴¹.

Datos biométricos

El creciente uso de nuestros cuerpos para desbloquear áreas de las esferas tanto pública como privada ha generado graves preocupaciones con respecto a la privacidad y el uso de estos datos con fines de vigilancia. De hecho, cuando se utilizan sistemas para procesar los datos biométricos de cualquier persona en espacios públicos como parques, plazas o foros en línea, esto puede considerarse vigilancia masiva biométrica, en la medida en que estas tecnologías recopilan o analizan los datos biométricos de toda persona que ingresa a esos espacios, incluso si sus datos se descartan posteriormente.

Dentro de este marco, NOYB presentó en 2021 una reclamación contra Clearview AI, Inc., una empresa de reconocimiento facial que afirmaba tener la base de datos más grande conocida a partir de cuentas de redes sociales y otras fuentes en línea. Si bien en mayo de 2023 se declaró ilegal el uso de Clearview en la UE, no se le impuso multa o prohibición, por lo que NOYB reclamó la decisión con el

⁴¹ Véase: <https://noyb.eu/en/project/online-advertising> Recuperado el 8 de enero de 2025.

objetivo de que se decrete la prohibición europea de los usos que constituyen vigilancia masiva, independientemente de que los implementen actores públicos o privados⁴².

Otra empresa denunciada recientemente por el uso de datos biométricos es la aerolínea Ryanair⁴³, la cual no solo requiere un registro obligatorio para reservar vuelos en su página *web*, sino que somete a sus nuevos clientes a un proceso de verificación que incorpora un proceso de reconocimiento facial. Según NOYB, «las “cuentas obligatorias” de Ryanair violan el principio de minimización de datos del RGPD. El artículo 5, apartado 1, letra c), del RGPD exige que los datos personales sólo se traten si es necesario» (NOYB, 2024d, párr. 2).

Además, la compañía aérea coacciona a sus usuarios para que cedan sus datos biométricos si quieren ahorrarse trámites molestos, como pueden ser el envío de una firma manuscrita y la copia de su documento de identidad. Una vez más, NOYB (2024d, párr.8) considera que esta verificación obligatoria, «viola el principio de limitación de la finalidad (artículo 5, apartado 1, letra b) del RGPD)».

Inteligencia Artificial

Entre los múltiples problemas que plantean las tecnologías denominadas como “inteligencia artificial” no podía faltar el vinculado a la protección de datos personales. Estos problemas suelen estar relacionados con el hecho de que los modelos de IA requieren una gran cantidad de información para ser entrenados, la cual a veces se extrae de Internet o se recopila de otras fuentes, sin distinguir entre datos personales (o sensibles) y otras categorías.

Es por ello que NOYB cuestiona las prácticas en las que el desarrollo y el uso de la IA violan los derechos fundamentales de los interesados, en relación tanto con prácticas ilegales como con otras violaciones de los principios de protección de datos como la limitación de la finalidad, la minimización de datos y la limitación del almacenamiento. De esta manera, han elevado reclamaciones a empresas como OpenAI, por el procesamiento incorrecto de datos por parte de ChatGPT y la imposibilidad de acceder a la información personal procesada por el algoritmo⁴⁴, y a Meta y Twitter (ahora denominada X), por la utilización en diferentes Estados de cantidades masivas de datos de usuarios para formas indefinidas de “modelos de aprendizaje automático” o “inteligencia artificial”, sin tampoco informar de forma proactiva a sus usuarios⁴⁵. De hecho, a mediados de 2024 se conoció que en respuesta a las 11

42 Véase: <https://noyb.eu/en/project/biometric-data/c043> Recuperado el 9 de enero de 2025.

43 Véase: <https://noyb.eu/en/project/biometric-data/c065> y <https://noyb.eu/en/project/biometric-data/c092> Recuperados el 9 de enero de 2025

44 Véase: <https://noyb.eu/en/project/artificial-intelligence/c078> Recuperado el 9 de enero de 2025

45 Para obtener enlaces a todos los casos véase: <https://noyb.eu/en/project/artificial-intelligence> Recuperado el 9 de enero de 2025

reclamaciones interpuestas por NOYB (2024b), la CPD irlandesa anunció que Meta se comprometió a no procesar datos de usuarios de la UE/EEE para estos fines.

Banners de cookies

Como es bien sabido, tras la aprobación del RGPD los sitios *webs* deben incluir una ventana o mensaje emergente en el que indicar si utilizan *cookies* para su funcionamiento, y deben aportar información relativa a ellas con el fin de que el usuario acepte o no su uso. En este sentido, conviene recordar, como explicaba en el punto 1.1.1, que siempre es posible rechazar todas aquellas que no sean estrictamente necesarias para el correcto funcionamiento de la página sin que ello nos impida seguir navegando por el sitio.

No obstante, desde la implantación del nuevo reglamento NOYB constató que, a pesar de que los usuarios rechazasen activamente las *cookies* de seguimiento, estas se mantenían en algunos sitios *web* como Allocine.fr o Vanity Fair, entre otros (NOYB, 2019), lo cual constituía una falsa aplicación de la exigencia del consentimiento.

Del mismo modo, la ONG documentó que en multitud de *webs* los mensajes de notificación del uso de *cookies* eran engañosos y no cumplían con los requisitos del RGPD (NOYB, 2022c). Ante ello, a lo largo de los años NOYB ha desarrollado una exhaustiva campaña de recopilación de información y notificación de las infracciones a las empresas involucradas con el objetivo de que modifiquen sus notificaciones de *cookies* para cumplir con la normativa y evitar las posibles reclamaciones por parte de la organización. Aquellas empresas que no cumplieron tras este primer aviso se vieron envueltas en litigios por incumplimiento del RGPD. Según datos de la ONG, a fecha de 2023, se habían interpuesto un total de 700 denuncias de este tipo, respaldadas en gran medida por las APD europeas (NOYB, 2023b).

Pay or Okay

Directamente relacionados con las acciones sobre los “*banners de cookies*” y el “consentimiento forzado y omisión del consentimiento” se encuentran los casos agrupados con el nombre “*Pay or okay*”. Con ello se alude a la tendencia por la que a que cada vez más sitios *web* utilizan “muros de pago para *cookies*” o *banners* del tipo “Pagar o aceptar” (o acaso “Paga o traga”), que fuerzan a los usuarios a optar entre aceptar todas las *cookies*, lo que hace que sus datos se transmitan a cientos de empresas de seguimiento, o realizar una suscripción al sitio *web* —a menudo por un precio exorbitante—.

En estos casos, para NOYB resulta evidente que, los usuarios no tienen libertad de elección, ya que

decir “no” al seguimiento de cada sitio que emplea este tipo de *banners* no solo requiere mucho tiempo, sino que también entraña un alto coste económico. Este sistema lo comenzó en 2018 el diario austriaco *Der Standard* como un mecanismo para mantener la financiación del medio a través de la publicidad en el sitio *web*. Pese a que organizaciones como NOYB (2018) objetaron desde el principio que este tipo de *banners* eran ilegales independientemente de quién los utilizase, se permitió que los medios de comunicación empleasen esta práctica. Finalmente, en abril de 2023 la autoridad de protección de datos austriaca decidió que la llamada suscripción “*Pay or Okay*” ofrecida por el diario austriaco *Der Standard* era ilegal en su forma actual (NOYB, 2024a, p. 24).

Si bien la autoridad de protección de datos confirmó la admisibilidad general de “*Pay or Okay*”, especificó que los usuarios deben tener la oportunidad de decir “sí” o “no” a cada procesamiento de datos específico, tal como lo exige el RGPD. Dado que la decisión de la APD sembraba ciertas dudas, NOYB presentó un recurso ante el Tribunal Administrativo de Austria en mayo de 2023, el cual aún está pendiente de resolución.

De manera similar, el informe de ese año de NOYB (2024a, pp. 24-25) recoge cómo en junio de 2023 la autoridad de protección de datos de Baja Sajonia (LfD) decidió también que el *Pay or Okay* adoptado por el sitio de noticias tecnológicas *heise.de* en 2021 era ilegal. Aunque consideró que tal enfoque podría ser permisible en principio, consideró que el modo de adoptarlo del sitio de noticias en cuestión no se ajustaba a la ley porque no ofrecía la opción de dar el consentimiento explícito para ciertos fines. Esta decisión estaba en línea con las directrices de la Conferencia de Autoridades Alemanas de Protección de Datos (DSK), que en marzo de 2023 ya expresó explícitamente su preocupación por la falta de consentimiento específico y transparente en los sitios *web* que utilizan modelos “*Pay or Okay*”, sin abordar la cuestión más amplia de que los usuarios tengan que pagar precios exorbitantes para mantener la privacidad de sus datos personales. Además de los problemas relacionados con “*Pay or Okay*”, la citada LfD concluyó que *heise.de* utilizó métodos ilícitos y metódicos para influir en los usuarios en su propio beneficio, y que el consentimiento del usuario no fue informado, específico ni dado libremente. Además, señalaba que no fue lo suficientemente fácil revocar *a posteriori* un consentimiento dado previamente, lo que llevó al LfD a concluir que no existía una base legal para el procesamiento de los datos del usuario.

Sin embargo, la aceptación de su uso a lo largo de los años y el hecho de que el RGPD no haga distinción entre diferentes tipos de empresa, abrió la posibilidad de que otras corporaciones también hiciesen uso de estos sistemas.

Así es como en 2023, tal y como recoge Pérez Yélamo (2024, pp. 24-25), Meta emitió un mensaje a sus usuarios en el que les indicaba que si a partir de octubre de ese año deseaban utilizar su cuenta de la plataforma sin publicidad a través de la aplicación móvil, debían abonar mensualmente 12,99 euros (incluidos impuestos correspondientes), garantizando de esta manera que su información no sería utilizada para la publicidad segmentada. Y para cada aplicación extra que se quisiera emplear sin seguimiento de actividad debía aportarse 8 euros más. En el caso de que solo se visitase la red social a través de Internet, el importe era de 9,99 euros, añadiendo 6 por cada cuenta extra. En resumen, tener una cuenta en Facebook e Instagram en la aplicación móvil sin publicidad personalizada bajo este nuevo esquema de consentimiento forzado costaría 20,99 euros mensuales.

Por el contrario, si el usuario deseaba continuar utilizando sus productos de forma gratuita, debía autorizar a Meta a mantener el tratamiento de los datos que había guardado en sus cuentas para mostrarle publicidad, así como continuar utilizando las *cookies* de sus productos para personalizar la publicidad y realizar estadísticas.

Debido a esto, el 28 de noviembre de 2023 NOYB presentó una denuncia contra Meta ante la APD de Austria⁴⁶, alegando que el “*Pay or Okay*” no es más que otro intento por parte de la compañía de eludir las leyes de privacidad de la UE (NOYB 2023e, párr. 2), ya que en julio de 2023 el TJUE ya había dictaminado que el tratamiento de los datos de los usuarios por parte de Meta para anuncios personalizados era ilegal. Pero no solo eso, en enero de ese mismo año, el CEPD multó a Meta con 390 millones de euros por esta misma infracción y ordenó a la empresa obtener el consentimiento de los usuarios, todo ello en respuesta a una denuncia de NOYB interpuesta en 2018⁴⁷.

Aunque la reclamación de NOYB sigue sin resolverse, a finales de 2024 notificaron que Meta había modificado su método hacia otra variante que tampoco es el consentimiento de “Sí o No”, sino la alternativa de ofrecer «anuncios menos personalizados, en los que se seguirán utilizando datos como la ubicación y la fecha de nacimiento, sin consentimiento. Además, los “anuncios menos personalizados” aparecerán como anuncios “a pantalla completa” que no se pueden omitir» (NOYB, 2024c, párr. 1). Según NOYB, su equipo jurídico seguirá «de cerca la próxima ronda de este juego y siempre haremos cumplir el RGPD si Meta no ofrece las mismas opciones a los usuarios que dan su consentimiento para el seguimiento y a los que no» (NOYB, 2024c, párr. 5).

46 Véase: <https://noyb.eu/en/project/forced-consent-consent-bypass/c075> Recuperado el 9 de enero de 2025.

47 Véase: <https://noyb.eu/en/project/forced-consent-consent-bypass/c002> Recuperado el 9 de enero de 2025.

3.2.4. GDPRhub

En octubre de 2019, NOYB inició un boletín informativo con el objetivo de sintetizar, traducir y divulgar las resoluciones de las autoridades de protección de datos, así como las resoluciones judiciales de todos los países miembros de la UE. Para ello establecieron una base de datos que incluía a todas las fuentes nacionales de Europa de las resoluciones de las autoridades de protección de datos y los tribunales, junto con una herramienta para monitorearlas y generar alertas ante cualquier actualización. Luego, en febrero de 2020, presentaron GDPRhub: una *wiki* gratuita y abierta donde todo el mundo pueden hallar y compartir datos sobre el RGPD de toda Europa, además de un boletín informativo, denominado GDPRtoday, donde recopilan las últimas decisiones judiciales, junto con comentarios sobre los más recientes progresos a nivel global en materia de privacidad y protección de datos.

El nacimiento del GDPRhub surge de una necesidad interna de la organización, según explican en su página *web*⁴⁸, necesitaban una buena visión general de las decisiones de las autoridades de protección de datos (APD) y los tribunales nacionales. Bajo un espíritu de los bienes comunes creativos y el conocimiento compartido, decidieron publicar la mayor parte de su investigación de forma pública y gratuita en este *wiki*, y permitir la modificación y actualización con la ayuda de sus colaboradores voluntarios. De esta manera NOYB sigue un enfoque puramente académico, ofreciendo a los responsables de la toma de decisiones la realidad de la implementación del RGPD, lo que puede ayudar a un mayor cumplimiento incluso antes de que se inicie un litigio.

La información dentro del GDPRhub se divide en dos bases de datos independientes: las resoluciones y el conocimiento. En la sección de resoluciones, recolectan síntesis de resoluciones de las autoridades nacionales de protección de datos, los tribunales europeos y los estados miembros. Estos resúmenes se pueden encontrar categorizados bien según el artículo correspondiente del RGPD, la autoridad de protección de datos que los emitió o el tribunal que los resolvió. Para cada Estado miembro, supervisan diariamente más de 100 sitios *web*. Mientras que la sección de “conocimiento” incluye observaciones acerca de los artículos del RGPD y los perfiles de las autoridades encargadas de la protección de datos. Durante el 2023, gracias a más de 300 persona voluntarias se han recopilado y resumido más de 3000 decisiones, con más de 10000 suscriptores al boletín semanal de GDPRtoday (NOYB, 2024a, p. 21), además todo el contenido, a menos que se indique lo contrario, se comparte mediante una licencia *Creative Commons Attribution-NonCommercial-ShareAlike*.

⁴⁸ Véase: <https://noyb.eu/en/gdprhub>

The image consists of two side-by-side screenshots of the GDPRhub website. The left screenshot shows the homepage, which includes a search bar at the top, navigation links, and a 'Welcome to GDPRhub!' section. Below this, there are sections for 'New on GDPRhub', 'GDPR Decision Database', and 'GDPR Knowledge'. The right screenshot shows the 'Advanced Search' results page, which displays a list of search results. Each result includes details such as the case number, jurisdiction, relevant GDPR articles, type of decision, and a summary. The results are organized into a table with columns for 'Decision by', 'Case number/name', 'Jurisdiction', 'Relevant GDPR articles', 'Relevant national/other laws', 'Type of decision & outcome', 'Fine', and 'Contributor'.

Figura 42. Capturas de pantalla de la página de inicio de <https://gdprhub.eu/> y de la página de la base de datos de decisiones de GDPRhub https://gdprhub.eu/index.php?title=Advanced_Search Recuperado el 9 de enero de 2025

4. Tácticas de acción directa y expresiva frente al extractivismo de datos personales: Ofuscación como generación de ruido para vencer a la vigilancia digital

4.1. Antecedentes históricos

La ofuscación (*obfuscation* en inglés) es el acto de hacer que algo sea oscuro o difícil de entender. En su primer texto sobre la cuestión, Brunton y Nissenbaum (2011, párr. 1), la definen como:

una táctica de “resistencia vernácula” al registro y procesamiento automatizados de información personal que consiste en “producir datos engañosos, falsos o ambiguos con la intención de confundir a un adversario o simplemente de aumentar el tiempo o el coste de separar los datos malos de los buenos.

Más adelante, Brunton y Nissenbaum (2015, p. 46) puntualizan que, en su forma más abstracta, se trata de la producción de ruido modelado a partir de una señal existente para hacer que una colección de datos sea más ambigua, confusa, más difícil de explotar y trabajar sobre ella y, por lo tanto, menos valiosa.

En estas líneas cuentan que eligieron la palabra “ofuscación” para las actividades que estudian porque connota oscuridad, ininteligibilidad y desconcierto, y también porque ayuda a distinguir este enfoque de los métodos que se basan en la desaparición o el borrado de la información. Lo que desconozco es si estos autores tuvieron en cuenta que en castellano, “ofuscar” tiene dos connotaciones más que resultan muy pertinentes para este caso: la primera es «deslumbrar, turbar la vista» (RAE, s.f.), es decir impedir una observación por exceso —en este caso de luz—; y la segunda es «trastornar, conturbar o confundir las ideas, alucinar» (RAE, s.f.), es decir, en nuestro idioma sí tiene un enfoque más relacionado con la intención de confundir, cegar a alguien. Esto complementa muy bien la idea que estos autores reflejan de que la ofuscación supone que la señal puede detectarse de alguna manera para agregarle un exceso de señales relacionadas, similares y pertinentes: una multitud con la que un individuo puede mezclarse y, aunque sea por un corto período de tiempo, ocultarse (Brunton y Nissenbaum, 2015, p. 46).

La ofuscación ha sido durante mucho tiempo una metodología utilizada por investigadores y desarrolladores en ciertos subcampos de la informática, la ingeniería y las tecnologías aplicadas (Brunton y Nissenbaum, 2017, p. 1). Así, la ofuscación de código es ampliamente empleada con el objetivo de dificultar la ingeniería inversa de *software*, por motivos de seguridad, con la intención de ocultar código malicioso o para proteger la propiedad intelectual entre otros motivos (Clarís Viladrosa, 2015). Sin embargo, tal y como han estudiado Brunton y Nissenbaum (2015), la ofuscación también ha sido una táctica ampliamente empleada a lo largo de la historia en los campos tanto social como artístico.

Un ejemplo que suelo emplear cuando comienzo a explicar qué es la ofuscación ante un público que no está muy familiarizado con el término es la película dirigida por Stanley Kubrick, *Espartaco* (1960), a través de la escena en la que los soldados romanos piden a los esclavos rebeldes que identifiquen a su líder, a quien pretenden crucificar. Cuando Espartaco (interpretado por Kirk Douglas) está a punto de delatarse, uno por uno sus compañeros comienzan a identificarse a través del grito “¡Yo soy Espartaco!” hasta que toda la multitud reivindica ser ese a quien los soldados buscan, quedando la identidad del líder diluida.

Aunque este ejemplo es ampliamente conocido por la fama que tuvo la película, podemos rastrear otro caso similar en la literatura española del Siglo de Oro, concretamente en la obra teatral de Lope de Vega, *Fuenteovejuna* (1619), donde el dramaturgo se hizo eco de un suceso ocurrido siglos antes en el pueblo homónimo:

Los de Fuente Ovejuna, una noche del mes de abril de mil y cuatrocientos y setenta y seis, se apellidaron para dar la muerte a Hernán Pérez de Guzmán, Comendador Mayor de Calatrava, por los muchos agravios que pretendían haberles hecho. Y entrando en su misma casa le mataron a pedradas, y aunque sobre el caso fueron enviados jueces pesquisidores que atormentaron a muchos dellos, así hombres como mujeres, no les pudieron sacar otra palabra más ésta: “Fuente Ovejuna lo hizo”. (Covarrubias, 1611/1943, p. 612).

Este tipo de tácticas en la que muchas personas asumen la misma identidad para protegerse la reconocen también Brunton y Nissenbaum (2015, p. 16) en los levantamientos agrícolas ingleses de 1830 con la figura del capitán Swing, el omnipresente “Jacques” adoptado por los radicales en *Historia de dos ciudades* de Dickens, o la máscara de Guy Fawkes en la novela gráfica *V de Vendetta*, tan asociada actualmente con el grupo hacktivista *Anonymous*.

De manera similar, encontramos otros ejemplos de ofuscación en los que un grupo de personas trabajan de manera colaborativa para producir señales engañosas para ocultar su verdadera intención. Esta actividad se ve reflejada en diversas obras cinematográficas como la obra de Alfred Hitchcock *Con la muerte en los talones* (1959), donde su protagonista, Roger Thornhill, soborna a un mozo de equipajes de la estación de tren de Chicago para que le preste su uniforme y así evadir a la policía al mezclarse con el resto de trabajadores de la estación. Otra obra más reciente en la que vemos esta táctica es *La Casa de Papel* (2017), donde los ladrones hacen vestirse con el mismo mono rojo y careta de Dalí a sus secuestrados para ofuscar su identidad.

Aunque no solo se ofuscan identidades, pues Brunton y Nissenbaum (2015, pp. 16-17) relatan cómo existen diferentes casos en los que se han producido objetos idénticos como modos de ofuscación. En primer lugar, encontramos la leyenda de los ancilas de la antigua Roma: durante el reinado de Numa Pompilio, el segundo rey de Roma (753-673 a. C.), un escudo (*ancile* en latín) cayó del cielo y fue interpretado como un signo de favor divino, una reliquia sagrada cuya propiedad garantizaría la continuidad del imperio de Roma. Para su protección fue colgado en el Templo de Marte junto con once duplicados exactos, para que los posibles ladrones no supieran cuál tomar. Otro ejemplo son los seis bustos de yeso de Napoleón, de los que toma su título la historia *Los seis Napoleones* de Sherlock Holmes. En ella, el villano clava una perla negra en el yeso húmedo de un objeto que no sólo tiene cinco duplicados, sino que también pertenece a una clase más amplia de objetos (bustos blancos baratos de Napoleón) que son lo suficientemente omnipresentes como para ser invisibles. Este reclamo es utilizado de manera similar en la novela *Harry Potter y las reliquias de la Muerte* (2007), donde una maga realiza un hechizo sobre un objeto que quieren arrebatarle, provocando que cada vez que se toque se multiplique, ocultando el verdadero entre un mar de réplicas.

Un ejemplo real y más cercano sobre esto es el del llamado ladrón de Craigslist: A las 11 de la mañana del martes 30 de septiembre de 2008, un hombre vestido de exterminador (con una camisa azul, gafas protectoras, una máscara antipolvo y un pulverizador) se acercó a un vehículo blindado aparcado frente a un banco en Monroe (Washington) e incapacitó al guardia con gas pimienta para huir con el dinero. Cuando llegó la policía, encontró a trece hombres en la zona que llevaban una indumentaria idéntica siguiendo las instrucciones de un anuncio de empleo Craigslist, donde se prometía un buen salario por un trabajo de mantenimiento que debía comenzar a las 11:15 de la mañana en la dirección del banco. «Sólo se necesitaron unos minutos para determinar que ninguno de los trabajadores era el ladrón, pero unos pocos minutos fue todo el tiempo que necesitó para escabullirse» (Brunton y Nissenbaum, 2015, p. 17).

Otro campo en el que podemos hallar casos de ofuscación es el de las tácticas militares donde, al tener que transitar por territorio enemigo, es necesario ocultar la posición el mayor tiempo posible. Así, durante la Primera Guerra Mundial encontramos el empleo del camuflaje disruptivo (*dazzle camouflage* en inglés) para ocultar la presencia de barcos. Atribuida al artista marino británico Norman Wilkinson (Wilkinson, 1969), esta técnica consistía en trazar patrones únicos y complejos de formas geométricas con colores que generaban grandes contrastes en los buques para así ocultar su forma y, por lo tanto, confundir a los submarinos enemigos sobre la posición, dirección y velocidad en que se desplazaba el buque (Wilkinson, 1969, p. 79).

Sin embargo, este método perdió utilidad a medida que los telémetros y, especialmente, los aviones se hicieron más avanzados. Más aún, cuando el camuflaje disruptivo volvió a utilizarse en la Segunda Guerra Mundial, el uso de los radares provocó que se redujese aún más su eficacia, si bien aún conservaban cierta utilidad con los submarinos (Sumrall, 1973).

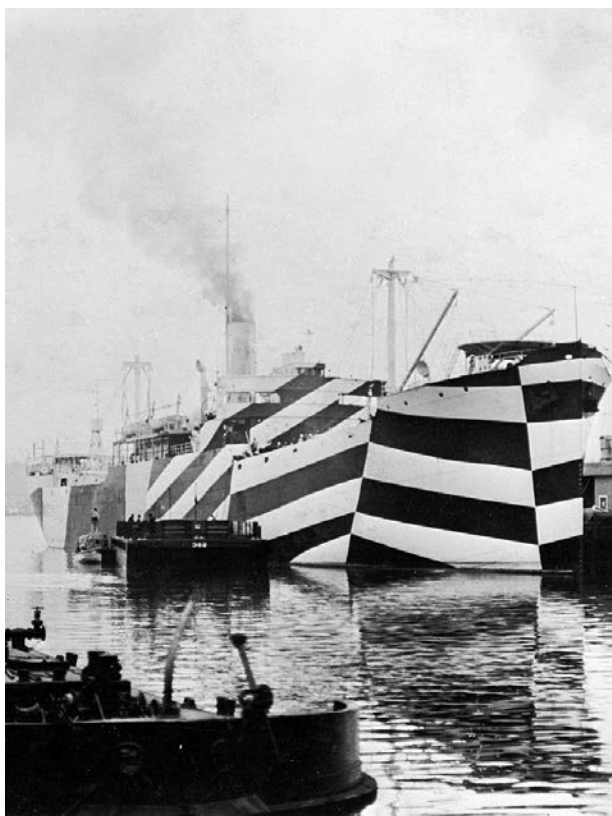


Figura 43. Barco de vapor *West Mahomet* con camuflaje disruptivo (1918). Fuente: Naval History & Heritage Command

Fue este desarrollo de los radares lo que provocó que, durante la Segunda Guerra Mundial, la aviación británica pusiese a prueba otra técnica. Impulsada por Joan Curran, única científica de la Telecommunications Research Establishment (la principal organización británica de I+D en materia de radionavegación, radar, detección de infrarrojos para misiles guiados por calor y trabajos relacionados) (Griffiths, 2020), esta técnica consistía en lo siguiente: durante un vuelo sobre espacio enemigo susceptible al rastreo mediante sus radares, los pilotos británicos lanzaban unos reflectores antirradar (conocidos como *chaff* en inglés), esto es, unas tiras de papel negro con una capa de aluminio en su parte posterior que, en grandes cantidades, quedaban flotando por el aire y generaban la falsa detección de muchos aviones, inhabilitando así la posibilidad de discernir cuál era el real.

Para Brunton y Nissenbaum (2015, p. 8), este ejemplo representa el más puro y simple enfoque de ofuscación: como el descubrimiento del avión real era inevitable (en ese momento no había una manera

de hacer que un avión fuera invisible al radar), los *chaff* buscaban agotar las limitaciones de tiempo y ancho de banda del sistema de descubrimiento al crear demasiados objetivos potenciales. El hecho de que tales *chaffs* funcionaran solo brevemente mientras revoloteaban hacia el suelo y no fueran una solución permanente no era relevante en esas circunstancias. Solo tenían que operar lo bastante bien y durante el tiempo suficiente para que el avión superara el alcance del radar.



Figura 44. Reflectores antirradar desplegados desde un bombardero de la RAF Lancaster.

Fuente: <https://ieeaeess.org/post/blog/history-column-chaff>

Una variante ya no bélica sino en favor de los derechos humanos la encontramos en la historia que recogen Brunton y Nissenbaum (2015, pp. 21-24) acerca de la ofuscación empleada por un grupo que buscaba liberar a Nelson Mandela de la prisión sudafricana durante la lucha contra el *apartheid*. La operación, llamada Operación Vula (abreviatura de *Vulindlela*, que significa Abrir el camino), fue ideada por los líderes del Congreso Nacional Africano (CNA) en Sudáfrica que estaban en contacto con Mandela y coordinaban sus esfuerzos con los de agentes, simpatizantes y generales del grupo en todo el mundo.

Brunton y Nissenbaum detallan que, para comprender el inicio y la aplicación de la ofuscación en la Operación Vula, es esencial analizar algunos de los desafíos que enfrentaron sus diseñadores. La opción de canalizar las comunicaciones del CNA empleando líneas telefónicas fijas en Sudáfrica, cada una asociada a un nombre y una dirección, no era viable, ya que cualquier filtración podría desembocar en escuchas telefónicas y lo que hoy se denominaría análisis de metadatos, permitiendo así articular un perfil de la red de activistas a partir de los registros de llamadas tanto nacionales como internacionales. Si bien los integrantes de Vula contaban con varios métodos de cifrado, éstos resultaban dificultosos

por la laboriosa y tediosa tarea de realizarlos manualmente, por lo que siempre existía la inclinación de “volver a susurrar por teléfono”, en especial durante las crisis cuando las acciones comenzaban a acelerarse. La operación necesitaba una coordinación impecable entre Sudáfrica, concretamente en Durban, Johannesburgo, Lusaka, Londres y Ámsterdam y así como otros lugares del mundo donde se movían los activistas del CNA. El correo era lento y susceptible de interceptarse, cifrar información requería un tiempo considerable y con frecuencia era propenso a fallos, el uso de teléfonos convencionales estaba prohibido y la coordinación entre distintas zonas horarias a nivel mundial parecía casi imposible.

Consciente de las posibilidades de utilizar ordenadores personales para hacer que el cifrado fuera más rápido y eficaz, el arquitecto principal de la Operación Vula, Tim Jenkin, trabajó en el sistema de comunicaciones necesario para superar todos esos obstáculos. El método consistía en un cifrado de mensajes que se realizaba en un ordenador personal y que luego se transformaba en una serie rápida de tonos grabados en un reproductor de casetes portátil. Un agente iba a un teléfono público y marcaba un número de Londres, donde respondía un contestador automático que Jenkin había modificado para que grabara durante un máximo de cinco minutos. Una vez activada dicha grabación, el agente en cuestión reproducía el casete en el micrófono del teléfono. Culminada la transmisión, al otro lado de la línea se reproducían los tonos grabados a través de un módem acústico en el ordenador para luego descifrarlos. De esta manera, los agentes de campo podían llamar desde un teléfono público, grabar los tonos de sus mensajes y descifrarlos en cualquier lugar en el que tuvieran acceso a un ordenador que pudiera ejecutar los sistemas de cifrado que Jenkin había ideado.

Aunque este método funcionaba bien, a medida que la Operación Vula seguía creciendo y la red de agentes se expandía, la gran cantidad de tráfico amenazaba con saturar la red. Ello, sumado a algunos problemas técnicos derivados del crecimiento de la operación, hizo que se plantease cambiar al correo electrónico cifrado, si bien el problema era que todo el sistema se había desarrollado para evitar el uso de líneas telefónicas reconocibles y propias dentro de Sudáfrica. La cuestión es que en los años en los que la red que Brunton y Nissenbaum (2015, p. 23) describen iba tomando forma, el entorno más amplio de los negocios internacionales estaba produciendo exactamente el tipo de trasfondo contra el cual este subterfugio podía ocultarse, pues cada día salían del país miles de mensajes y el grupo desconocía si existía un filtrado de ellos. Ante ello los activistas vieron que necesitaban un usuario típico de correo electrónico —uno sin una afiliación política clara— para averiguar si sus mensajes podían pasar desapercibidos en la marea general de correo.

Para probarlo utilizaron el perfil de un sudafricano nativo que regresaba a Sudáfrica tras trabajar como programador en el extranjero. Esta persona debía actuar como lo haría un ciudadano típico que envía muchos mensajes de correo electrónico todos los días, utilizando un proveedor de correo electrónico comercial en lugar de un servidor personalizado y confiando en el hecho de que muchas empresas utilizan cifrado en sus comunicaciones, aunque los autores no determinan si se trataba de cifrado “punto a punto” (de cliente a servidor) o “extremo a extremo” (de cliente a cliente, entre emisores y receptores sin que nadie por el camino pueda leer nada). El sistema funcionó: los mensajes del agente se mezclaron con el tráfico ordinario, proporcionando una plataforma para comunicaciones abiertamente secretas que podían expandirse rápidamente.

A través de una combinación de proveedores de correo electrónico comerciales y servicios de tablón de anuncios que funcionaban con ordenadores personales, los activistas del CNA pudieron hacer circular mensajes dentro de Sudáfrica y alrededor del mundo. La actividad cotidiana de usuarios ordinarios con direcciones comerciales anodinas se convirtió en un canal informativo de alto valor, moviendo enormes volúmenes de datos cifrados de Londres a Lukasa y luego a Sudáfrica, así como entre las células Vula en ese país. Para Brunton y Nissenbaum (2015, p. 25), el éxito de este sistema se produjo en parte gracias a ciertas circunstancias históricas: los ordenadores personales y el correo electrónico (incluido el correo electrónico cifrado) se habían vuelto lo suficientemente comunes como para no provocar sospechas, pero no tan comunes como para inspirar la construcción de nuevos sistemas de vigilancia digital más completos como los que tienen los gobiernos hoy. Por todo ello la red Vula ofrece un excelente ejemplo del papel que puede desempeñar la ofuscación en la construcción de un sistema de comunicaciones seguro y secreto.

Por último, aunque no se trate de un ejemplo humano, merece la pena citar el caso de la araña *Cyclosa mulmeinensis*. Tal y como cuentan Brunton y Nissenbaum (2015, p. 25), esta araña se enfrenta a un problema particular para el cual la ofuscación es una buena solución: su red debe quedar expuesta para atrapar a sus presas, lo que la hace mucho más vulnerable al ataque de su depredador natural, las avispas. La particular solución de esta araña es fabricar sustitutos de sí misma con restos de sus presas, maleza y seda de araña, que desde la perspectiva de una avispa tengan el mismo tamaño, color y reflectividad que la propia araña, y colocar estos señuelos alrededor de la red. Esto disminuye las probabilidades de que una avispa la ataque y le da tiempo a escapar, algo que en el siguiente apartado (y más específicamente en el 4.2.1) veremos que reviste una singular importancia en muchos otros contextos.



Figura 45. *Cyclosa mulmeinensis*. Fuente: <https://indiabiodiversity.org/species/show/275583>

4.2. Clasificación y casos

Para Brunton y Nissenbaum (2011, párr. 27), la ofuscación, como la extracción de datos, es una estrategia múltiple que se lleva a cabo tanto con una variedad de propósitos, como por diversos métodos y agentes. A su vez, estos agentes ofusadores pueden actuar en solitario o junto con otras personas, y ocultar solo cierta información o bien responder de manera tan exorbitada que su contribución sesgue todos los resultados de la recopilación. Se puede recurrir a la ofuscación por un simple deseo de defensa ante los peligros percibidos en la agregación de los datos personales o como respuesta ante las evidentes asimetrías de poder y saber. Igualmente debemos advertir que la ofuscación se puede emplear para ocultar actividades tanto legítimas como ilegítimas, incluso para causar un daño a un adversario, aunque en ocasiones lo que se busca es que el sistema de extracción de datos en su conjunto sea inútil. Esta diversidad de propósitos, métodos y agentes se refleja en la amplia gama de formas que adoptan las prácticas de ofuscación.

A partir de estas cuestiones, Brunton y Nissenbaum (2011, párr. 29-50) ofrecen una clasificación de diferentes tipos de ofuscación en torno a una serie de modalidades que, en la mayoría de ocasiones, podrían combinarse entre sí. De este modo, podría distinguirse la ofuscación dependiendo de si confía en las limitaciones temporales del adversario, requiere el “efecto red” de cooperación o colaboración por parte de grupos de ofusadores, interfiere selectivamente con los datos o hace que estos se vuelvan ambiguos y dudosos a largo plazo. Basándonos en esta relación podemos diferenciar cuatro tipos de ofuscación: ofuscación temporal, ofuscación cooperativa, ofuscación selectiva y ofuscación por ambigüación.

A continuación explicaré cada una de ellas y expondré algunos casos que emplean o se basan en estas prácticas. Pero antes de ello, considero importante recalcar de nuevo aquí que esta categorización no se basa en tipos estancos, puesto que dependiendo de si ponemos el foco en unas características o en otras, un ejemplo podríamos incluirlo en una o varias de las categorías presentadas. A su vez, los casos que cito a continuación no resultan un compendio de todos los existentes, puesto que esa tarea escapa en magnitud al fin de este trabajo, pero valen como una primera aproximación para mostrar la universalidad del hecho sin que exista una coordinación jerarquizada de este tipo de tácticas. Por último, bien por su relevancia, como son los ejemplos desarrollados por Helen Nissenbaum y sus colaboradores, bien por la obtención de la información de manera directa, como son los diversos proyectos creados tanto por Adam Harvey como por Martín Nadal, me detendré en explicar ciertos casos con mayor profundidad, mientras que otros serán presentados de una forma más esquemática.

4.2.1. Ofuscación temporal

Frente a las citadas formas de ofuscación que intentan inyectar desconfianza en los datos recopilados de forma permanente, la ofuscación basada en limitaciones temporales (en muchos sentidos, la forma más simple de táctica de ofuscación) agrega una cantidad extra de información para dilatar el procesamiento en una situación donde el tiempo resulta esencial (Brunton y Nissenbaum, 2011, párr. 30).

Ejemplos de este tipo de ofuscación los encontramos en los citados ejemplos del camuflaje disruptivo de los buques de guerra británicos (y también después estadounidenses) durante la Primera Guerra Mundial, así como en la dispersión de reflectores por parte de los aviones británicos durante la Segunda Guerra Mundial para confundir a los radares alemanes cuando sobrevolaban su espacio aéreo. En ambos casos, era inevitable que el enemigo detectase el tránsito de las naves, por lo que estas tácticas buscaban simplemente ganar el mayor tiempo posible para poder ponerse fuera del alcance de las defensas enemigas. En los también citados ejemplos de la araña *Cyclosa mulmeinensis*, así como en la historia relatada sobre el robo de Craigslist, el tiempo también desempeñaba un papel crucial en la facilitación de la escapatoria de una situación amenazante.

Además de éstas, existen otras circunstancias en las que emplear prácticas de ofuscación resulta de ayuda cuando el tiempo es una cuestión crucial. Buena prueba de ello lo ofrece la técnica financiera del HFT (*high frequency trading*, negociación de alta frecuencia) que, según Brunton y Nissenbaum (2015, p. 27), consiste en el empleo dentro de la compraventa bursátil de algoritmos que realizan grandes volúmenes de operaciones mucho más rápido de lo que podrían hacerlo los humanos. En efecto, en este tipo de negociación automatizada tan solo unas milésimas de segundo separan las ganancias de las pérdidas, y han surgido estrategias complejas para acelerar sus operaciones y retrasar las de sus competidores:

Los analistas del comportamiento del mercado comenzaron a notar patrones inusuales de actividad HFT durante el verano de 2010: ráfagas de solicitudes de cotización para una acción en particular, a veces miles de ellas en un segundo. Tal actividad parecía no tener una lógica económica, pero una de las teorías más interesantes y plausibles es que estas ráfagas son una táctica de ofuscación. Un observador explica el fenómeno de esta manera: “Si usted puede generar una gran cantidad de cotizaciones que sus competidores tienen que procesar, pero usted puede ignorarlas porque las generó usted mismo, gana un tiempo de procesamiento valioso” (Brunton y Nissenbaum, 2015, p. 27).

Otro caso lo encontramos en los momentos donde conviene camuflar ante otros una respuesta gestual

para la que se dispone de poco tiempo, como ocurre en las partidas de póker. Brunton y Nissenbaum (2015, p. 11) señalan estas prácticas por las que los jugadores gesticulan o se comportan de maneras que confundan a sus oponentes sobre si cuentan con una buena mano o van de farol como tácticas de ofuscación con limitaciones temporales.

Y si en este juego de cartas la táctica consiste en engañar al oponente literalmente en un abrir y cerrar de ojos, Brunton y Nissenbaum (2015, p. 17) argumentan que la sobreproducción de documentos también se puede entender como una forma de ofuscación, como ocurre en los casos de divulgación excesiva de material en un proceso judicial:

En situaciones en las que uno no puede decir No, hay oportunidades para un coro de Síes inútiles; por ejemplo, no envíe una carpeta en respuesta a una solicitud, envíe un palé de cajas de carpetas que contengan documentos potencialmente relevantes (Brunton y Nissenbaum, 2015, p. 18).

Al comienzo de este capítulo me referí a la acepción de ofuscación más conocida, la del código informático. En ella, ingenieros y programadores asumen que sus aplicaciones serán visibles por humanos o algoritmos de desensamblaje (ingeniería inversa) que buscan grietas para copiarlos o atacarlos y, en respuesta, ofuscan su código con capas extra de complejidad que multiplican el coste temporal de intentarlo (Brunton y Nissenbaum, 2015, pp. 33-34).

Por último, quisiera destacar aquí dos proyectos artísticos llevados a cabo, respectivamente, por Adam Harvey y por un grupo de estudiantes de la Universidad de Artes de Utrecht:

El primero se titula *Camoflash*⁴⁹ y es una de las primeras obras del artista visual Adam Harvey, a cuyo trabajo sobre tecnologías de visión por computación, privacidad y vigilancia aludí en la sección 1.4.1. Pensado para frustrar preventivamente los ataques de los *paparazzi* o cualquiera que pueda tomarte una foto sin consentimiento con una cámara réflex con *flash*, este dispositivo materializa el concepto de ofuscación de “deslumbrar” al que apuntaba en un principio. En efecto, se trata de un dispositivo LED de alta potencia que es capaz de detectar el *flash* de una cámara y, en menos de 0,1 milisegundos, activar un destello de 12000 lúmenes que sobreexpone el sensor del objetivo, frustrando el intento de captura de tu imagen.

49 Véase: <https://adam.harvey.studio/camoflash/>



Figura 46. Anti-Paparazzi Clutch Prototype. Fuente: <https://adam.harvey.studio/camoflash/>

Este proyecto comenzó como un prototipo conceptual enmarcado en el *Interactive Telecommunications Program* de la Universidad de Nueva York en 2008 y luego en 2010 se convirtió en un prototipo funcional capaz de frustrar los ataques de los *paparazzi* que empleaban réflex digitales en un radio de 3 metros. Aunque este producto alcanzó finalmente el nivel de prototipo funcional, lo cierto es que actualmente no está disponible debido a que no resultaba muy ergonómico y, sobre todo, a que las pruebas que el autor realizó para comprobar si la intensidad de la luz era suficiente para bloquear las cámaras réflex digitales profesionales mostraron que también lo era para causar un daño ocular temporal.

En cuanto al segundo proyecto artístico, se trata de la obra de cinco estudiantes holandeses de diseño de productos, Jing-Cai Liu, Sanne Weekers, Joppe Besseling, Jip van Leeuwenstein y Marcel Coufreur. En 2017 estos alumnos de la Escuela de Artes de Utrecht diseñaron algunas piezas conceptuales que tenían como objetivo mantener el anonimato en un mundo ficticio y futurista donde el reconocimiento facial fuese una cuestión (aún más) importante. En concreto, el concepto de “*wearable face projector*” de Jing-cai Liu, consiste en un dispositivo *prêt-à-porter* que, a través de la instalación de un pequeño

proyector que transforma la apariencia del rostro, dotándolo de un aspecto completamente nuevo. La iniciativa fue presentada en la Semana del Diseño de Milán de 2017, la *Design Gallery Utrecht* en 2017, la *DDW*, *Robot Love* de 2018, el evento *Bring Your Own Beamer* de Gante en 2019 y la muestra *Colectiva*, *AWA Cultura* de 2020 (Jing-Cai Liu, s.f., párr. 3).



Figura 47. *Wearable face projector* de Jing-Cai Liu. Fuente: <https://jingcailiu.com/wearable-face-projector/>

Este proyecto artístico fue protagonista de una controversia en 2019, cuando se extendió la falsa idea de que la obra de Jing-Cai Liu se estaba utilizando en el contexto de las protestas democráticas de Hong Kong, donde la decisión de las autoridades chinas de prohibir a los manifestantes ocultar su rostro les empujó a buscar formas alternativas de anonimato (Felton, 2019). Ante ello, en octubre de 2019 se añadió a la descripción del vídeo sobre el proyecto colgado en YouTube (Marcel Coufreur-Blaauwendraad, 2017, párr. 3), la siguiente declaración:

Jing-Cai Liu y los demás miembros del proyecto de diseño quieren dejar claro que no han tenido intenciones políticas con sus obras, ni entonces ni ahora. También quieren dejar claro que la mayoría de las obras son conceptos que no funcionan y que no tienen ningún interés en fabricar esos productos. Los derechos de autor del producto/concepto siguen en manos de esos diseñadores. Se ruega que se coloquen sus obras en el contexto adecuado y que siempre se haga referencia a sus sitios *web* o a las fuentes mencionadas anteriormente cuando se compartan sus conceptos. No se deben utilizar sus obras en ninguna declaración política.

4.2.2. Ofuscación cooperativa

Como comentaba anteriormente, las tácticas de ofuscación se pueden llevar a cabo de manera satisfactoria con la intervención de un solo actor, pero otras formas de ofuscación requieren de la

cooperación para su correcto funcionamiento, apelando al “efecto red” para volverse más valiosas y efectivas a medida que más personas se suman a ella (Brunton y Nissenbaum, 2011, párr. 36).

En este caso, a los ejemplos de “¡Yo soy Espartaco!”, Fuenteovejuna, la Operación Vula y el resto de referencias literarias y cinematográficas citadas, debemos sumar otros como el intercambio de tarjetas de fidelidad de los supermercados que comenté en el apartado 2.5.2. En la misma línea, Brunton y Nissenbaum (2015, pp. 18-19) citan el intercambio de tarjetas SIM, una táctica utilizada para evitar que analistas de la Agencia de Seguridad Nacional estadounidense (NSA) utilicen los metadatos de geolocalización de teléfonos móviles para identificar y rastrear objetivos, dado que con ellos pueden crear un modelo de red social que ayuda a localizar a personas sospechosas, ubicarlas e incluso asesinarlas sin un contacto visual directo. Ante ello, quienes están en el punto de mira se protegen mediante tácticas para confundir las señales, como compartir tarjetas SIM aleatoriamente con otros compañeros e incluso con amigos y familiares, lo que complica el rastreo, aunque esto también puede tener el fatídico resultado del asesinato de estas personas interpuestas.

Brunton y Nissenbaum (2015, pp. 29-30) rescatan también dentro de esta categoría el caso de *BitTorrent Hydra*, un proyecto que se opuso a la vigilancia por parte de aquellas industrias culturales que quieren perseguir la compartición de archivos mediante redes P2P (*peer-to-peer*, entre pares) en Internet. Partiendo de la base de que, como es sabido, el protocolo BitTorrent permite dividir un archivo en fragmentos pequeños que se comparten entre usuarios, de modo que, en lugar de descargar un archivo completo, se ensambla usando fragmentos de dispositivos pertenecientes a diferentes personas, este proyecto mezcla solicitudes reales de fragmentos de archivos por parte de pares con otras falsas. Dado que los “rastreadores de torrents” ayudan a los usuarios a encontrar las direcciones IP que albergan los fragmentos deseados, los representantes de la industria de los monopolios intelectuales usan también estos rastreadores para identificar a quienes comparten archivos sin autorización y amenazarles o incluso actuar contra ellos (sobre todo en EEUU). Pues bien, *Hydra* respondía a esto agregando direcciones IP aleatorias a las recopiladas por los rastreadores, lo que dificultaba la identificación de los usuarios reales e introducía incertidumbres en todo el sistema de seguimiento. En definitiva, este método de ofuscación cooperativa no pretende ocultar el tráfico en redes P2P basadas en Torrent, sino deteriorar la fiabilidad de los datos emanados de él, cuestionando así los hallazgos específicos de los que perseguían supuestas violaciones de derechos de autor.

Otro ejemplo lo encontramos en la criptografía, que cuya protección de la información a través del uso de cifrado puede entenderse estrictamente como una ofuscación de datos (y metadatos), que se esconden entre capas de ruido matemático. Este tipo de movimientos representa una estrategia de

ofuscación colectiva, puesto que la criptografía se vuelve más efectiva cuanto más la usamos los ciudadanos con normalidad, ya que complica a los gobiernos y corporaciones proclives a la vigilancia digital la tarea de identificar los intercambios triviales de aquellos otros verdaderamente relevantes o perseguidos. Lo mismo sucede con *Tor*, el sistema de encaminamiento de cebolla «cuya función de desagregación y camuflaje criptográficos de la identidad y actividad del tráfico *web* se vuelve más rápida y segura cuanta más gente lo adopta, más aún si entre ellas surgen nuevos nodos de salida de la red» (Cabello y Solera, 2020, p. 343).

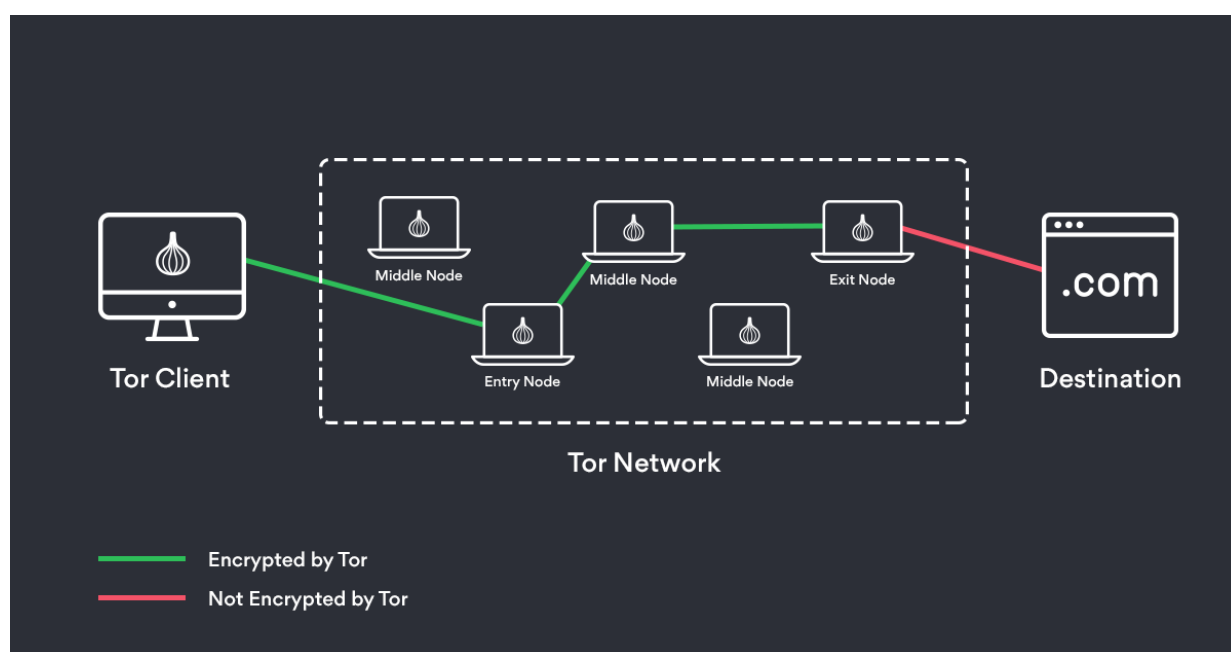


Figura 48. Representación gráfica de los nodos de *Tor*.

Fuente: <https://hackpuntos.com/torghost-reenvia-todo-el-trafico-a-la-red-tor/>

De manera similar opera la organización mediática sin ánimo de lucro Wikileaks, que tal y como relatan Brunton y Nissenbaum (2015, pp. 14-15) usó desde el principio diferentes sistemas para proteger la identidad de sus visitantes y colaboradores. Sin embargo, Wikileaks era muy consciente que en su operativa habitual persistía un riesgo insoslayable vinculado a las subidas de archivos por parte de los alertadores (*whistleblowers* en inglés) que se los confiaban para revisarlos, verificarlos y, ulteriormente, difundirlos. La cuestión radicaba en que si las agencias de seguridad que les tenían en su punto de mira escrutaban a fondo el tráfico en la página *web* de Wikileaks, podrían identificar cuándo, cómo y desde qué dispositivo y conexión se enviaba a su buzón seguro las filtraciones de archivos comprometedores. Ante este riesgo, desde la organización crearon una secuencia de comandos (un *script* en inglés) que generaba señales falsas de subida de archivos en los navegadores de los visitantes de la *web* de Wikileaks, haciendo que pareciera que había muchas personas filtrando información, cuando en realidad la

mayoría solo leía documentos disponibles. Aunque los datos cifrados aún tienen metadatos, Brunton y Nissenbaum (2015, p. 15) rescatan *OpenLeaks*, una versión fallida de WikiLeaks, que propuso un modelo de cargas falsas que imitaba las proporciones de tamaños de archivos comunes en el tráfico de un sitio de filtraciones.

Por último, dentro de esta categoría citaré el proyecto artístico *Facial Weaponization Suite* de Zach Blas, artista, cineasta y escritor cuya práctica abarca la imagen en movimiento, la computación, la teoría, la *performance* y la ciencia ficción. Elaborado entre 2012 y 2014, esta iniciativa nació con la intención de protestar contra el reconocimiento facial biométrico (y las desigualdades que estas tecnologías propagan) mediante talleres de creación de “máscaras colectivas” que se modelan a partir de los datos faciales agregados de los participantes. Como resultado de estos talleres, Blas (s.f., párr. 1) lograba generar unas máscaras amorfas que no podían detectarse como rostros humanos mediante tecnologías de reconocimiento facial biométrico.



Figura 49. Imágenes del proyecto *Facial Weaponization Suite* de Zach Blas. Fuente: <https://zachblas.info/works/facial-weaponization-suite/>

4.2.3. Ofuscación selectiva

Los ejemplos descritos hasta ahora se refieren a métodos generales para ocultar toda la información, pero los autores de esta categorización se plantean una pregunta muy aguda: ¿qué ocurre si se desea que estos datos sean útiles sin menoscabar la privacidad, o si se desea que interfieran con algunos métodos de análisis de datos pero no con otros? (Brunton y Nissenbaum, 2011, párr. 41). Hablamos entonces de tácticas de ofuscación selectiva.

En 2009, el equipo de Urs Hengartner, profesor de la Universidad de Waterloo, desarrolló una extensión para el navegador libre Firefox denominada *FaceCloak*. Se trataba de una arquitectura que buscaba reforzar la privacidad de los usuarios de Facebook al proteger la información personal que ellos eligieran tanto del propio sitio como de otros usuarios que no hubiesen sido autorizados explícitamente por ellos, todo ello sin percibir modificaciones de los servicios o la interfaz de la red social. Aunque este proyecto estaba orientado a su implementación en la plataforma de Facebook, sus desarrolladores no descartaban incluso extrapolarlo a otras redes sociales (Luo *et al.*, 2009, p. 26).

FaceCloak llevaba a cabo la protección de la privacidad en tres fases: configuración, cifrado y descifrado (Luo *et al.*, 2009, p. 28). Al configurar *FaceCloak* en tu navegador, éste generaba varias claves para distribuir entre aquellos con los que querías compartir tu información real, con la posibilidad adicional de configurar un servidor de terceros, que se utilizaba para almacenar y recuperar la información personal cifrada del usuario. En la fase de cifrado, *FaceCloak* te guiaba para cifrar la información publicada y enviarla al servidor de terceros a través de una conexión protegida por TLS, lo cual garantizaba que cualquier información que quisieses ocultar del sitio y de los usuarios no autorizados no se enviara a Facebook, al tiempo que se transmitía información falsa al sitio. La fase de descifrado se producía cuando la persona propietaria de una cuenta u otra persona autorizada deseaba ver la información real publicada. El visor de contenido descifraba la información real obtenida del servidor de terceros a través de una conexión protegida por TLS y la utilizaba para reemplazar la información falsa obtenida de Facebook. Esta fase garantizaba que los servicios ofrecidos por el sitio siguiesen funcionando correctamente a pesar de la intervención de *FaceCloak*. Este proyecto estuvo vigente hasta 2011, cuando debido a los cambios realizados por Facebook en su sitio *web*, dejó de funcionar correctamente⁵⁰.

⁵⁰ Véase: <https://crysp.uwaterloo.ca/software/facecloak/download.html>

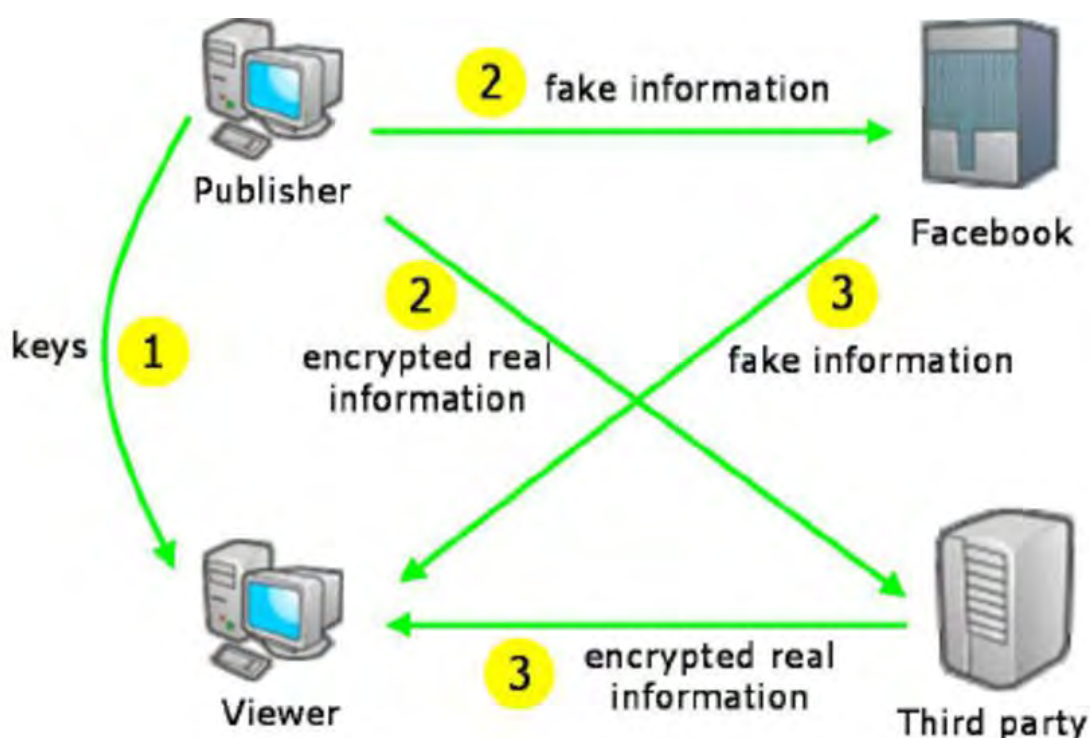


Figura 50. Arquitectura de FaceCloak. Fuente: Wanying *et al.*, 2009, p. 28

El siguiente proyecto del que quiero hablar lo presentó el doctor Paul Ashley, director de tecnología de Anonymome Labs⁵¹ en el Congreso sobre Ofuscación organizado por Brunton y Nissenbaum en 2017, y lleva por título *Sudo App*, en alusión al clásico programa de los sistemas operativos tipo UNIX *sudo* (acrónimo de *super user do*), que permite a cualquiera ejecutar acciones con los permisos de otro usuario, especialmente acceder a los privilegios de administración mediante una consola de superusuario (o *root*, en inglés). Este proyecto tiene como objetivo recuperar el control de nuestra identidad en línea, dándole a las personas las mismas libertades de expresión, creencias y experiencias que se supone ya disfrutaban *offline*. Para ello desarrollaron un avatar, “sudo”, que realiza interacciones en línea como comprar, vender, realizar búsquedas o socializar en nombre del usuario. De esta manera, Ashley (2017, p. 24) presenta *Sudo App* como una herramienta de comunicación basada en un protocolo de conocimiento cero (por el que una declaración puede verificarse sin revelar información sobre su contenido) para gestionar llamadas, mensajes de texto y correos electrónicos con otras personas. De este modo, para proteger estas comunicaciones frente a quienes están fuera de los círculos sociales íntimos, *Sudo App* te da la opción de revelar tanto o tan poco de ella como quieras, mientras mantienes el acceso a todos los sitios y servicios en línea desde los dispositivos móviles u ordenadores.

⁵¹ Véase: <https://anonymome.com/>

Dentro de esta categoría encontramos también multitud de proyectos orientados a generar un discurso crítico en torno a la desmesurada implantación de cámaras de video-vigilancia en los espacios públicos, sumada a los potenciales riesgos de combinarlas con herramientas de identificación facial o biométrica, así como a la tendencia a delegar la responsabilidad en sus algoritmos en detrimento de la intervención humana. En dichos proyectos hallamos una combinación de prendas de vestir, maquillaje y peinados a la que Lyon (2018, p. 42) denomina como *glamouflage* (combinando el concepto de camuflaje al del *glamour*). Aunque ya he presentado otros ejemplos encuadrables bajo este término, como el *Facial Weaponization Suite* de Zach Blas o el *Wearable face protector* de Jing-cai Liu, a continuación, veremos otros casos que también ilustran de modo singular cómo nuestro propio cuerpo puede funcionar como arma para ofuscar los sistemas de vigilancia digital.

En esta variante quisiera destacar en primer lugar una serie de proyectos realizados por el citado Adam Harvey en torno a diferentes formas de usar la moda, el maquillaje o el peinado para camuflar nuestro rostro y/o cuerpo frente a dispositivos de reconocimiento facial o biométrico. Este artista e ingeniero afincado en Berlín tomó consciencia de los riesgos que suponía la vigilancia mediada por la tecnología digital a través de su propia experiencia como fotógrafo en Nueva York entre 2004 y 2008:

Si dejas de lado la fotografía y piensas en el proceso técnico de lo que está sucediendo, la fotografía no es diferente de la vigilancia. Quiero decir, es la forma de arte de la vigilancia, en muchos casos, no en todos, pero en muchos casos.

Y me di cuenta de que ¿qué era esta cosa en mi mano? ¿En qué me había convertido? Me miré al espejo y era un actor de la vigilancia, grababa a la gente y cada foto que tomaba era una prueba. Trabajé en un periódico escolar y las fotografías que tomamos fueron citadas por la policía local. Y pensé: “Bueno, no quiero crear pruebas, quiero hacer arte”. Y si la fotografía es crear pruebas, no quiero hacer fotografía, quiero hacer otra cosa. Y, de hecho, lo que quería hacer era *antifotografía* (Harvey, comunicación personal, 14 de noviembre del 2023).

A raíz de esto, y gracias a su formación previa en ingeniería mecánica y física, Harvey (citado en Herrmann, 2017, párr. 19) decidió abordar la privacidad y la contravigilancia desde una perspectiva mucho más técnica durante sus estudios en el máster: *Interactive Telecommunications Program* de la Universidad de Nueva York. Y así es como nace su primer proyecto, *CV Daz  le*⁵², abreviatura de *Computer Vision Daz  le*, una forma de camuflaje de visión artificial que, a diferencia del camuflaje

⁵² Véase: <https://adam.harvey.studio/cvdaz  le/>

tradicional, está diseñado para romper los sistemas de visión artificial sin dejar de ser perceptible para otras personas. Inspirado en la anteriormente comentada técnica de camuflaje de los barcos de la Primera Guerra Mundial (*daẓẓle*), estamos ni más ni menos que ante la primera técnica de camuflaje documentada que atacaba con éxito un algoritmo de visión artificial.

El objetivo de *CV Daẓẓle* era mitigar bajo el disfraz de la moda los riesgos de la captura y el análisis de información visual computacional y estaba motivado por la necesidad de recuperar la privacidad en un mundo de mayor vigilancia visual y recopilación de datos:

Entonces, el proyecto trata de cómo hacer que la fotografía sea más divertida. Es una especie de juego de busca y captura, y necesitamos darle poder e innovar en tecnología o métodos para que las personas que están siendo fotografiadas se comuniquen de otra manera. Entonces, veamos, el proyecto *CV Daẓẓle*, por más que parezca que trata sobre peinados, trata sobre comunicación y diálogo, sobre camuflaje, el proyecto es un proyecto de camuflaje y trata de poder modular la información que se intercambia. Si las personas tienen cámaras que se están volviendo más potentes, ¿qué información se está entregando? ¿Y cómo se controla esa información? Ese es el arte del camuflaje. Entonces, el proyecto consistía en inventar una nueva forma de camuflaje y era la primera vez que alguien había descifrado un algoritmo de visión artificial. [...] La idea era crear una ilusión óptica y con este proyecto, el sistema de visión artificial *Daẓẓle* creó una especie de ilusión algorítmica. Y funcionó, así que fue la primera vez que se derrotó a cualquier sistema de visión artificial, a computadoras y algoritmos (Harvey, comunicación personal, 14 de noviembre del 2023).

Para captar mejor la trascendencia de esta pionera derrota a la que alude Harvey, conviene precisar que las técnicas de generación de patrones llamativos que Harvey desplegó para separar las características esperadas de los perfiles de detección de rostros iban dirigidas a romper el algoritmo de detección de rostros Viola-Jones⁵³. Hablamos del que hasta hace una década era el único algoritmo de detección de rostros, por lo que *CV Daẓẓle* creaba un agujero en toda esta rama de la industria de vigilancia al lograr que no funcionase. Finalmente este algoritmo acabaría por volverse obsoleto en materia de seguridad alrededor de 2013-2016 y ya no se utiliza, por lo que los contra-patrones originales (diseñados por Harvey entre 2010 y 2013) tampoco funcionan ya, pero hasta entonces una tecnología clave en el aparato de seguridad que parecía infalible después del 11 de septiembre podía verse frustrada por culpa de emplear una serie de técnicas del maquillaje y peinado.

⁵³ Véase: https://en.wikipedia.org/wiki/Viola%E2%80%93Jones_object_detection_framework

Más concretamente, los diseños iniciales de *CV Dazzle* funcionaban modificando las áreas oscuras y claras de un rostro (u objeto) según las vulnerabilidades de un algoritmo de visión artificial concreto. Pero debemos tener en cuenta que *CV Dazzle* no es un diseño o patrón específico, sino más bien una estrategia de camuflaje para evadir los sistemas de visión computacional que evoluciona, como lo hace el camuflaje, junto con la tecnología que pretende subvertir.

El primer diseño de *CV Dazzle* (Figura 51) se creó en 2010 como prueba de concepto para su trabajo fin de máster. Los diferentes *looks* se crearon posteriormente en colaboración con *DIS Magazine*⁵⁴ (Figura 52) y para un encargo del *New York Times* (Figura 53) con el objetivo de investigar el potencial de un estilo que fuera funcional pero que aún se mantuviera dentro de los márgenes de la moda conceptual.



Figura 51. Aspecto original *CV Dazzle* para su exposición en el máster de la Universidad de Nueva York.

Fuente: <https://adam.harvey.studio/cvdazzle/>

Figura 52. *CV Dazzle* Look para *DIS Magazine*

Fuente: <https://adam.harvey.studio/cvdazzle/>

⁵⁴ Véase: <https://dismagazine.com/>

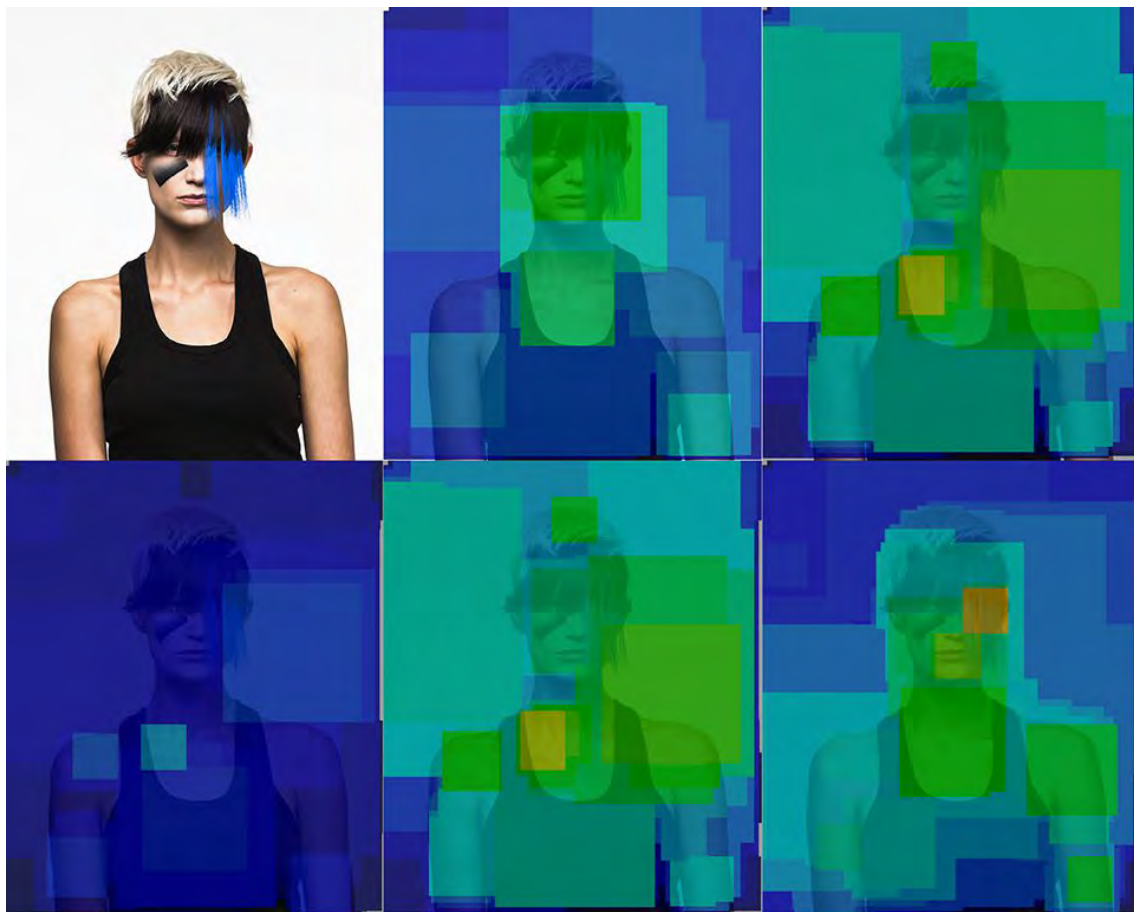


Figura 53. Evaluación de prominencia de la sesión fotográfica *Op-Art* del *New York Times*.

Fuente: <https://adam.harvey.studio/cvdazzle/>

Desde la publicación de *CV Dazzle* hubo una respuesta muy positiva al proyecto, y diversos grupos activistas y artísticos realizaron talleres para explorar y exponer las vulnerabilidades de los sistemas de reconocimiento biométrico. En nuestra entrevista, Harvey realizaba la siguiente valoración a este respecto:

Y ahora creo que la declaración ya está hecha. Y mucha otra gente ha trabajado de cosas similares. Así que el arte del proyecto no consistía en cambiar la percepción, cambiar de paradigma o cambiar la forma en que la gente piensa sobre el reconocimiento facial. Esto fue en 2010 y la gente todavía hoy no entiende lo que está pasando, a veces tiene miedo de interactuar con la tecnología. ¿Cuáles son las partes más geniales de eso? Ha inspirado a mucha gente, [...] Y, ya sea que lo hayan hecho o no, la parte importante es que las personas están investigando la tecnología y al hacerlo pueden encontrar una debilidad. [...] Para entender los algoritmos, tienes que concentrarte, permanecer cerca. Y luego descubres qué funciona y qué no, y luego puedes interactuar con ellos, ¿sabes? Los algoritmos están

diseñados para que interactúes con ellos de cierta manera, pero para interactuar con ellos tienes que encontrar las vulnerabilidades y luego puedes ser más humano en lugar de adoptar un posicionamiento más dictatorial (Harvey, comunicación personal, 14 de noviembre del 2023).

Basado en el trabajo anterior, durante el otoño de 2012 Harvey estuvo trabajando en un nuevo proyecto denominado *Stealth Wear*⁵⁵ (traducible como ropa furtiva), el cual fue presentado por primera vez en la sede de la revista *Tank*⁵⁶ en Londres el 17 de enero de 2013. Con este proyecto, continuó explorando formas estéticas de protección individual de la privacidad junto con el potencial de la moda para desafiar las tecnologías de vigilancia autoritarias, pero esta vez a través de la vestimenta y cómo con ella se podía eludir la detección por parte de las cámaras térmicas que llevan integradas algunos drones.

En concreto, Harvey realizó una colección de prendas inspiradas en la vestimenta islámica tradicional (*burka*, *hijab*, aunque también diseñó sudaderas con capucha), fabricadas con un tejido sintético bañado en plata muy flexible y termorreflexivo. De esta manera, las fibras bañadas en este metal reflejan y difunden la radiación térmica emitida por un cuerpo, lo que reduce la huella térmica del que la porta bajo la observación de una cámara infrarroja de onda larga (LWIR), por ejemplo, una cámara FLIR.

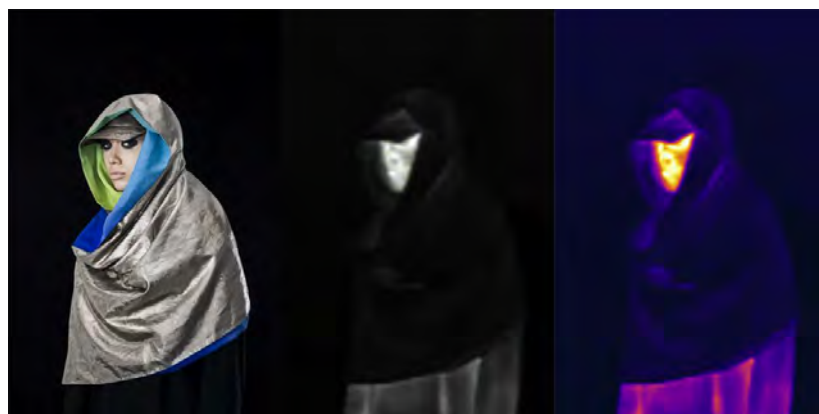


Figura 54. Anti-Drone Hijab, pieza de la colección Stealth Wear. Fuente: <https://adam.harvey.studio/stealth-wear/>

Aunque Harvey puso a la venta alguno de estos modelos a través de una tienda *online* denominada *Privacy Gift Shop*⁵⁷, desarrollada junto con un estudio de investigación y diseño con sede en Nueva York denominado *Undisclosed LLC*, la base de clientes que tuvo era «de nicho y de moda» (Harvey, citado en Priest, 2013, párr. 25). En esa misma entrevista de 2013, el artista explicaba que, lejos de los números de

⁵⁵ Véase: <https://adam.harvey.studio/stealth-wear/>

⁵⁶ Véase: <https://tank.tv/magazine>

⁵⁷ Véase: <https://privacygiftshop.com/>

ventas, lo que más le interesaba eran las conversaciones que estas prendas generaban.

En este sentido, el proyecto logró exponerse en centros como la Galería Marta Hergord en Alemania, la Galería Boghossian en Bruselas, el Museo de Arte Contemporáneo de Utah o la Escuela del Museo de Bellas Artes de la Universidad de Tufts en Boston. Igualmente recibió una cobertura mediática por parte de medios como *The New York Times*, el *Washington Post*, la revista *Wired* o el periódico alemán *Spiegel*; e incluso llegó a ser mencionado en un tuit de la cuenta de la Fuerza Aérea en el Pentágono⁵⁸.

El último proyecto de Adam Harvey que presento dentro de esta categoría de ofuscación es *HyperFace*⁵⁹. Se trata de un tipo de camuflaje que tiene como objetivo reducir el grado de confianza en la detección y el reconocimiento facial al proporcionar caras falsas que confunden a los algoritmos de reconocimiento facial. El desarrollo de *HyperFace* comenzó en 2013 y se presentó por primera vez en el *Chaos Communication Congress (33c3)*⁶⁰ de Hamburgo (Alemania) el 30 de diciembre de 2016. Posteriormente, su primera versión se desarrolló en el marco del *Festival de Cine de Sundance* de 2017 dentro del proyecto *NeuroSpeculative AfroFeminism* que promovían los miembros *Hyphen Labs*⁶¹ Ashley Baccus-Clark, Carmen Aguilar y Wedge, Ece Tankal, Nitzan Bartov y JB Rubinovitz. El proyecto también fue presentado por Adam Harvey en el *Obfuscation Workshop* de 2017 organizado por Helen Nissenbaum y Ero Balsa (de Cornell Tech), junto con Seda Gürses (de TU Delft) y Jara Rocha (investigadora independiente a quien pude conocer en su etapa en el Medialab-Prado de Madrid)⁶².

Concebido técnicamente como una extensión de *CV Dazzle*, *HyperFace* funciona proporcionando rostros falsos basados en representaciones algorítmicas ideales de un rostro humano, dirigidos a algoritmos específicos.

58 Véase: <https://twitter.com/AirForceGC/status/351715936815939584>

59 Véase: <https://adam.harvey.studio/hyperface/>

60 Véase: https://events.ccc.de/congress/2016/wiki/Static:Main_Page

61 Véase: <https://hyphen-labs.com/>

62 Véase: <https://www.obfuscationworkshop.org/participants2017/>

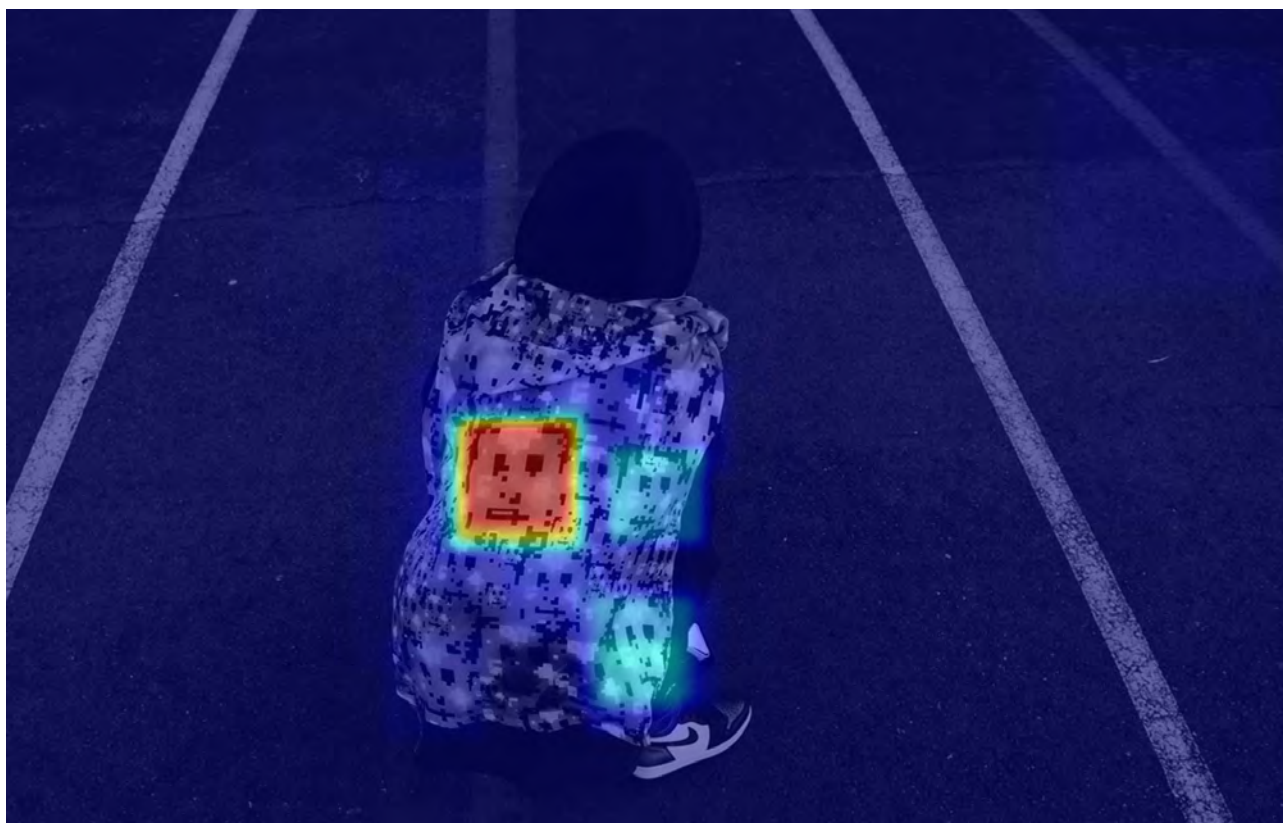


Figura 55. HyperFace de Adam Harvey para Hyphen-Labs. Fuente: <https://adam.harvey.studio/hyperface/>

Desde una perspectiva conceptual, con este proyecto Harvey reconoce que ocultar completamente un rostro a los algoritmos de detección facial sigue siendo un gran desafío técnico y estético. Ante ello, en lugar de buscar el anonimato mediante el camuflaje de una cara verdadera, como hacía con *CV Dazzle*, el artista plantea que *HyperFace* genere un ruido alrededor del rostro que impida al algoritmo de reconocimiento facial delimitar cuáles son los contornos verdaderos de la cara. En consecuencia, aunque *HyperFace* no te hace invisible ante estos mecanismos, actúa como un señuelo contra algoritmos de detección de rostros específicos.

Así pues, como estrategia de ofuscación, el objetivo principal de *HyperFace* es introducir ruido mostrando regiones de rostros falsos que, observados por humanos, no son perceptibles como tales. Como elemento de contravigilancia, *HyperFace* se puede utilizar como señuelo en combinación con *CV Dazzle* para permitir que el rostro verdadero del usuario quede oculto en el fondo de puntuaciones de rostros de mayor confianza.

Además de estos objetivos, con el proyecto *HyperFace* Harvey también pretendía involucrar al público en el diálogo sobre los posibles riesgos de la visión artificial mediante el uso de un enfoque no técnico y analógico. De este modo, al presentar sus artilugios como accesorios de moda el artista se proponía

volverlos accesibles a grupos fuera de las comunidades de investigación académica.

En esta misma línea destaco el proyecto de *Adversarial Fashion*⁶³, de la hacker y diseñadora de moda Kate Rose. Se trata de una iniciativa orientada a su denuncia del aumento de sistemas de video-vigilancia, así como al hecho de que multitud de ellos, aun pudiendo llegar a resultar útiles en determinadas circunstancias, no están bajo supervisión humana, abriendo con su acción un interesante debate al respecto. Para vehicular tal denuncia, Kate Rose recurre a la estampación de imágenes de matrículas de coches en la ropa que diseña, con el fin de confundir a los lectores automatizados, cosa que la autora destaca que no ocurriría si hubiese un humano detrás de esta supervisión (*Adversarial Fashion*, s.f.). Para finalizar, estimo importante enfatizar que este proyecto está realizado con *software* libre, por lo que está abierto a réplicas y adaptaciones, algo que la propia Rose incentiva explicando en su página *web* diversos recursos para el diseño textil DIY (*Do It Yourself*, Hazlo tú misma)⁶⁴.

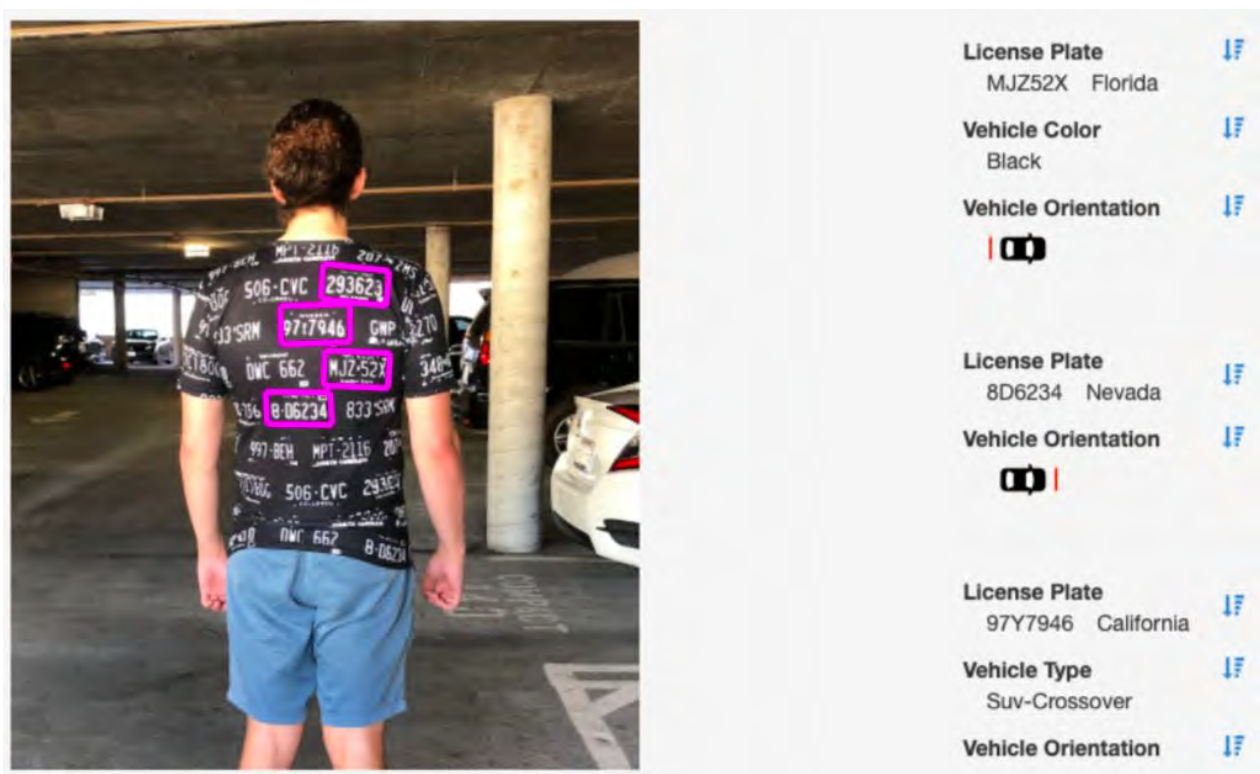


Figura 56. Ejemplo de cómo funciona *Adversarial Fashion* con un lector de matrículas.

Fuente: <https://adversarialfashion.com/pages/defcon-27-crypto-privacy-presentation>

Otro proyecto similar es el del diseñador suizo Simone C. Niquille, quien en 2013 desarrolló unas camisetas bajo el proyecto *Realface Glamouflage*, una investigación de diseño con carácter humorístico para contrarrestar las tendencias emergentes del ubicuo reconocimiento facial asistido por ordenador.

⁶³ Véase: <https://adversarialfashion.com>

⁶⁴ Véase: <https://adversarialfashion.com/pages/diy-resources>

Estas prendas de ropa están estampadas con rostros distorsionados de imitadores de celebridades y están diseñadas para que los algoritmos de Facebook los etiqueten de manera incorrecta (Niquille, 2013).



Figura 57. Ejemplo de cómo funciona *Realface Glamouflage*.

Fuente: <https://www.designforsustainability.studio/signals/realface-glamouflage>

Otra prenda de ropa que destacar aquí es el proyecto *CHBL Jammer Coat*, desarrollado por la cooperativa de arquitectos COOP HIMMELB(L)AU⁶⁵ para la exposición “*Abiti da lavoro*” que se llevó a cabo a finales de junio de 2014 bajo el comisariado de Alessandro Guerriero. El *CHBL Jammer Coat* es una prenda confeccionada con telas metalizadas que bloquean las ondas de radio y protegen al usuario contra dispositivos de seguimiento, evitando que se le pueda localizar a través de su teléfono móvil y capturar información de su tarjeta de crédito. El patrón *Wave Circle* de la tela crea una ilusión de múltiples partes extrañas del cuerpo, lo cual oculta también la morfología de quien lo porta (Architizer, s.f.).

⁶⁵ Juego de palabras intraducible entre “*bimmelblau*” y “*bimmelbau*”, respectivamente “azul celeste” y “construcción celestial” en alemán.



Figura 58. *CHBL Jammer Coat* desarrollado por los arquitectos de la firma COOP HIMMELB(L)AU.

Fuente: <https://svetlanavladimirova.tumblr.com/post/91759357467/chbl-jammer-coat-coat-of-the-future>

Ya alejado del concepto de *glamouflage*, encontramos en primer lugar el reciente proyecto del artista e ingeniero informático Martin Nadal, denominado *FangøCam*⁶⁶ y presentado en 2023. Enmarcado dentro de una residencia artística en el centro de datos artísticos y DIY de Graz (Austria) *Mur.at*⁶⁷, *FangøCam* supone una evolución conceptual de otro proyecto anterior suyo, *Fangø*, del cual hablaré más adelante.

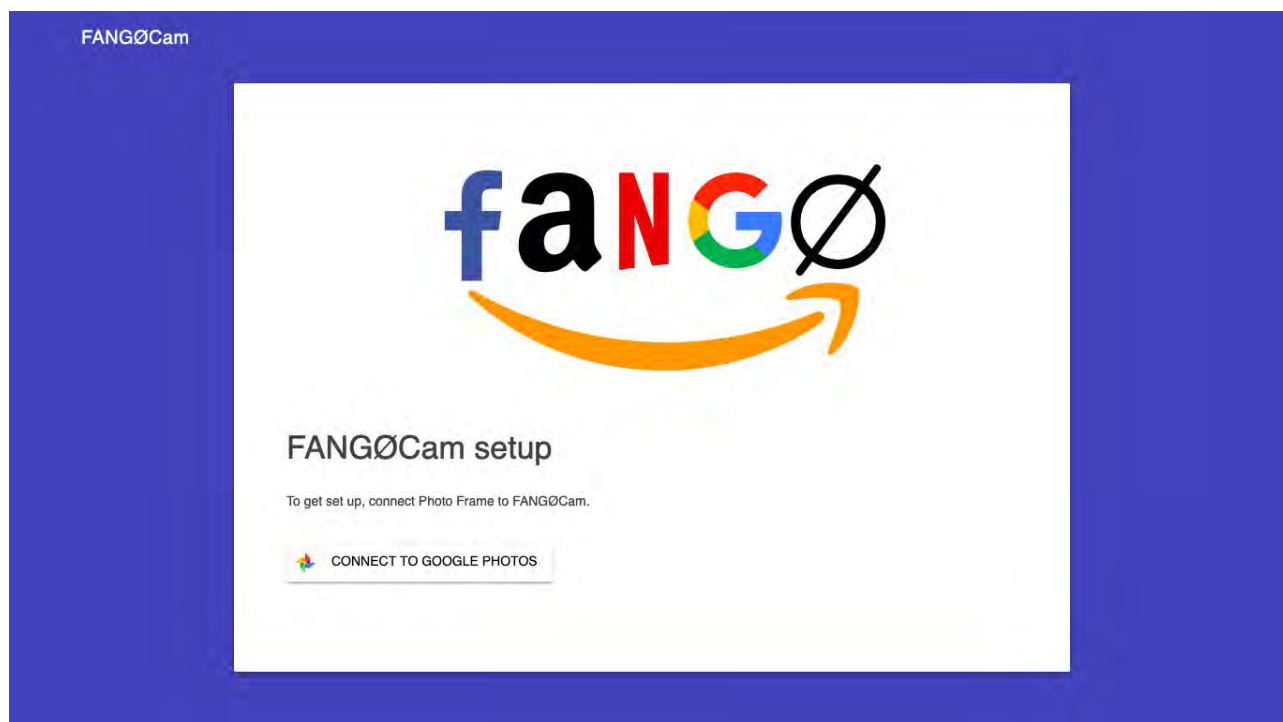


Figura 59. Captura de pantalla de la página de inicio de *FangøCam*. Recuperado el 5 de febrero de 2025.

FangøCam nace como respuesta a la acuciante problemática derivada del empleo de las fotografías que guardamos en la (mal) llamada “nube”, como Google Photos o Amazon Photos, para el entrenamiento de algoritmos de reconocimiento facial de estas corporaciones sin un claro consentimiento de sus usuarios (Monckton, 2024). Además, en el caso de Amazon su servicio serviría para entrenar Amazon

⁶⁶ Véase: <https://fangocam.muimota.net/>

⁶⁷ Véase: <https://mur.at/>

Rekognition, el cual es utilizado por una serie de agencias gubernamentales y departamentos de policía de EEUU (Das, 2017; Guliani, 2018), incluido el Servicio de Inmigración y Control de Aduanas (ICE, por sus siglas en inglés), que actualmente copa telediciarios y portadas por el propósito de la nueva presidencia de Donald Trump de convertirlo en punta de lanza de un (pretendidamente) masivo programa de deportaciones de migrantes.

La característica principal del proyecto, pensado para ser una aplicación de cámara para móviles pero actualmente desarrollado como un servicio *web*, es que las imágenes capturadas con *FangøCam* se ofuscan haciéndolas irreconocibles y sin ningún valor para las compañías citadas, que de esta forma no pueden utilizarlas para entrenar sus sistemas de reconocimiento. Este proceso de ofuscación, que materializa la aspiración de Harvey a una “antifotografía” citada al comienzo de esta sección, se revela como plenamente selectivo en la medida en que es reversible para los usuarios de *FangøCam*, que siempre pueden acceder a las fotos en su formato original. De esta manera, con su proyecto Nadal pretende impedir la extracción de valor de nuestra galería de imágenes y parasitar los archivos e infraestructuras de estas empresas (Nadal, comunicación personal, 14 de noviembre del 2023).

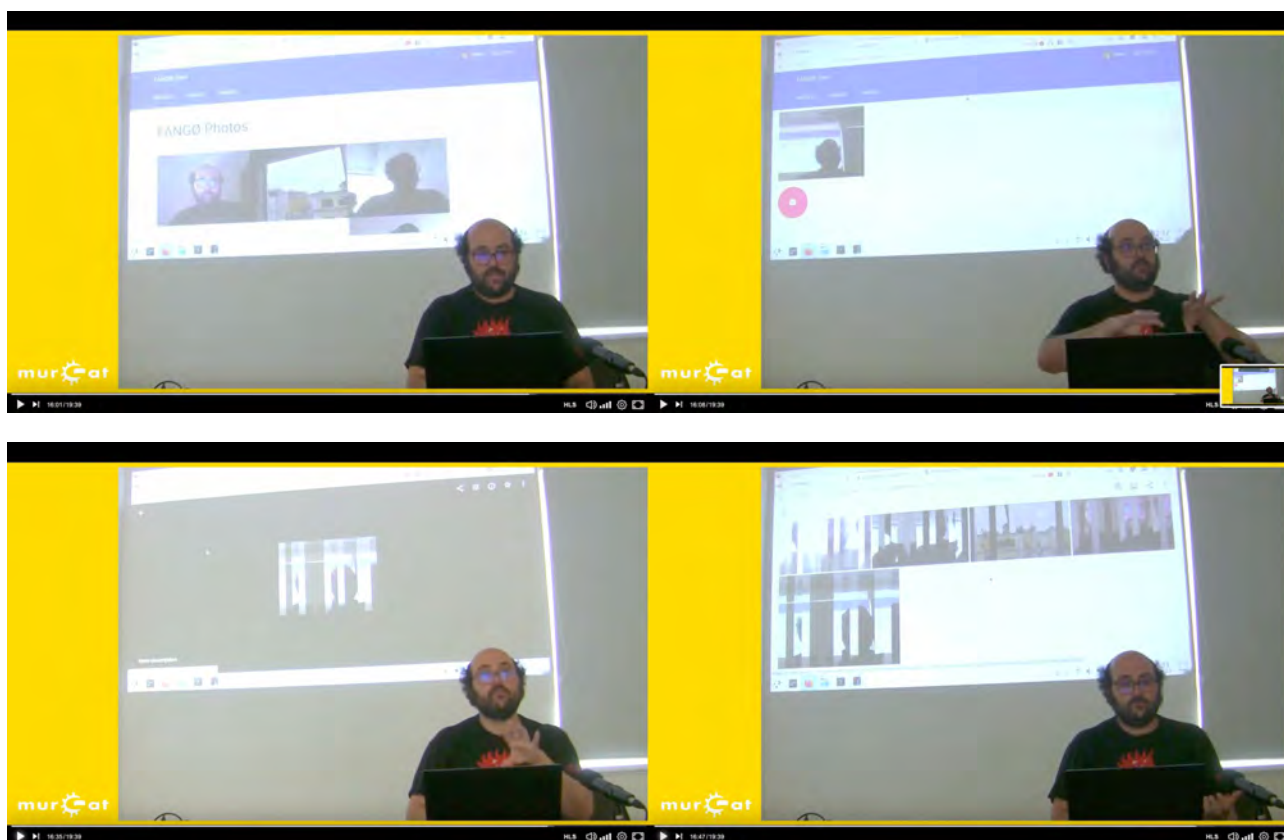


Figura 60. Presentación de FangøCam por Martín Nadal en el Worklab 2023 en mur.at.
Disponible en: <https://tube.graz.social/w/iKhKrDMSZMWpVvGB1xLz2a>

Con el mismo propósito de frustrar el entrenamiento de algoritmos de herramientas de “inteligencia artificial” el equipo del profesor de Ciencias de la Computación de la Universidad de Chicago Ben Y. Zhao ha desarrollado dos iniciativas vinculadas a la búsqueda de soluciones para artistas independientes, *Glaze*⁶⁸ y *Nightshade*⁶⁹. De esta manera, ambas nacen como denuncia ante modelos de IA generativa que, como MidJourney y Stable Diffusion, han sido entrenados con grandes conjuntos de datos de imágenes extraídas de Internet, muchas protegidas por derechos de autor.

Concretamente, *Glaze* se enfrenta a la problemática derivada de que muchos de estos modelos se utilicen también para imitar el estilo de diferentes artistas. De esta manera, diversos artistas independientes han encontrado réplicas de baja calidad de sus obras en línea, a menudo con sus nombres aún incrustados en los metadatos de las referencias del modelo, lo cual no solo devalúa su trabajo en cuanto a ingresos se refiere, sino también en cuanto a reputación. Frente a ello, *Glaze* se concibe como una plataforma *online* diseñada para proteger a los artistas mediante la interrupción de la imitación de sus estilos por parte de estos algoritmos de aprendizaje automático, aplicando una capa de ruido sobre un conjunto de cambios mínimos en las obras de arte, de modo que estas parezcan inalteradas a simple vista pero a los modelos de IA les parezcan de un estilo artístico radicalmente diferente. De esta manera, un observador humano puede percibir una obra realizada bajo un estilo determinado y el modelo de IA entenderlo como un estilo completamente opuesto. Con todo, los desarrolladores del proyecto recalcan que:

Desafortunadamente, *Glaze* no es una solución permanente contra la imitación de la IA. Sistemas como *Glaze* se enfrentan al reto inherente de ser a prueba de futuro (Radiya *et al.*). Siempre es posible que las técnicas que utilizamos hoy sean superadas por un algoritmo futuro, lo que podría hacer vulnerable el arte previamente protegido. Por lo tanto, *Glaze* no es una panacea, sino un primer paso necesario hacia herramientas de protección centradas en los artistas para resistir la imitación de la IA. Esperamos que *Glaze* y los proyectos posteriores brinden protección a los artistas mientras se consolidan las iniciativas a largo plazo (legales y regulatorias) (Glaze, s.f., párr. 8).

68 Véase: <https://glaze.cs.uchicago.edu/index.html>

69 Véase: <https://nightshade.cs.uchicago.edu/>

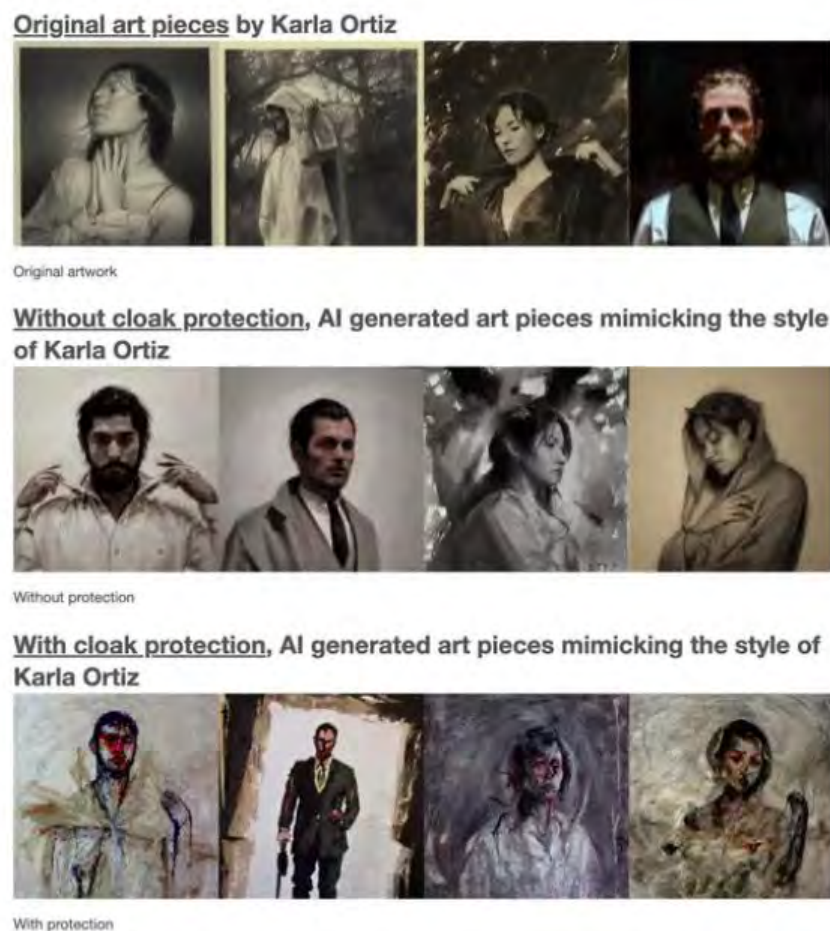


Figura 61. Muestra de cómo funciona Glaze. Fuente: Hill (2023)

Por su parte, *Nightshade* nace con la intención de abordar la asimetría de potencia entre diseñadores y modelos de aprendizaje automático mediante una herramienta que convierte cualquier imagen en una muestra de datos no apta para el entrenamiento de estos modelos. Concretamente, *Nightshade* transforma dichas imágenes en muestras “tóxicas”, de modo que los modelos entrenados con ellas sin consentimiento aprenden comportamientos impredecibles que se desvían de las normas esperadas. A través de este “envenenamiento” de los modelos de aprendizaje automático se busca disuadir a sus desarrolladores de ignorar los derechos de autor, las listas de exclusión voluntaria y las directivas de no extraer datos o robots.txt. El objetivo de *Nightshade* no es dañar los modelos como tales, sino aumentar el coste del entrenamiento con datos sin licencia, de modo que la negociación por los artistas de la cesión de los derechos sobre sus imágenes se convierta en una opción viable.

En suma, *Nightshade* funciona de forma similar a *Glaze*, pero en lugar de ser una defensa contra la imitación de estilos, está diseñado como una herramienta ofensiva para distorsionar las

representaciones de características dentro de los modelos de imágenes generativos. Sea como fuere, tanto en *Glaze* como en *Nightshade* se consigue que, mientras que los ojos humanos ven una imagen sombreada que prácticamente no ha cambiado con respecto a la original, el modelo de IA vea una composición radicalmente diferente, como se ilustra en la Figura 62.

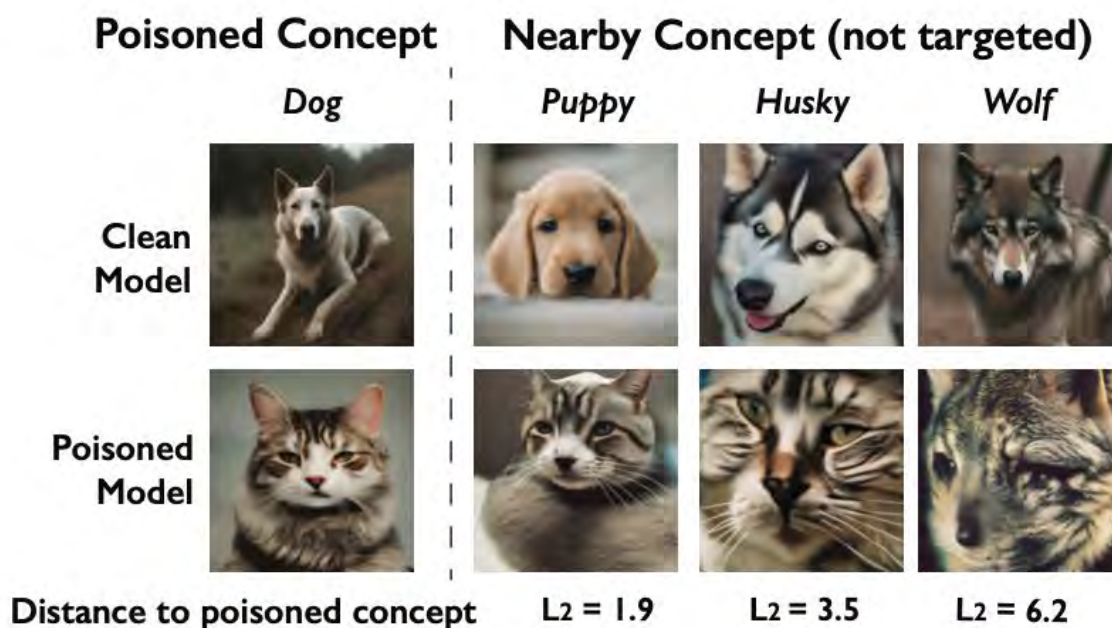


Figura 62. Imágenes generada a partir de diferentes indicaciones por un modelo SD-XL donde el concepto “perro” está “envenenado” por el empleo de *Nightshade*. Fuente: Shan *et al.* (2024, p. 817).

4.2.4. Ofuscación por ambigüación

Si la ofuscación temporal es morosa, al jugar con las oportunidades que abre la demora de su inevitable detección, la ofuscación cooperativa se basa en el poder de los grupos para enturbiar la información y la ofuscación selectiva busca ocultar una serie de datos a una serie de agentes, la ofuscación por ambigüación pretende contaminar de modo permanente las fuentes de datos personales (individuales o colectivos) para sembrar dudas sobre el valor de su recopilación y procesamiento.

Ya en el punto 2.5.2 adelanté algo de esto al referirme a cómo las tácticas de *data fandom* y *fan activism* conseguían manipular resultados estadísticos o de búsquedas. Sin embargo, no debemos olvidar que esta misma práctica se emplea con intereses menos legítimos, como relatan Brunton y Nissenbaum (2015, pp. 9-12) sobre el empleo de *bots* en Twitter (hoy X) para interferir en las conversaciones sobre las elecciones en Rusia o México (hoy cabría hablar del papel de su nuevo dueño, Elon Musk, en las elecciones de EEUU de 2024). En la misma categoría también encontramos las “granjas de likes” (*like-farming* en inglés), que consisten en el pago de pequeñas cantidades a cambio de un “Me gusta” en una

página de Facebook. Estas técnicas revelan la diversidad de motivos que podemos encontrar para la ofuscación, pues de hecho en este último caso no se trata de la resistencia a la dominación política, sino simplemente de la generación de confusión como un simple servicio a cambio de un pago (Brunton y Nissenbaum, 2015, p. 40).

Otro de los focos de interés de los desarrolladores de aplicaciones de ofuscación ha sido enturbiar las búsquedas en Internet y las interacciones en redes sociales. Respecto de las primeras, en 2006, Daniel Howe, Helen Nissenbaum y Vicent Toubiana desarrollaron *TrackMeNot*, una extensión del navegador *web* Mozilla Firefox escrita en Javascript, C++ y XUL y destinada a ocultar las búsquedas *web* reales de los usuarios en un flujo de consultas falsas (Howe y Nissenbaum, 2009, p. 5). Para ello, *TrackMeNot* recopilaba frases similares a consultas de la *web* y las enviaba, a través de solicitudes HTTP, a los motores de búsqueda que hubiese especificado el usuario (Google Search, Yahoo! Search, Bing Search, Baidu Search y Aol Search). De esta manera, *TrackMeNot* pretendía frustrar una elaboración de perfiles de los usuarios a través de sus búsquedas que había quedado en evidencia desde 2005 con las revelaciones de que el Departamento de Justicia de EEUU había requerido a Google sus registros de búsqueda de Google, unidas al sorprendente descubrimiento de un periodista del *New York Times* de que algunas identidades y perfiles podían inferirse incluso a partir de registros de búsqueda anónimos publicados por AOL (Brunton y Nissenbaum, 2015, p. 13).

Para aumentar esta funcionalidad básica y frustrar los intentos de los motores de búsqueda de distinguir entre consultas reales y las artificiales, con el tiempo se implementaron una serie de mecanismos adicionales para simular los comportamientos de búsqueda reales de los usuarios de manera más efectiva. En efecto, la emisión de estas consultas de relleno evolucionaba de modo que los diferentes usuarios desarrollaban diferentes listas de búsquedas, y la precisión de la imitación se perfeccionaba continuamente al volver a poblar dichas listas con nuevos términos generados a partir de los resultados obtenidos de las consultas previas. Todo este enmascaramiento de las actividades de los individuos alrededor de muchas consultas fantasmas hacía que sus patrones de búsqueda fuesen más difíciles de discernir, de modo que resultaba mucho más complicado determinar si una consulta era producto de la intención humana en lugar de un resultado automático de *TrackMeNot*. De esta manera, *TrackMeNot* extendía el papel de ofuscación, en algunas situaciones, para incluir la negación plausible (Brunton y Nissenbaum, 2015, p. 14), un concepto que hasta finales de siglo XX solía estar reservado a las inconfesables operaciones de guerra sucia de gobiernos, como las que el Comité Church (citado en Zinn, 1991, párr. 38) y citado en la sección 2.1 que imputaba en 1975 a la CIA y agencias similares de EEUU:

La no atribución a Estados Unidos de operaciones encubiertas era el propósito original y principal de la llamada doctrina de la “negación plausible”. Las pruebas presentadas ante este Comité demuestran que este concepto, diseñado para proteger a Estados Unidos y a sus operativos de las consecuencias de posibles revelaciones, se ha expandido para enmascarar las decisiones del presidente y sus altos cargos.

TrackMeNot contaba con una serie de parámetros configurables para personalizar aún más su comportamiento. Estos incluían opciones para habilitar o deshabilitarlo, la visualización de la barra de estado y la ráfaga de consultas. Además, los usuarios podían seleccionar los motores de búsqueda a los que deseaban dirigirse, seleccionar una frecuencia de consulta promedio y administrar las opciones de registro, así como una lista de palabras a excluir. Finalmente, el panel de control contaba con botones que permitían a los usuarios ver la lista de consultas y los registros de acciones dentro del propio navegador, así como acceso al sitio *web* de *TrackMeNot* para obtener información adicional.

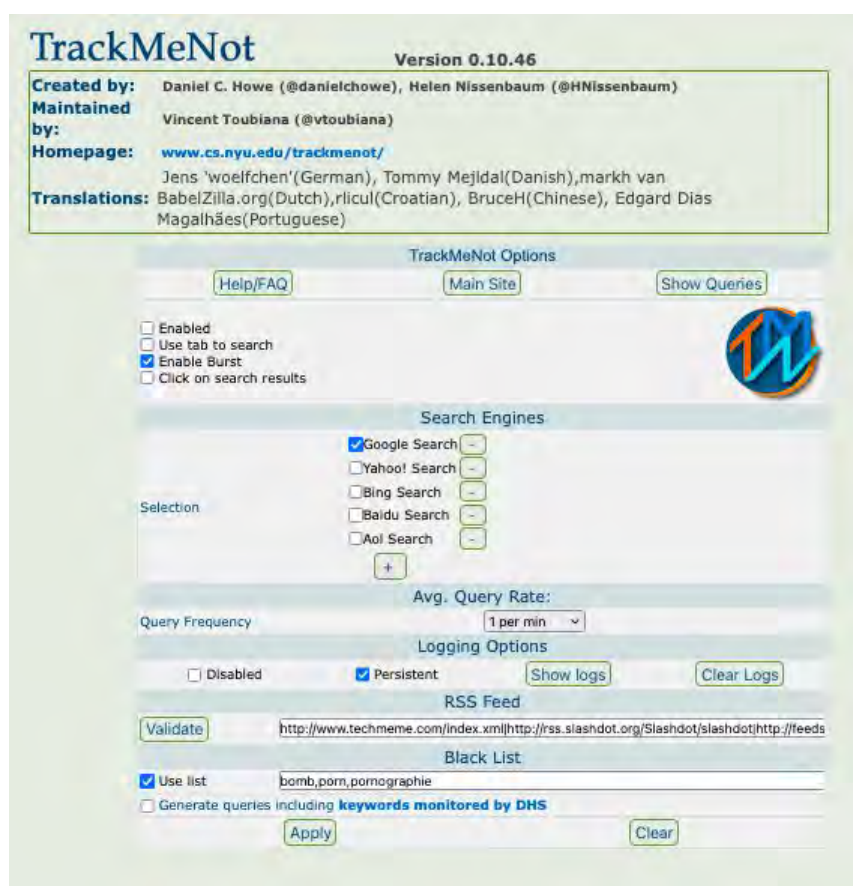


Figura 63. Captura de pantalla del panel de control de *TrackMeNot*. Recuperado el 3 de febrero de 2025.

Aunque *TrackMeNot* ya no recibe mantenimiento (Toubiana, s.f.), para Howe (2015, p. 91) se trata de un proyecto que ha inspirado a otros de manera directa e indirecta. Buena muestra de ello es la

iniciativa *I Like What I See* (2012)⁷⁰, del ingeniero de *software* Steve Klise, una extensión del navegador *web* Firefox que hacía clic automáticamente en todos los enlaces de “Me gusta” en Facebook. Con ello se pretendía ofuscar los verdaderos intereses de la persona que lo utilizase dentro de esta red social. Otra extensión del navegador similar que también se centra en Facebook es *Go Rando*⁷¹, del artista Ben Grosser, la cual ejecuta interacciones aleatorias en las publicaciones de Facebook que van más allá del inicial “me gusta” hacia otros sentimientos. De esta manera, *Go Rando* también ofusca las verdaderas interacciones en una masa de reacciones que abarcan los “me gusta”, “me encanta”, “me entristece”, “me sorprende” o “me enfada”, todo ello con vistas a devaluar un posible perfilado del usuario por parte de anunciantes u otras organizaciones.

Con todo, quizá el descendiente más directo de *TrackMeNot* haya sido *AdNauseam*, desarrollado en 2014 también por Daniel Howe, Helen Nissenbaum, y diseñado por Mushon Zer-Aviv. *AdNauseam* es una extensión del navegador Mozilla Firefox que aprovecha la ofuscación para frustrar el seguimiento por parte de los anunciantes en línea. En esencia, *AdNauseam* funciona como un bloqueador de anuncios y rastreadores, pero ofrece dos funciones adicionales: en primer lugar, recopila los anuncios que encuentra para su posterior visualización, lo que permite a los usuarios explorar de forma interactiva los anuncios que han visto y proporciona información sobre los perfiles algorítmicos en los que figuran; y, en segundo lugar, simula clics en todos los anuncios que aparecen con el objetivo de confundir a los rastreadores y disminuir el valor de los datos de seguimiento agregados (Howe y Nissenbaum, 2017, p. 57). Al mismo tiempo, el *software* ofrece a los usuarios una vía de expresión proactiva, alterando activamente el sistema económico que impulsa la lucrativa industria publicitaria en línea y sembrando la desconfianza (los anunciantes generalmente pagan a las redes publicitarias por los clics esperando que conlleven una reacción orgánica a sus reclamos) dentro de él.

⁷⁰ Véase: <https://github.com/sklise/i-like-what-i-see>

⁷¹ Véase: <https://bengrosser.com/projects/go-rando/>



Figura 64. Captura de pantalla de la visualización de la extensión AdNauseam cuando navegas una página con publicidad. Recuperado el 4 de febrero de 2025

Como puede verse en la Figura 65, con la intención de hacer más transparente el seguimiento y la elaboración de perfiles por parte de los anunciantes, *AdNauseam* ofrece a sus usuarios visualizaciones interactivas de los datos de anuncios recopilados. Estas visualizaciones proporcionan también la opción de inspeccionar los anuncios de manera individual para obtener una variedad de información. Otra serie de funciones derivadas proporcionan métricas adicionales, como el coste total estimado para las redes publicitarias por los anuncios supuestamente visitados en una página, sitio o período de tiempo concretos. Además, los anuncios se pueden filtrar y ordenar por fecha, categoría, red publicitaria, tipo de página visitada, etc. A su vez, este panel de visualización incluye mecanismos para importar y exportar conjuntos de datos de anuncios (en formato abierto JSON) desde dentro de la extensión.

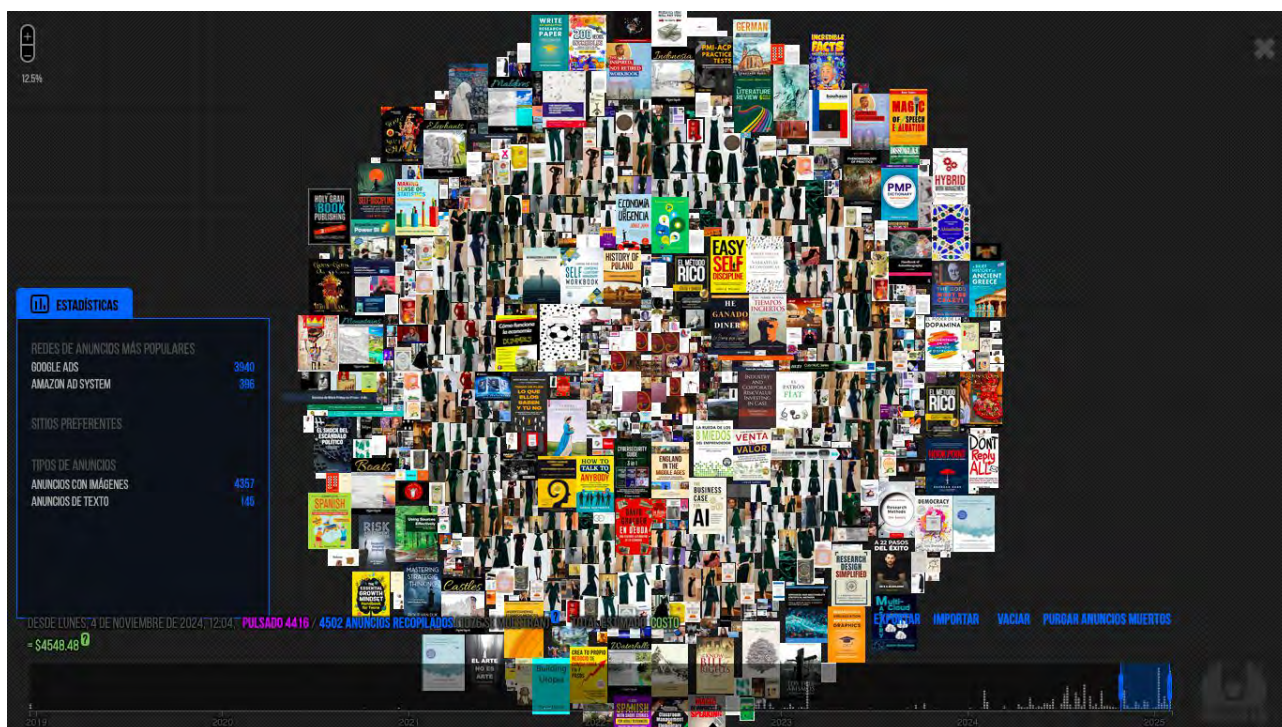


Figura 65. Captura de pantalla de mi página de estadísticas de *AdNauseam* de los últimos tres meses. Recuperado el 4 de febrero de 2025.

Es interesante resaltar aquí que Howe y Nissenbaum (2017, p. 60) cuentan que uno de los impedimentos con los que ha contado el proyecto es que, en un primer momento, el prototipo se desarrolló como una extensión exclusiva para Firefox disponible en la tienda de complementos de Mozilla. Más adelante, en la versión de producción, añadieron la compatibilidad con Opera y Chrome e hicieron una extensión para sus tiendas. Sin embargo, en enero de 2017, tuvieron conocimiento de que Google había prohibido *AdNauseam* en su tienda y, además, había comenzado a prohibir incluso la instalación o las actualizaciones manuales en Chrome, lo que impedía a los usuarios acceder a sus propios datos guardados, todo ello sin previo aviso ni advertencia.

Google respondió a las solicitudes de justificación que enviaron argumentando que *AdNauseam* había violado la siguiente cláusula de los Términos de servicio de la tienda: «una extensión debe tener un único propósito que sea claro para los usuarios» (citado en Howe y Nissenbaum, 2017, p. 60). Dado que el único propósito de *AdNauseam* era resistir la vigilancia no consensuada realizada por las redes publicitarias, de las que Google es un excelente ejemplo, esta empresa justificaba su decisión basándose en que la extensión se opone a su modelo de negocio principal. Para culminar, los autores lamentan que, independientemente de si uno es partidario de la ofuscación o no, es desconcertante saber que Google puede hacer que una extensión de privacidad, junto con los datos y preferencias almacenados,

desaparezca sin previo aviso. En este caso, se prohíbe una herramienta de contravigilancia, tal vez mañana sea una aplicación de chat segura o un administrador de contraseñas. En suma, para desarrolladores que, por lo demás, deben pagar una cuota para publicar elementos en la tienda Chrome, no puede ser más preocupante que no solo se pueda prohibir su *software* sin previo aviso, sino que con él se eliminen también comentarios, calificaciones, reseñas, lanzamientos y estadísticas (Howe y Nissenbaum, 2017, p. 60).

Muy influenciado por el proyecto de *AdNauseam*, así como por obras como *La era del Capitalismo de la Vigilancia* (2019) y *Signal and Noise* (2012), el mencionado Martín Nadal emprendió en 2019 el proyecto *Fango*, que al año siguiente en 2020 se enmarcó ya en el programa EMAP/EMARE (European Media Artist in Residence Exchange de la European Media Art Platform). En consonancia, el artista define *Fango* como «un arma en defensa del capitalismo de vigilancia» (Nadal, comunicación personal, 14 de noviembre del 2023), defendiendo durante nuestra entrevista el uso del concepto “arma” de la siguiente manera:

[E]s algo que nos están atacando y que no podemos hacer nada, efectivamente tú te puedes conectar con SSA en Beirut, y a lo mejor puedes conseguir que no te *trackeen*, o a lo mejor puedes nunca nunca hablar por WhatsApp y que nunca te *trackeen* o nunca ver Instagram, pero a mí me interesa más el lanzar ideas para el público normal, para mi madre, para mi prima, para mí (Nadal, comunicación personal, 14 de noviembre del 2023).

En este sentido, el dispositivo *Fango* consiste en un cargador de teléfono móvil modificado de manera que mientras lo estás utilizando, por ejemplo al cargar tu dispositivo durante la noche, toma el control del teléfono y va lanzando aplicaciones de manera aleatoria y realizando diferentes interacciones dentro de ellas, como dar “me gusta” a diferentes publicaciones dentro de Instagram. Con ello se busca que estas plataformas no puedan estar seguras de quién está manejando el teléfono, añadiendo esa capa de ruido que deslegitima el perfilado que realizan sobre nosotros a partir de nuestras interacciones. El autor determina de la siguiente manera el fin del proyecto:

[E]n el punto de a quién está dirigido ese proyecto, tiene como dos visiones, tiene una visión individual, de proteger la privacidad de una persona, pero luego también tiene una visión más utópica, que es una visión global [...] si todo el mundo usara un dispositivo de estos, el capitalismo de vigilancia no tendría razón de ser y colapsaría (Nadal, comunicación personal, 14 de noviembre del 2023).



Figura 66. Captura de pantalla de la página del proyecto. Fuente: <https://fango.martinnadal.eu/index.html>

Por otra parte, a la hora de presentar *Fangø* en cualquier espacio donde se expone, el proyecto también tiene un mensaje y una intención bien claros:

[U]na cosa que se cuidó mucho es que tenga un aspecto muy reconocible, [o] sea, el proyecto, sin ningún tipo de pudor, utiliza los logos de las grandes marcas, tiene como un chiste en castellano es como que es fango, que es barro, porque estás ensuciando toda tu interacción [...] luego cuando se presenta en una exposición, se presenta como si fuera una tienda, como si fuera un producto que realmente te lo podrías comprar y que te podría salvar. Que por lo menos tendría que tener alguna utilidad. Eso yo lo que intento es, que igual que hay objetos preciosos que son un poco chungos, pues por ejemplo, el iPhone o el Pixel 8, que son como una preciosidad y que luego de repente el negocio que tiene ese teléfono no es que tú hables bien, el negocio es extraerte el mayor número de datos y el que haya unas campañas de publicidad que estén perfectamente orientadas hacia ti (Nadal, comunicación personal, 14 de noviembre del 2023).

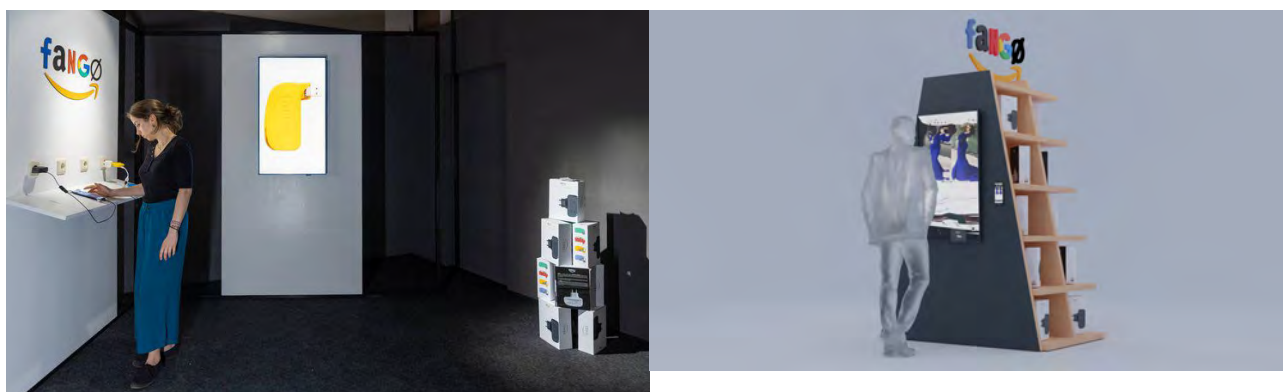


Figura 67. Imágenes de exposiciones de *Fango*. Fuente: <https://fango.martinnadal.eu/curator.html>

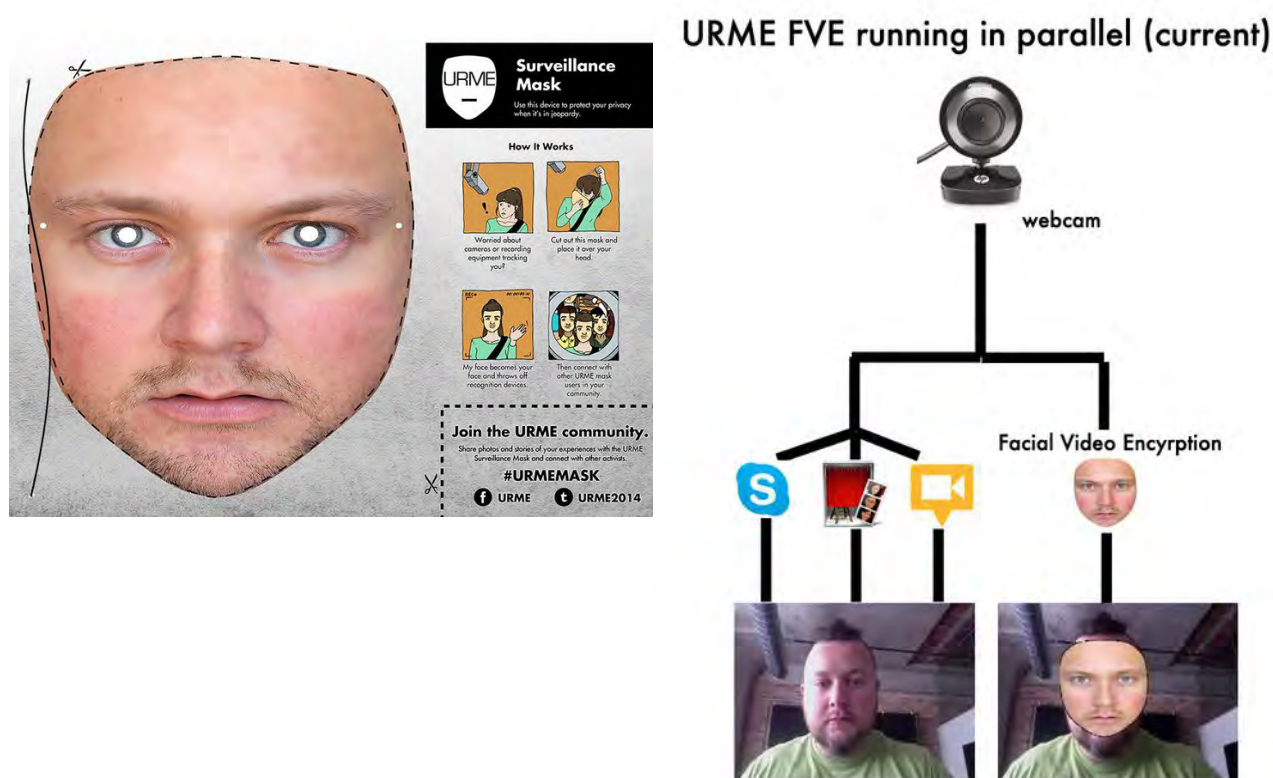
Por otro lado, dentro de esta categoría, encontramos proyectos con una fuerte vocación reivindicativa, empezando por *URME Surveillance*⁷² del artista interdisciplinar Leonardo Selvaggio. Se trata de una prótesis facial fabricada con resina dura pigmentada del rostro del propio Selvaggio para ser utilizada como reemplazo de la identidad del que la porta. La idea del autor es que, en lugar de esconderse de las cámaras, simplemente se le proporcione a la gente una cara rastreable pero distinta a la suya, de modo que pueda pasarse entre una multitud sin llamar la atención al tiempo que las cámaras identificarían un rostro que no es propio, en este caso la cara de Selvaggio. Si bien en un principio la máscara se podía adquirir por 200\$ más gastos de envío —para cubrir únicamente lo que cuesta producirlas—, actualmente no está disponible para su compra y, en su lugar, el autor ha puesto a disposición de quien lo precise unas réplicas gratuitas para imprimir en papel⁷³. El proyecto también incluye una modalidad para las videollamadas, el *URME Facial Video Encryptor*, un filtro que superpone la cara de Selvaggio sobre la tuya propia durante la videollamada.

⁷² Véase: <https://www.urmesurveillance.com/>

⁷³ Véase: <https://www.urmesurveillance.com/urme-paper-mask>



Figura 68. Ejemplo de cómo funciona URME Surveillance. Fuente: <https://www.urmesurveillance.com/>



Figuras 69 y 70. Ejemplos de cómo funcionan URME Paper Surveillance Mask y URME Facial Video Encryptor. Fuentes: <https://www.urmesurveillance.com/urme-paper-mask> y <https://www.urmesurveillance.com/urme-fve>

En segundo lugar, se encuentra el proyecto *Invisible*⁷⁴, de la artista y *biohacker* Heather Dewey-Hagborg, quien en 2014 diseñó como una provocación artística este producto de privacidad genética totalmente funcional que apunta más allá de la vigilancia para cuestionar la supuesta infalibilidad de las muestras de ADN. *Invisible* se compone de dos productos: por un lado, el spray *Erase*, que elimina el 99,5 % del ADN que puedes dejar en una superficie; y por otro, el spray *Replace*, que oculta el material biológico con “ruido” genético, derivado de más de 50 fuentes de ADN diferentes y que, al utilizar un conservante especial, lleva el método de ofuscación de la privacidad electrónica a lo biológico.

Invisible existe como una síntesis de representaciones: una instalación de arte, un producto funcional y un objeto diseñado, el sitio *web* de una empresa ficticia, un video/comercial, una intervención en los medios tradicionales y sociales, una serie de talleres prácticos, una intervención pública continua donde se colocan paquetes de forma encubierta en tiendas de todo el mundo y un conjunto de guías de código abierto disponibles en línea⁷⁵.

En tercer lugar, dentro de esta variante de proyectos destaco otro del ya citado Ben Grosser, denominado *ScareMail*⁷⁶. Lanzado en 2013, se trata de otra extensión del navegador *web* Mozilla Firefox que hace que el proveedor Gmail de Google agregue a la firma de cada correo electrónico una narrativa generada algorítmicamente que contenga una colección de términos de búsqueda probables para la NSA. Esta acción genera una sobreproducción de material para los programas de la NSA como PRISM y XKeyscore que afecta a su trabajo. Además, en un intento por evitar el filtrado automático por parte de los sistemas de búsqueda de la NSA, *ScareMail* se asegura de que el texto generado en cada correo electrónico es único.

74 Véase: <https://deweyhagborg.com/projects/invisible>

75 Véase: <https://web.archive.org/web/20190704202901/http://biononymous.me/diy-guides/>

76 Véase: <https://bengrosser.com/projects/scaremail/>

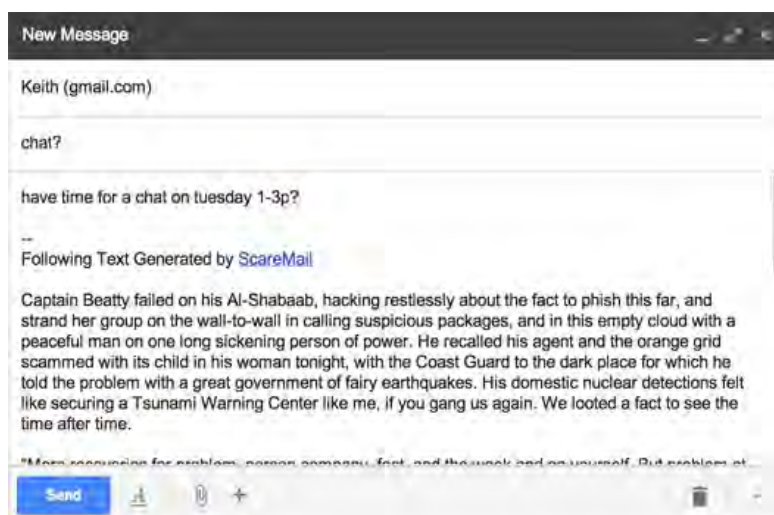


Figura 71. Captura de pantalla de ScareMail agregando texto a un correo electrónico en Gmail.

Fuente: <https://bengrosser.com/projects/scaremail/>

Con el objetivo distintivo de ofuscar la ubicación de un usuario móvil nació *CacheCloak*, diseñada por Joseph T. Meyerowitz y Romit Roy Choudhury. Se trata de un sistema que permite la anonimización en tiempo real de los datos de ubicación, a través de un servidor de confianza que recibe la ubicación de un usuario, la procesa utilizando *CacheCloak* y expone los datos ya expurgados a los distintos servicios basados en localización (LBS por sus siglas en inglés) (Meyerowitz y Choudhury, 2010, p. 38). Para Brunton y Nissenbaum (2015, pp. 12-13), *CacheCloak* adopta un enfoque de ofuscación que es adecuado para los servicios basados en la ubicación por actuar desde dos perspectivas distintas: en primer lugar, se asegura de que el usuario pueda seguir extrayendo datos relevantes; y en segundo lugar, trata de encontrar un enfoque que pueda funcionar indefinidamente en lugar de como una estrategia temporal para ganar tiempo.

A diferencia del uso estándar de geolocalización, en el modelo de *CacheCloak* tu teléfono predice sus posibles rutas y luego obtiene los resultados para varias rutas probables. De este modo, alguien que te espíe recibe información sobre diversos caminos posibles y queda incapacitado para distinguir el principio del final de una ruta, así como para determinar de dónde viene, a dónde quiere ir o incluso dónde está la persona en cuestión.

Otro proyecto en el que se ofusca la geo-localización de quien lo emplea es *SkyLift*⁷⁷, desarrollado por Adam Harvey en colaboración con Surya Mattu⁷⁸, y mejorado posteriormente gracias a una residencia *online* en la Schloss Solitude⁷⁹. Se trata de un dispositivo de bajo coste que reproduce las señales *Wi-Fi*

⁷⁷ Véase: <https://adam.harvey.studio/skylift/>

⁷⁸ Véase: <https://www.surymattu.com/>

⁷⁹ Véase: <https://schloss-post.com/the-future-of-living-with-surveillance/>

utilizadas para los servicios de geolocalización, lo que permite que el usuario de un teléfono inteligente aparezca virtualmente en casi cualquier parte del mundo.

La primera versión fue creada en el verano de 2016 para la exposición del !Mediengruppe Bitnik's Assange Room⁸⁰: *Welcome to Ecuador!* en la Zoo Galerie de Nantes, con la intención de trasladar virtualmente a los visitantes a una recreación de la habitación de Julian Assange en la que fue su ubicación real durante siete años, a saber, la Embajada de Ecuador en Londres. Este primer prototipo utilizó una Raspberry Pi y un *software* llamado mdk3 para emular la infraestructura *Wi-Fi* de la citada embajada (Harvey, citado en Herrmann, 2017, párr. 4).

En una versión posterior, el dispositivo se ejecuta en un ESP8266, un microcontrolador de *Wi-Fi* compatible con Arduino de bajo coste y que es de código abierto⁸¹, por lo que es posible replicarlo. *SkyLift* funciona mediante la difusión de direcciones MAC (las direcciones físicas que los fabricantes imprimen en el *hardware* para identificarlo) y, en consecuencia, no recurre a suplantación de IP o señal de GPS, ni a VPN, ni a aplicaciones de terceros, y tampoco requiere ningún clic. Este dispositivo funciona con cualquier aplicación de teléfono con servicios de ubicación disponibles, incluido *FindMyPhone* de iOS, si bien solo está operativa cuando tienes habilitados los servicios de ubicación de *Wi-Fi* y lo hace mejor en interiores (donde el GPS está atenuado) y en lugares donde las señales de *Wi-Fi* cercanas son inferiores a -80dBm, pudiendo quedar inhabilitado en áreas con señales de GPS fuertes, pues estas pueden anular los servicios de geolocalización de *Wi-Fi*.

Ya en 2018, y en el marco del evento artístico de verano *Tropez*⁸² en Berlín, Adam Harvey y Anastasia Kubrak⁸³ se valieron de una tecnología similar a la empleada en el proyecto *SkyLift*, para desarrollar : *Data Pools*⁸⁴. Jugando con el doble sentido de la expresión inglesa (depósitos de datos y piscinas de datos, o incluso datos de piscinas), los artistas lanzaron un proyecto de suplantación de geolocalización de *Wi-Fi* que reubica virtualmente tu teléfono en las latitudes y longitudes de las piscinas de la élite de Silicon Valley.

80 Véase: <https://www.bitnik.org/>

81 Véase: <https://github.com/adamhrv/skylift>

82 Véase: <https://tropeztropez.de/en/>

83 Véase: <https://anastasiakubrak.com/>

84 Véase: <https://adam.harvey.studio/datapools/>

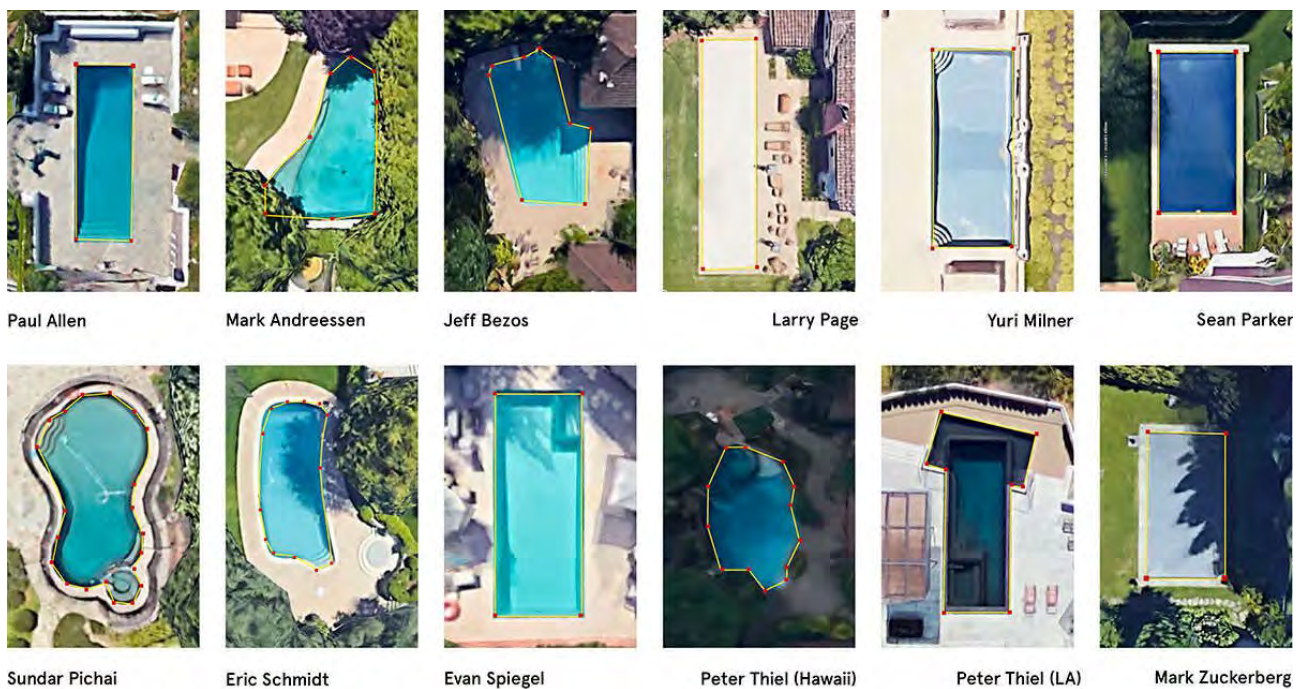


Figura 72. Ubicaciones de los grupos de datos para la suplantación de geolocalización de Wi-Fi del proyecto Data Pools. Fuente: <https://adam.harvey.studio/datapools/>

Según Harvey, *Data Pools* sirve como metáfora de un depósito de riqueza que es privado, como son las lujosas piscinas y mansiones de Silicon Valley, las cuales son financiadas mediante los mecanismos de vigilancia y extractivismo de nuestra información personal. Dado que las ubicaciones geográficas de estos espacios a menudo se ocultan, se esconden y se eliminan de las bases de datos de código abierto, con este proyecto los autores exploran la idea de qué pasaría si pudiéramos invertir esta lógica y sumergirnos en estos ridículos depósitos de riqueza, tanto virtual como físicamente, y si con ello podríamos aplicar los mismos métodos de extracción de datos para resaltar las ridículas desigualdades entre los directores ejecutivos y los usuarios de sus plataformas.

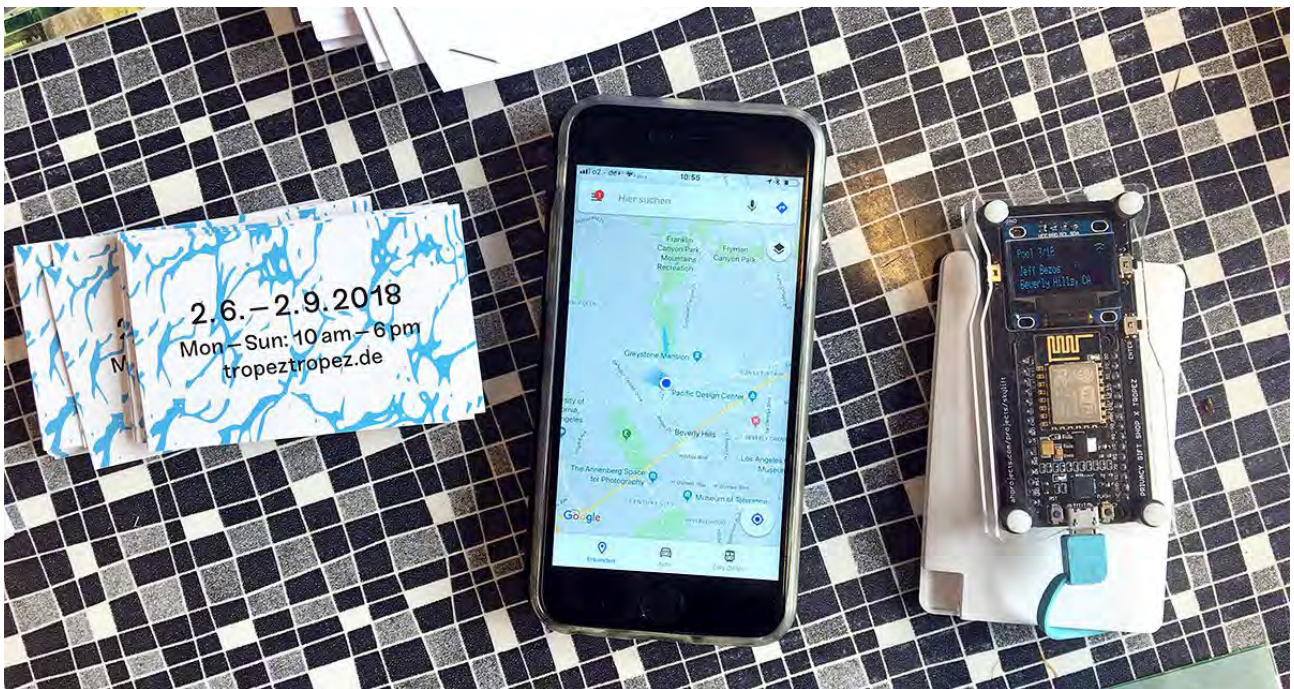
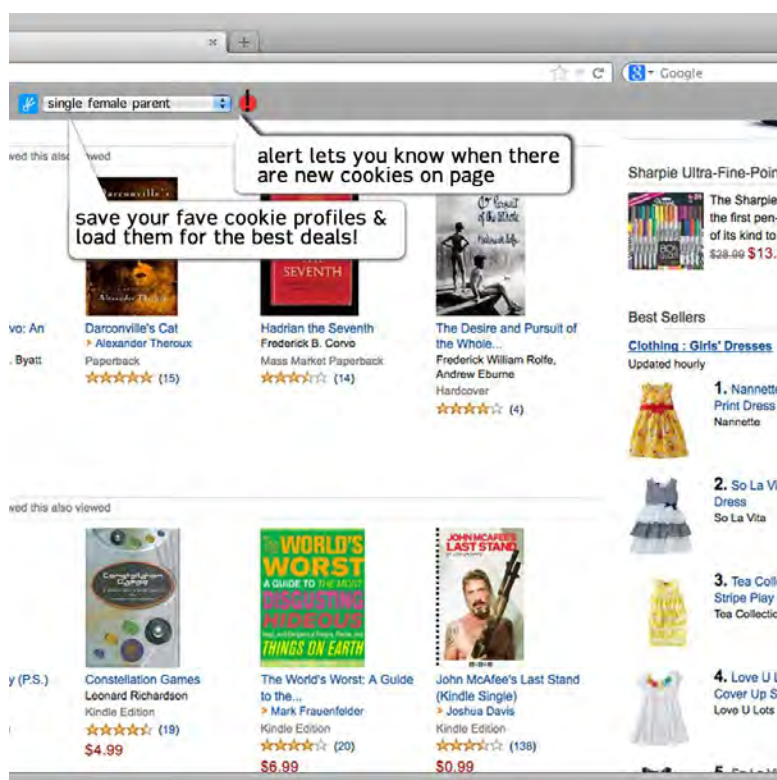


Figura 73. DataPools en la exposición en Tropez. Muestra de cómo el móvil te localiza en la casa de Jeff Bezos en Beverly Hills Fuente: <https://adam.harvey.studio/datapools/>

Este proyecto se instaló en el Humboldtthain Pool Park de Berlín en 2018 con la ubicación de Jeff Bezos, pero luego se cerró debido a quejas de suplantación de geolocalización, por lo que su dimensión expresiva realmente caló. Es más, Harvey apunta en su descripción del proyecto, que el personal del evento berlinés donde (se) lanzaron (a) esta piscina detectó que esta particular ubicación también se convirtió en una forma popular de navegar por Tinder en Beverly Hills.

El último caso que presento en esta categoría, de nombre *Vortex* y obra de la artista, diseñadora y programadora Rachel Law, resulta significativamente diferente a los presentados. Se trata de un videojuego masivo multi-jugador de gestión e intercambio de datos personales cuyas actividades principales son “extraer” *cookies* de los sitios *web* e intercambiarlas con otros jugadores. De este modo, *Vortex* te da la opción de intercambiar tu identidad entre los dueños de esas *cookies* de manera efectiva y experimentando una *web* diferente, ya que te permite cambiar *cookies* que te presentan como alguien con un género, etnia y profesión distintos y, de esta manera, convertir los anuncios “personalizados” en un mero ruido de fondo en lugar de en componentes distractores y manipuladores que te etiquetan como el modelo de tu identidad para algún vendedor. Con *Vortex* se busca educar sobre cómo los sistemas de filtrado en línea afectan nuestra experiencia en Internet, a la vez que se confunde y desvía la publicidad dirigida basada en *cookies* del navegador y otros sistemas de identificación (Brunton y Nissenbaum, 2015, p. 37).



Figuras 74 y 75. Ejemplos de cómo funciona Vortex. Fuente: <https://mfadt.parsons.edu/2013/projects/vortex/>

Además, este videojuego te permite compartir *cookies* de cuentas que te habilitan a comprar objetos que no están disponibles en tu ubicación. En este sentido, en lugar de optar por ocultarse o renunciar a los beneficios que pueden brindar las *cookies* y la personalización, *Vortex* permite a los usuarios implementar una multitud de identidades al tiempo que la propia identidad se ofrece a una multitud (Brunton y Nissenbaum, 2015, p. 38).

4.2.5. Tabla resumen de clasificación ejemplos de ofuscación

Nombre:	Desarrollado por:	Año:	Tipo de ofuscación:	Más información disponible en:
Dazzle camouflage	Norman Wilkinson	1914-1918	Temporal	https://en.wikipedia.org/wiki/Dazzle_camouflage
Chaff – Aviones II Guerra Mundial	Joan Curran	1939-1945	Temporal	https://iee-aess.org/post/blog/history-column-chaff
Cyclosa mulmeinensis	Cyclosa mulmeinensis	s.f.	Temporal	https://doi.org/10.1016/j.anbehav.2009.05.017
High frequency trading	VV.AA.	2010	Temporal	https://en.wikipedia.org/wiki/High-frequency_trading
Robo de Craigslist	Craigslist	2008	Temporal	https://abcnews.go.com/US/story?id=5930862
Muecas en el póker	VV.AA.	s.f.	Temporal	Brunton, Finn y Nissenbaum, Helen. (2015). <i>Obfuscation: A User's Guide for Privacy and Protest</i> . The MIT Press.
Exceso de información en un caso judicial	VV.AA.	s.f.	Temporal	Brunton, Finn y Nissenbaum, Helen. (2015). <i>Obfuscation: A User's Guide for Privacy and Protest</i> . The MIT Press.
Ofuscación de código	VV.AA.	90-actualidad	Temporal	https://en.wikipedia.org/wiki/Obfuscation_(software)
Camoflash	Adam Harvey	2008-2010	Temporal	https://adam.harvey.studio/camoflash/
Wearable face protector	Jing-cai Liu	2017	Temporal	https://jingcailiu.com/wearable-face-projector/
¡Yo soy Espartaco!	Esclavos romanos	73-71 a. C.	Cooperativa	<i>Espartaco</i> , (1960) película de Stanley Kubrick
Fuenteovejuna	Lope de Vega (basándose en hechos históricos)	1619	Cooperativa	<i>Fuenteovejuna</i> (1619) obra de Lope de Vega
Operación Vula	African National Congress (ANC)	Años 80	Cooperativa	https://en.wikipedia.org/wiki/Operation_Vula
Intercambio de tarjetas de fidelidad	VV.AA.	Años 90 - actualidad	Cooperativa	Brunton, Finn y Nissenbaum, Helen. (2015). <i>Obfuscation: A User's Guide for Privacy and Protest</i> . The MIT Press.
Intercambio de tarjetas SIM	VV.AA.	s.f.	Cooperativa	Brunton, Finn y Nissenbaum, Helen. (2015). <i>Obfuscation: A User's Guide for Privacy and Protest</i> . The MIT Press.
Criptografía	VV.AA.	s.f.	Cooperativa	https://en.wikipedia.org/wiki/Cryptography
Tor	VV.AA.	2008-actualidad	Cooperativa	https://www.torproject.org/

Nombre:	Desarrollado por:	Año:	Tipo de ofuscación:	Más información disponible en:
Wikileaks	VV.AA.	2006-actualidad	Cooperativa	https://wikileaks.org/
Bit Torrent Hydra	VV.AA.	2001-actualidad	Cooperativa	https://code.google.com/archive/p/hydraproject/
Facial Weaponization Suite	Zach Blas	2012-2014	Cooperativa	https://zachblas.info/works/facial-weaponization-suite/
FaceCloak	Wanying Luo, Qi Xie y Urs Hengartner	2009	Selectiva	https://crysp.uwaterloo.ca/software/facecloak/
SudoApp	Paul Ashley	2014	Selectiva	https://anonymome.com/individuals/mysudo/
Adversarial fashion	Kate Rose	2019	Selectiva Ambiguación	https://adversarialfashion.com
Realface Glamouflage	Simone C. Niquille	2013	Selectiva Temporal	https://www.designforsustainability.studio/signals/realface-glamouflage
CHBL Jammer Coat	COOP HIMMELB(L)AU	2014	Selectiva	https://architizer.com/projects/chbl-jammer-coat/
CV Dazzle	Adam Harvey	2010	Selectiva Temporal	https://adam.harvey.studio/cvdazzle/
HyperFace	Adam Harvey	2013	Selectiva Ambiguación	https://adam.harvey.studio/hyperface/
Stealth Wear	Adam Harvey	2012	Selectiva Temporal	https://adam.harvey.studio/stealth-wear/
FangøCam	Martín Nadal	2023	Selectiva	https://fangocam.muimota.net/
Glaze	Ben Y. Zhao <i>et al.</i>	2023	Selectiva Ambiguación	https://glaze.cs.uchicago.edu
Nightshade	Ben Y. Zhao <i>et al.</i>	2023	Selectiva Ambiguación	https://nightshade.cs.uchicago.edu/
Fan activisms	VV.AA	s.f.	Ambiguación	https://en.wikipedia.org/wiki/Fan_activism
Data fandom	VV.AA	s.f.	Ambiguación	https://doi.org/10.1177/1367877920904064
Twitter bots	VV.AA	2006-actualidad	Ambiguación	https://es.wikipedia.org/wiki/Twitterbot
TrackMeNot	Daniel Hove, Helen Nissenbaum y Vicent Toubiana	2009	Ambiguación	https://github.com/vtoubiana/TrackMeNot

Nombre:	Desarrollado por:	Año:	Tipo de ofuscación:	Más información disponible en:
I like what I see	Steve Klise	2012	Ambiguación	https://github.com/sklise/i-like-what-i-see
Likefarming	VV.AA	s.f.	Ambiguación	https://en.wikipedia.org/wiki/Click_farm
Go Rando	Ben Grosser	2017	Ambiguación	https://bengrosser.com/projects/go-rando/
AdNauseam	Daniel Howe, Mushon Zer-Aviv y Helen Nissenbaum	2014	Ambiguación	https://adnauseam.io/
Fangø	Martín Nadal	2019-2020	Ambiguación Selectiva	https://fango.martinnadal.eu/
ScareMail	Ben Grosser	2013	Ambiguación	https://bengrosser.com/projects/scaremail/
Invisible	Heather Dewey-Hagborg	2014	Ambiguación	https://deweyhagborg.com/projects/invisible
URME	Leonardo Selvaggio	2013	Ambiguación	https://www.urmesurveillance.com/
CacheCloak	Joseph T. Meyerowitz y Romit Roy Choudhury	2010	Ambiguación	https://doi.org/10.1145/1710130.1710138
Skilift	Adam Harvey y Surya Mattu	2016	Ambiguación	https://adam.harvey.studio/skylift/
Data Pools	Adam Harvey y Anastasia Kubrak	2018	Ambiguación	https://adam.harvey.studio/datapools/
Vortex	Rachel Law	2013	Ambiguación Cooperativa	https://web.archive.org/web/20160323030426/http://www.milkred.net/vortex

Tabla 3. Recopilación de ejemplos de ofuscación. Fuente: elaboración propia

4.3. La dimensión expresiva de la ofuscación

A pesar de que los pormenores de los proyectos presentados a lo largo de este capítulo son bastante diversos, se pueden reconocer ciertos aspectos en común. El primero es que todos critican la inclinación hacia la datificación que se facilita mediante el procesamiento algorítmico de grandes cantidades de datos. En este sentido, para Howe (2015, p. 92) la escala es crucial, ya que implica el uso de máquinas para la recopilación y el análisis de datos, eliminando en muchos casos el papel de la observación humana. Por lo tanto, es importante destacar que las tecnologías de ofuscación que he examinado a menudo se dirigen a sistemas algorítmicos. En efecto, dado que los tipos de interferencias presentadas en estos sistemas de recolección pueden ser frecuentemente detectados a través de un análisis humano (como ilustran los casos dentro del *glamouflage* o el ejemplo de *ScareMail*), mientras que en otros casos (como *FangoCam*, *Glaze*, *Nightshade* o *AdNauseam*) el usuario ni siquiera percibe que la ofuscación está teniendo lugar, puesto que funciona como un “ruido de fondo”, podemos concluir que lo que ataca la ofuscación aquí estudiada es específicamente «la naturaleza maquina de tales sistemas» (Howe, 2015, p. 92).

En este sentido, aunque las tecnologías que ofuscan estos sistemas algorítmicos de vigilancia generalmente se apoyan también en la automatización, en su caso no se trata de la automatización instrumental que impulsa al capital implacablemente hacia adelante, requiriendo aún más automatización en cada paso subsiguiente. En cambio, Howe (2015, p. 93) matiza que se trata de «una automatización táctica tan limitada en alcance y contexto que su objetivo final es a menudo borrar la necesidad de sí misma», culminando con esta elocuente apostilla de Munster (citado en Howe, 2015, p. 93). «La esperanza permanece, incluso si este esfuerzo fracasa, de crear un patrón más poético destinado a desagregar el comportamiento como una construcción predictiva y normativa». A partir de todo lo anterior, compartimos la conclusión de Howe (2015, p. 93) de que a menudo las herramientas basadas en la ofuscación son clasificables como «tecnologías *expresiva*» las cuales, «no sólo existen para cumplir una función instrumental, sino también para amplificar perspectivas sociales, culturales o políticas».

A partir de estas características, Howe puntualiza igualmente que los sistemas de ofuscación representan estrategias colectivas, en contraste con los enfoques más tradicionales orientados a la seguridad que se centran en la protección del individuo. En un nivel básico, las herramientas analizadas anteriormente pueden entenderse como comunales simplemente en la medida en que son expresivas: la amplificación de las voces sociales no dominantes puede concebirse como una práctica comunitaria en

sí misma. Más allá, el grado en que el ruido generado por las herramientas de ofuscación disminuye el valor de los datos recopilados en los sistemas puede servir para proteger incluso a quienes no utilizan estas herramientas. E incluso en los casos en que es posible eliminar dicho ruido, hay que tener en cuenta los recursos necesarios para hacerlo. Por lo tanto, la producción coordinada de pequeñas cantidades de ruido adicional que se agregan a los sistemas pueden causar costes significativos a los proveedores de servicios de minería de datos y, por lo tanto, influir en las decisiones futuras sobre qué información recopilar y almacenar e incluso, potencialmente, sobre las opiniones que se deben considerar al tomar tales decisiones.

Si nos remontamos al punto 1.1.5, donde exponía las metas que perseguía la ofuscación (protección, subversión y expresión), podemos observar que, si bien cada uno de estos objetivos parece estar presente en algún grado en los casos previamente analizados, su importancia relativa varía de una herramienta a otra. Pensemos, por ejemplo, en los casos relativos a las tácticas de ofuscación durante las grandes guerras, donde la protección es el elemento clave, mientras que las metas de expresión y subversión no resultan tan importantes. Y ello por mucho que después resultasen fuentes de inspiración directa para proyectos de ofuscación como *CV Dazzle*, donde la subversión y la expresión cobraban mucha más importancia que la protección. Recordemos también otros casos, como *Invisible* o *Wearable face protector*, proyectos puramente artísticos que, más allá de una estricta función de protección, se planteaban como objetivo primordial generar un debate en torno a la fe ciega en los rastros de ADN, en el primer caso, o a los excesos de los sistemas de vigilancia digital, en el segundo.

Por otro lado, Howe (2015, p. 94) detecta ciertas tensiones entre los objetivos que una u otra herramienta persigue primordialmente. Por ejemplo, para que la ofuscación actúe como una forma de protección, el ruido producido por un sistema debe mostrar un elevado nivel de indistinción en relación con los datos que ese sistema intenta capturar. En pocas palabras, debe resultarle complicado a un oponente diferenciar este ruido de la información que busca recopilar.

En coherencia con ello, si concebimos una herramienta que sea perfecta en el aspecto de protección, una en la cual nunca se pueda filtrar el ruido de la información, el sistema sería prácticamente invisible al adversario. Sin embargo, las capacidades expresivas de un sistema tan completamente indetectable serían probablemente mínimas, precisamente porque el adversario no tendría noción del ruido que se introduce. Por el contrario, en una situación donde un sistema es muy expresivo, podría ser más sencillo para el contrario filtrar el ruido generado, lo que reduciría las capacidades protectoras de las herramientas sin por ello privarlas de la capacidad de crear momentos (más o menos efímeros) a salvo de la vigilancia. Así, aunque parece existir una relación inversa entre los objetivos de expresividad y

protección, Howe (2015, p. 95) encuentra interesantes contraejemplos que pueden diluir esta supuesta incompatibilidad. No en vano, los protocolos de conocimiento cero a los que aludí en torno a *Sudo App* podrían respaldar la idea de una herramienta que, siendo fácilmente detectable, produzca datos altamente indistinguibles, de modo que un oponente pueda reconocer que está inyectando ruido en su sistema, pero por razones técnicas, culturales o de otro tipo, no pueda o no quiera filtrarlo. En esta situación, podemos concluir que no son descartables los sistemas técnicos de ofuscación que protejan efectivamente al usuario y al mismo tiempo permitan un alto grado de expresividad.

5. Tácticas recursivas para una democracia participativa: Ofuscación selectiva como generación de un procomún de datos a través de Decidim ⁸⁵

⁸⁵ Esta sección se basa parcialmente en un capítulo titulado *Decidir Decidim: prácticas recursivas para una democracia participativa* que forma parte del libro (Solera, 2025), para el libro *Algoritmos II*, [pendiente de publicación]

5.1. Qué es Decidim

5.1.1. Imaginar colectivamente la ciudad

«Las ciudades comienzan en la mente»: Graeber y Wengrow (2021/2022, p. 343) se apoyan en esta cita del filósofo Elias Canetti para desmontar las arraigadas creencias sobre unas estructuras sociales de los cazadores-recolectores basadas en el parentesco familiar y abocadas a conflictos derivados del debilitamiento de dichos lazos a medida que crecían sus poblaciones. Se nos ha inculcado que cuanto mayor es el grupo, menos estable resulta. Sin embargo, estudios recientes en la demografía de cazadores-recolectores de nuestros días muestran que las estructuras sociales «anidadas» simplemente no existen (Wengrow, 2019, párr. 4). Estos grupos no son diferentes a los habitantes de la ciudad o a los antiguos cazadores-recolectores. Todos compartimos la capacidad de sentirnos cerca de personas que quizá nunca conozcamos y tomamos parte de una sociedad que en su mayoría existe solo virtualmente. «Los recolectores pueden existir a veces en pequeños grupos, pero no viven en *sociedades* a pequeña escala —y probablemente jamás lo han hecho» (Wengrow, 2019, párr. 5).

Por tanto, estos estudios apuntan hacia la idea de que vivir en la ciudad no debiera haber resultado un hecho tan antinatural como para abocarnos a delegar nuestro futuro en «nuevas clases de administradores, sacerdotes, reyes y políticos-guerreros que tomaran decisiones por nosotros y mantuvieran el orden» (Wengrow, 2019, párr. 9). En lugar de ello, lo que hemos venido haciendo a lo largo de la historia es, efectivamente, vivir en estos grupos sin límites (como son las ciudades) y, lo que es más interesante, no siempre organizados bajo regímenes autoritarios, sino más bien alrededor de concejos y asambleas populares que se autogobiernan (Graeber y Wengrow, 2021/2022).

Al retrotraernos hasta el estudio de la historia de los primeros urbanitas aprendemos que nuestras reclamaciones sobre el derecho a inventar la ciudad (España Naveira, 2021), en lugar de ir contra el desarrollo de la historia o de la evolución social, buscan seguir su curso. Cuando perseguimos dicho derecho, realmente no estamos más que reavivando la creatividad política que dio vida a las ciudades y sembrando esperanza en un futuro sustentable para, en última instancia, nuestro planeta.

De hecho, cuando se nos da, ya en sociedades contemporáneas, la oportunidad de inventar colectivamente la ciudad, en lugar de imaginar grandes rascacielos o nuevas atracciones que atraigan un turismo cada vez más insostenible, decidimos apostar por la mejora del pavimento, crear zonas infantiles inclusivas, así como aumentar los kilómetros de carril bici y mejorar el ecosistema con más zonas verdes. En definitiva, crear más espacios seguros y comunes donde encontrarnos.

Y aquí no hablo de futuribles, sino de casos como la convocatoria de 2020 de los presupuestos participativos de la ciudad de Barcelona⁸⁶, un proceso a partir del cual vecinas y vecinos de la ciudad pudieron presentar, definir, debatir y escoger proyectos de inversión que el Ayuntamiento de la ciudad ejecutaría en cada uno de sus distritos, disponiendo de 30 millones de euros del presupuesto municipal para que decidiesen dónde querían invertirlos.

Dicha convocatoria se apoyó en una plataforma de *software* libre denominada Decidim⁸⁷, desarrollada en primer lugar desde el propio Ayuntamiento, y que luego fue ganando cierta autonomía gracias a la comunidad que la mantiene. Qué es Decidim, cómo surgió, cómo funciona y qué posibilidades brinda para estimular nuestra inteligencia colectiva, son cuestiones que resultan claves de cara a desbancar esas «zonas muertas de la imaginación» (Graeber, 2015, pp. 49–106) a las que los mecanismos burocráticos actuales generalmente nos conducen.

5.1.2. Pensar colaborativamente los procesos de participación democrática

Los impulsores del proyecto (Barandiaran *et al.*, 2024, pp. 1–3) definen Decidim como una infraestructura digital para la democracia participativa. Se trata de una plataforma construida íntegra y colaborativamente con *software* libre y configurable para ser utilizada como una red política para la participación democrática. Decidim permite crear multitud de procesos de planificación estratégica, presupuestos participativos, diseños colaborativos de normativas o elecciones. Además, posibilita estructurar órganos y asambleas de gobierno, convocar consultas públicas y referéndums y canalizar iniciativas para diferentes procesos de toma de decisiones. Y todo ello lo hace no solo facilitando los encuentros en línea sino conectando las reuniones presenciales con el mundo digital a través del envío de invitaciones a reuniones geolocalizadas, la gestión de inscripciones o la facilitación de la publicación de actas.

Con todo, para poder entender en qué consiste Decidim, tenemos que tener en cuenta que este proyecto es hijo de un contexto muy concreto: por un lado, es descendiente del *hacktivismo* autónomo de los primeros 2000, que explora democratizar las tecnologías digitales más allá de su forma opaca y orientada al consumo; y por otro, se inserta dentro de las iniciativas municipalistas que buscan una mayor participación ciudadana en sus entornos. Estas tendencias, lejos de recorrer caminos paralelos, se vieron entrelazadas en torno al movimiento 15M y a todos los cambios en el ámbito tanto político como social que fueron desarrollándose tras él, entre los que conviene destacar como pioneros la red

⁸⁶ Véase: <https://www.decidim.barcelona/processes/PressupostosParticipatius/f/4688/?locale=es>

⁸⁷ Véase: <https://decidim.org/>

social N-1 (Cabello *et al.*, 2013) o iniciativas políticas como el Partido X (Barandiaran *et al.*, 2024, pp. 1–3).

Muchas de las ideas, prácticas y alianzas sembradas durante este tiempo llegaron finalmente al ámbito institucional con la victoria en las elecciones locales de España de mayo de 2015 de decenas de candidaturas municipalistas. No en vano, en muchas de ellas, destacando los casos de Madrid y Barcelona, se habían integrado algunos de los mencionados *hacktivistas* con el objetivo de promover infraestructuras públicas y digitales para la democracia participativa.

Es así cómo, en primer lugar, el Ayuntamiento de Madrid puso en marcha la plataforma decide.madrid.es⁸⁸, basada en un *software* libre denominado Cónsul⁸⁹, seguido del de Barcelona, que a principios de 2016 optó por una bifurcación (o *fork*) de Cónsul para desarrollar su espacio digital para procesos participativos, decidim.barcelona⁹⁰. Sin embargo, algunas diferencias tanto en la visión como en la práctica entre los diferentes equipos de innovación democrática provocaron una división entre las dos ciudades. Como resultado, a principios de 2017 el gobierno de Barcelona lanzó Decidim como un *software* completamente nuevo con una arquitectura más modular y co-desarrollable (Barandiaran, 2019), cuyas funcionalidades han ido creciendo con los años.

Desde entonces, y a escala estatal, Decidim se ha extendido a otros municipios, como Sabadell, Martorell o Pamplona, y a gobiernos autonómicos como el de Cataluña o el de Castilla La Mancha. A escala internacional, se ha implementado en ciudades como Helsinki, Ciudad de México y Nueva York, en instituciones nacionales como la Asamblea Nacional francesa o el Gobierno Federal de Brasil, así como en instancias supranacionales como la Conferencia sobre el Futuro de Europa. Decidim también se ha implementado con éxito en iniciativas de la economía social y solidaria como la cooperativa de energía limpia Som Energia, y en universidades como la UNED o la Universidad de Burdeos⁹¹.

88 Véase: <http://decide.madrid.es/>

89 Véase: <https://consuldemocracy.org/es/>

90 Véase: <http://decidim.barcelona/>

91 Véase: <https://decidim.org/es/usedby/>

5.2. Cómo funciona

5.2.1. Articulación de la plataforma

En cuanto a su articulación, Decidim funciona como una matriz de participación personalizable y flexible con múltiples posibilidades. No obstante, en la instancia original decidim.barcelona la mayoría de procesos sigue un esquema metodológico dividido en cuatro fases: una primera informativa, donde se enmarca el proceso, seguida de una serie de debates para generar y discutir propuestas, una posterior selección deliberativa de las mismas, y finalmente su implementación durante todo el mandato. Sea como fuere, para entender cómo opera Decidim, debemos realizar una primera distinción entre los dos elementos básicos sobre los que está pensada: los espacios y los componentes participativos (Barandiaran *et al.*, 2024, pp. 77–85):

Por un lado, los “espacios” son los marcos que definen cómo se llevará a cabo la participación y los entornos o medios donde se pueden realizar diversas actividades, distinguiéndose cinco y contando cada uno con un diseño específico: “Iniciativas”, “Procesos”, “Asambleas”, “Consultas” y “Jornadas”. De manera ilustrativa, una propuesta ciudadana para cambiar una norma se realizaría a través de “Iniciativas”; la articulación de las reuniones de un consejo a través de “Asambleas”; el desarrollo de un presupuesto participativo, una planificación estratégica o una convocatoria electoral tendría lugar en “Procesos”; para un referéndum o votación utilizaríamos “Consultas”; y para organizar un evento como una conferencia o un congreso recurriríamos a “Jornadas”.

Por otro lado, los “componentes participativos” son los que permiten y definen una serie de operaciones e interacciones entre las entidades participantes y la plataforma, así como entre las propias participantes, dentro de cada uno de los espacios. Entre estos componentes participativos destaco: “blogs”, “debates”, “encuestas”, “páginas estáticas”, “presupuestos participativos”, “propuestas”, “rendición de cuentas”, “sorteos”, “votaciones” y “encuentros”. A través de la siguiente tabla resumen podemos ver qué componentes se pueden incluir en los distintos espacios:

Componentes	Espacios				
	Iniciativas	Procesos	Asambleas	Consultas	Jornadas
Propuestas	X	V	V	X	V
Rendición de Cuentas	X	V	V	X	X
Debates	X	V	V	V	X
Encuentros	X	V	V	V	V
Votaciones	X	V	V	V	X
Blogs	V	V	V	V	V
Presupuestos participativos	X	V	X	V	X
Encuestas	X	V	X	X	V
Páginas	V	V	V	V	V
Sorteos	X	V	V	X	X

Tabla 4. Tabla representativa de qué componentes pueden ir en cada espacio de Decidim. Fuente: Elaboración propia

A su vez, algunos de estos componentes comparten también características funcionales que incluyen la posibilidad de que las participantes comenten las acciones y las compartan en otro sitio *web* o sigan las novedades de la siguiente manera:

Componentes	Funciones							
	Comentar	Seguir	Compartir	Control de las versiones	Borradores colaborativos	Participación Textos	Enmiendas	Apoyos
Propuestas	V	V	V	V	V	V	V	V
Rendición de Cuentas	V	V	V	V	X	X	X	X
Debates	V	V	V	V	X	X	X	X
Encuentros	V	V	V	V	X	X	X	X
Votaciones	V	V	V	X	X	X	X	X
Blogs	V	V	V	X	X	X	X	X
Presupuestos participativos	V	V	V	X	X	X	X	X
Encuestas	X	X	X	X	X	X	X	X
Páginas	X	X	X	X	X	X	X	X
Sorteos	X	X	X	X	X	X	X	X

Tabla 5. Tabla representativa de qué funciones tiene cada componente. Fuente: Elaboración propia

A modo de ejemplo de cómo se pueden combinar los componentes en un espacio participativo, adelantaré cuál fue mi propuesta para la plataforma de Decidim para Quererla es Crearla que detallaré en el Capítulo 6 con mayor profundidad, pero que puede servir para ilustrar esta explicación: De esta manera, para un colectivo muy diverso que defiende la educación inclusiva, en el que se encuentran,

entre otros, familias, personal docente y orientador, asociaciones y ONGs, investigadores y alumnado, y el cual comenzó en el ámbito estatal pero poco a poco se ha ido expandiendo a otros territorios, sucede que, aunque se organizan reuniones periódicas en alguna plataforma o espacio físico, y cuentan con una página *web* donde se van publicando alguna información de interés, realmente no tienen un punto perenne y colaborativo de encuentro.

Por lo que, para este caso, propuse que quizá fuese conveniente, aprovechando un próximo congreso que se estaba organizando, comenzar habilitando el espacio “Jornadas”, que incluya el componente “Encuentros” para que sus afines puedan ir registrándose para este evento (tanto si van a participar presencialmente como si van a participar de manera telemática). Además, dentro de este espacio se pueden incluir otros componentes como “encuestas”, para recabar más información acerca de qué temas interesan a los asistentes, así como dilucidar otras cuestiones logísticas, un “blog” donde el equipo organizador puede ir sugiriendo lecturas previas y generando una conversación en torno a ellas, y el componente “propuestas” para que las participantes puedan ir aportando sus contribuciones previas de cara al desarrollo del evento. Y una vez que el proyecto hubiese madurado, quizá fuese conveniente abrir otros espacios como “Procesos y Asambleas” en función del marco de trabajo sobre el que cada participante o grupo de participantes vaya a centrarse, dado que estos espacios permiten incluir componentes como “debates”, “encuentros” y “propuestas” para trabajar de manera colaborativa.

En cuanto a las diferentes formas de participación podemos distinguir tres categorías diferentes: en un primer nivel encontraríamos a los “visitantes”, que tienen acceso a todos los contenidos sin tener que registrarse ni proporcionar ningún tipo de información. En segundo nivel hallamos a las “participantes registradas”, las cuales pueden crear contenido y comentarios, inscribirse en reuniones, respaldar contenido, seguir a otras participantes y temas en la plataforma, personalizar su perfil y recibir notificaciones, menciones y mensajes privados. Para registrarse deben elegir un nombre de usuario y una contraseña, aceptar el acuerdo de usuario y proporcionar una cuenta de correo electrónico. Las participantes registradas también pueden verificar su cuenta (lo que significa que su nombre de usuario va acompañado de un símbolo especial, que indica que realmente son quienes dicen ser en su perfil). En último nivel encontramos a las “participantes verificadas”, que contribuyen a la toma de decisiones. Para entrar en esta categoría, primero deben ser autenticadas como miembros de la organización, ciudadanas del municipio o constituyentes del grupo de toma de decisiones (una asociación, comunidad, colectivo, etc.) en cuestión. Decidim ofrece diferentes formas de realizar este proceso: verificación física, por código personal, por SMS o a través del censo de la organización o localidad de

las que se trate. Una vez verificadas, las participantes pueden tomar decisiones apoyando propuestas, firmando iniciativas y votando en consultas.

Es relevante puntualizar que las participantes pueden registrarse como individuo o como colectivo (asociaciones, organizaciones, etc.), además de que también pueden crearse grupos de usuarios que luego se integren en un colectivo. De este modo, Decidim permite a las participantes pertenecientes a un grupo expresarse o actuar, ya sea de forma individual o encarnando la identidad colectiva. De manera resumida vemos las opciones en la siguiente tabla:

Opciones	Participantes (individuales o grupos)		
	Visitante	Registrado	Verificado
Ver	v	v	v
Compartir	v	v	v
Insertar	v	v	v
Contestar una encuesta	v	v	v
Seguir	x	v	v
Apoyar	x	v	v
Crear	x	v	v
Comentar	x	v	v
Unirse a una reunión	x	v	v
Tener perfil personal	x	v	v
Votar	x	x	v

Tabla 6. Tabla representativa de qué acciones puede realizar cada participante. Fuente: Elaboración propia

Por último, quisiera resaltar la figura de las “administradoras”, que son las participantes que tienen permisos de acceso al panel de gestión. Existen diferentes tipos: las “administradoras generales” (ya sea de toda la plataforma o de espacios y componentes específicos), que diseñan, abren y cierran espacios y componentes, además de gestionar los permisos para usuarios registrados o verificados; los “moderadores”, que regulan las propuestas, comentarios o debates que hayan sido denunciadas, decidiendo si mantenerlos visibles u ocultarlos; los “colaboradores”, que leen contenidos inéditos y crean notas y respuestas a propuestas, pero no pueden modificar nada; y por último, los “evaluadores”, que aceptan o rechazan propuestas o asignan un coste económico a las mismas. En la siguiente tabla vemos sus funciones resumidas:

Funciones	Administración			
	Admin	Colaborador/a	Moderador/a	Valorador/a
Acceso al panel de control	V	V	V	V
Gestión y configuración de la plataforma	V	X	X	X
Gestionar permisos usuarios registrados o verificados	V	X	X	X
Diseñar la página principal	V	X	X	X
Abrir, configurar y cerrar espacios y componentes	V	X	X	X
Moderar propuestas, comentarios o debates	V	X	V	X
Leer contenidos inéditos	V	V	X	X
Crear notas y respuestas a propuestas	V	V	X	X
Aceptar o rechazar propuestas	V	X	X	V
Asignar un coste económico a la propuesta	V	X	X	V

Tabla 7. Tabla representativa de qué funciones tiene cada tipo de administradora. Fuente: Elaboración propia

A su vez, todo el contenido de la plataforma se puede clasificar según diferentes criterios. Por ejemplo de manera temática o territorial, así como según diferentes categorías, subcategorías o *hashtags* para que el contenido sea más sencillo de buscar por las personas interesadas. Es por estas características de construcción y funcionamiento que afirmo que estamos ante una herramienta diseñada desde su inicio tanto para una alta «modularidad» como para una variada «granularidad» de las formas de acción en ella (Benkler, 2006/2015, pp. 141–142), lo que favorece la participación a diversas escalas de implicación en la toma de decisiones:

La “modularidad” es aquella propiedad de un proyecto que describe la medida en que este puede descomponerse en componentes más pequeños, o módulos, que es posible producir independientemente antes de ensamblarlos en un conjunto. Si los módulos son independientes, los colaboradores individuales pueden elegir cuándo y cómo contribuir con independencia de lo que hagan los demás, lo cual maximiza su autonomía y flexibilidad para definir la naturaleza, alcance y temporalidad de su participación en el proyecto. [...] La “granularidad” se refiere al tamaño de los módulos, en términos de tiempo y esfuerzo que un individuo debe invertir para producirlos. [...] Por consiguiente, la cantidad de personas que, en principio, pueden participar en un proyecto es inversamente proporcional a la escala de la contribución mínima que se requiere para producir un módulo servible. Así pues, la granularidad de los módulos determina la mínima inversión individual posible que se requiere para participar en un proyecto.

5.2.2. Gobernanza: Decidir recursivamente Decidim

Sin embargo, llegados a este punto, no deberíamos caer en creencias tecnosolucionistas que profesan que más tecnología origina más participación y, por ende, más democracia. Más aún si atendemos una vez más al estudio sobre las grandes ciudades antiguas autogobernadas como Teotihuacán, que, sin contar siquiera con medios de transporte de tracción animal, dejaban a las antiguas ciudades-Estado griegas a la altura de poco más que aldeas fortificadas (Graeber y Wengrow, pp. 192, 336). Si a esto sumamos la cada vez menor esperanza de vida de algoritmos, *apps* y buzones ciudadanos que en los últimos tiempos se suman a la lista del «*participatory washing*» (Barandiaran *et al.*, 2024, p. 125), resulta pertinente preguntarnos por la viabilidad democrática de Decidim.

Y es que, a diferencia de otros modelos que persiguen un objetivo de participación eminentemente cuantitativo, en Decidim aprovecharon las tempranas discusiones durante su ya mencionada bifurcación de Consul para desplegar un proceso de reflexión e intervención democráticas que aspiraba a “decidir Decidim”. Así, en noviembre de 2016 se lanzó dentro de la propia plataforma decidim.barcelona un proceso abierto para el «diseño participativo de la plataforma Decidim»⁹². Culminado en febrero de 2017 tras casi 100 propuestas de más de 450 participantes, de él no sólo emergió el nuevo *software* sino algo mucho más decisivo: la comunidad democrática de (co)diseñadoras Metadecidim.

Con una operativa híbrida, dicha comunidad se apoya en el espacio virtual meta.decidim.org⁹³, y se estructura a través de una asamblea general, diferentes laboratorios de investigación y un congreso anual celebrado desde 2017, el Decidim Fest (y a cuyas ediciones de 2023 y 2024 he podido acudir como observadora participante). Todo ello ha permitido la rápida expansión de una «relación plataforma-comunidad [que] encarna una importante dinámica estructurante reflexiva y recursiva», sintetizada en la articulación entre «un testado más profundo del *software*, o testado político, y una construcción más profunda de la comunidad, o testado técnico» (Barandiaran *et al.*, 2024, p. 91).

Teniendo presente aquel recordatorio de Antonio Lafuente (2007, p. 16) sobre «cómo las tecnologías y las comunidades se coproducen de una forma tan sutil y profunda que el esfuerzo de distinguir entre los aspectos técnicos y los sociales sólo conduce a la melancolía», a continuación propongo retomar la conceptualización que Chris Kelty (2008/2019a) ofrece del *software* libre como un «*sistema técnico experimental de carácter colectivo* [...] cuya infraestructura es Internet y cuyas “hipótesis” conciernen a la reorientación del saber y el poder» (p. 78). Con ello pretendo fundamentar lo decisivo del «compromiso

⁹² Véase: <https://www.decidim.barcelona/processes/metadecidim>

⁹³ Véase: <http://meta.decidim.org/>

recursivo» (Kelty, 2008/2019a, p. 427) de Metadecidim desde la interpretación de esta plataforma como otra de esas «modulaciones» que «se dan cada vez que alguien aprende cómo funciona algún componente del *software* libre y se pregunta: “¿Puedo experimentar estas prácticas en algún otro ámbito?”» (Kelty, 2008/2019a, p. 78).

Para ello, Kelty propone cinco *prácticas* que, en su contingencia y evolución constante, componen el *software* libre a finales de los 90 y hoy nos ayudan a caracterizar sus modulaciones (en este caso, Decidim) sin reducirlas «a una mera repetición sin diferencia» sino preservando (en este caso, a través de Metadecidim) el «atributo más potente y distintivo» del *software* libre, su carácter adaptativo, emergente [y] público» (Kelty, 2008/2019a, p. 426):

1) Creación de un movimiento: Definido como las prácticas de argumentación y discrepancia (hasta el punto de la ruptura) sobre el significado del *software* libre a través de las cuales sus participantes se van percatando de la coherencia de sus diversos proyectos. Esta práctica llega al final del proceso permitiendo volver las otras cuatro «legibles, replicables y modificables» (Kelty, 2008/2019a, p. 426). Aunque la idea de que en el *software* libre se «comparten primero prácticas y luego ideologías» (Kelty, 2008/2019a, p. 196) no encaja con la genealogía de Decidim en el *hacktivismo*, el 15M y las candidaturas municipalistas, la trayectoria de Metadecidim sí permite establecer reveladores paralelismos. Así, recordemos cómo su germen surgió entre el lanzamiento basado en Cónsul y el nuevo Decidim, y dentro de un momento en el que las “discrepancias sobre el significado de la participación democrática virtual” con el equipo madrileño aconsejaron una “ruptura” acompañada, a su vez, de un proceso participativo de reflexión e intervención que permitió salir del *impasse* de la mano de una comunidad emergente de (co)diseñadores de la nueva plataforma (Barandiaran *et al.*, 2024, p. 89). Además, Metadecidim procura desde sus inicios articular y expandir las prácticas de argumentación mediante la mencionada organización en una asamblea general, los distintos laboratorios de investigación y el Decidim Fest, todo ello apoyado desde meta.decidim.org (Barandiaran *et al.*, 2024, pp. 90–91).

Finalmente, cabe enmarcar en estos mismos debates democráticos el crucial proceso de gobernanza participativa lanzado por la comunidad, el cual desemboca en la Asociación Decidim. Aquí de nuevo vemos cómo se anticiparon al posible *impasse* derivado de hipotéticos (y finalmente no producidos) cambios en la Alcaldía tras las elecciones municipales de 2019 para garantizar, no solo la libertad del código fuente y la (siempre relativa) autonomía operativa y financiera sobre la plataforma y la marca Decidim, sino su propia pervivencia como comunidad democrática no expuesta a cercamientos partidistas o corporativos, ni restringida a procedimientos gubernamentales:

Es este hecho el que supone la confirmación más rotunda de que nos encontramos ante un público recursivo, un tipo de público que está tan implicado con los medios prácticos materiales para convertirse en público como con cualquier debate público dado (Kelty, 2008/2019a, p. 196).

2) Compartición de código fuente: Tras esta síntesis de Metadecidim como «público recursivo», no deberíamos dar por obvio que la modulación de esta segunda práctica se reduce a compartir el código fuente, por más fundamental que ello sea. Así, si asumimos que, lejos de que la información quiera ser libre, es la (nada obvia) práctica de su compartición la que «produce su propio tipo de orden moral y técnico» con la consecuencia de que «la información hace que las personas quieran libertad» (Kelty, 2008/2019a, p. 201), podemos defender que los recursos (también informativos) que Decidim habilita a compartir van mucho más allá.

De entrada, la amplia implantación gubernamental de Decidim desde su lanzamiento facilita la compartición con la ciudadanía de parcelas (si hay voluntad política) de los presupuestos públicos y de la planificación urbana. Junto a esta apertura de las dinámicas de decisión de arriba a abajo, Decidim también ayuda a compartir las que parten desde abajo, como la transparencia y vigilancia ciudadana, además de la iniciativa legislativa y la gestión de servicios públicos, sin olvidar la ejecución de algunas de estas políticas, llegando a la propia constitución de «procomunes urbanos» gestionados parcial o totalmente por la ciudadanía organizada (Barandiaran *et al.*, 2024, p. 46). Finalmente, y al margen del ámbito estatal, Decidim impulsa la compartición de «dinámicas de abajo a abajo» entre diversos proyectos ciudadanos, centros sociales autoorganizados o movimientos reivindicativos. Con ello se apunta a «procesos diagonales» de toma de decisión en línea como la propuesta de *Extinction Rebellion* de asambleas ciudadanas climáticas (Barandiaran *et al.*, 2024, p. 47).

3) Concepción de sistemas abiertos: La referida compartición expansiva asistida por Decidim revela una práctica de disputa por el significado de la participación democrática similar a la «figuración» de sistemas (en este caso, gobiernos) abiertos que explora Kelty (2008/2019a, p. 390):

Cuando el *software* libre funciona como un patrón para proyectos [...], lo hace literalmente, al permitirnos trazar una forma de práctica conocida (la del *software* libre) sobre un trasfondo menos conocido y aparentemente caótico para ver donde encajan las formas y donde no.

En Decidim, esta práctica de figuración arranca con tres precedentes cruciales: por un lado, la divisa

«*software* libre para una sociedad libre» ha marcado desde temprano la concepción de este movimiento por su principal filósofo (Stallman, 2002/2004); por otro, la promoción de Decidim por el gobierno de Barcelona en Comú surge de la ola de impugnación democrática radical que el 15M cataliza en las plazas y calles de toda España desde 2011, y donde se ensaya un «proceso ciberorganizativo» que prefigura la «transición a una sociedad en la que las instituciones del común son hegemónicas respecto a las instituciones del capital» (Sánchez Cedillo, 2021, p. 125), y por último de su convicción de que el código generado con dinero público debe ser libre (*public money, public code*). Pero más allá, los impulsores de Decidim conciben la superación de la crisis de la democracia liberal representativa mediante una «alianza democrática público-común» (Barandiaran *et al.*, 2024, p. 49) que redistribuye las diversas formas de poder y capital. Con ello, aspiran a conjurar la deriva tecnocrática neoliberal de las instituciones públicas y a transformarlas en línea con un orden moral y técnico alternativo que Calleja-López (citado en Barandiaran *et al.*, 2024, p. 49) denomina «tecnoacracia»:

un activo trabajo tecnopolítico para subvertir las jerarquías y formas de poder que operan en los campos político, técnico y, potencialmente, en otros, mediante la producción y puesta en práctica de nuevas mediaciones y formas de deliberación, decisión y acción participativas.

4) Redacción de licencias de *copyright*: Al igual que la «controversia de EMACS» (Kelty, 2008/2019a, pp. 289–294) marcó la invención de la GPL, también Decidim demuestra «una aguda conciencia del punto ciego de los sistemas abiertos» (Kelty, 2008/2019a, pp. 289–294) de participación ciudadana, el sabotaje legal para vaciarlos de *decisividad*, y procura atajarlo con la redacción de otro tipo de licencias.

Para empezar, los promotores de Decidim se revelan una vez más como público recursivo al dotar a la plataforma de pleno reconocimiento legal en un Reglamento de Participación Ciudadana (RPC) de Barcelona cuyas reformas de 2017 y 2022⁹⁴ se desarrollaron mediante procesos participativos en la propia decidim.barcelona. No obstante, el encaje reglamentario de esta «tecnoacracia» ha chocado con la oposición de poderosas instancias políticas y económicas. El mayor sabotaje, que acabó con la suspensión del primer reglamento por el Tribunal Superior de Justicia de Cataluña en 2019, atacó la facilitación de la convocatoria de consultas municipales vinculantes (con base en Decidim) y fue promovido por el Gobierno estatal (que reclamaba derecho a veto con el trasfondo del *procès* independentista) y por la multinacional Agbar, que vio amenazada su gestión privada del servicio del

⁹⁴ Véase: <https://www.decidim.barcelona/processes/ReglamentParticipacio>

agua de Barcelona por la intencionalidad que había de lanzar un referéndum para su remunicipalización (Barandiaran *et al.*, 2024, pp. 112–113).

Con todo, lo más similar a una licencia que ha redactado la comunidad de Decidim es el «contrato social» (Barandiaran *et al.*, 2024, pp. 69–74), que sintetiza los principios fundamentales detallados en el Capítulo 8 del citado RPC y requiere que todos los gobiernos, instituciones y personas que adopten la plataforma se comprometan con ellos. Esta modulación legal orientada a conjurar el (auto)sabotaje democrático del *participatory washing* es la mejor prueba de que la adscripción de Decidim al *software* libre no puede reducirse a una cuestión de licencias sino que se efectúa en las prácticas de Metadecidim como un público recursivo que promueve un contrato social y vela por su cumplimiento.

A mi juicio, esta modulación legal orientada a conjurar el (auto)sabotaje democrático del *participatory washing* es la mejor prueba de que la adscripción de Decidim al *software* libre no puede reducirse a una cuestión de licencias (como sugiere la redacción del primer requisito) sino que se efectúa en las prácticas de Metadecidim como un público recursivo que (como hace la FSF con la GPL) promueve un contrato social y vela por que se cumpla.

Finalmente, la citada constitución de la Asociación Decidim es otra buena prueba de esta modulación legal, sobre todo por lo que respecta a la consiguiente redacción de acuerdos institucionales: por un lado, con el Ayuntamiento de Barcelona y el Consorcio Localret (en 2019 y renovado en 2023) para garantizar que el código fuente, la marca y los datos de la plataforma permanezcan libres bajo la gestión de la comunidad de Metadecidim; y por otro, con el mismo Ayuntamiento y la Generalitat de Cataluña (en 2021) para asegurar la financiación pública sin la cual la pervivencia del proyecto y su comunidad se vería amenazada, en línea con lo que apunta Kelty (2008/2019a, pp. 70–71): «La independencia de los públicos recursivos respecto del poder no es absoluta, sino provisional y estructurada en respuesta a la estratificación históricamente constituida de poder y control en el seno de las infraestructuras informáticas y comunicativas».

5) Coordinación de colaboradores: La clave de esta quinta práctica es que «privilegia la *adaptabilidad* sobre la planificación» (Kelty, 2008/2019a, p. 317). En el caso de Decidim, esta «dirección pública crítica y adaptativa de una iniciativa colectiva» se articula mediante una original combinación de dos elementos: por un lado, el conocido sistema de control de versiones de *software* libre GitHub⁹⁵, donde se publica el código fuente y su documentación y los desarrolladores se organizan para implementar sugerencias de mejoras; y por otro, una deliberación menos técnica en Metadecidim, donde dichas

⁹⁵ Véase: <https://github.com/decidim/>

sugerencias son propuestas y, tras analizar su viabilidad (política, técnica y financiera), aprobadas o rechazadas. De este modo, una vez que se reciben sugerencias o se consignan modificaciones al código y estas son aprobadas, desde GitHub se ejecuta su desarrollo y se prepara la publicación de una actualización de Decidim, invitando a su descarga.

Si hablamos de adaptabilidad, eso sí, sorprende que los promotores de Decidim omitan que el código de GitHub *no es libre* y despachen en unas líneas (Barandiaran, 2019, p. 185) las implicaciones de su adquisición en 2018 por Microsoft, que refuerza así el desplazamiento de su cuasimonopolio hacia la explotación de (y en) centros de datos cada vez más insostenibles (Broca, 2020). Tal falta de cuestionamiento de este límite al *compromiso recursivo* de Metadecidim no deja de ser históricamente irónico si recordamos cómo Keltz (2008/2019a, p. 384) narra la forja de la plataforma git original al calor de los debates sobre «la profundidad de recursión adecuada» para el *software* libre. Una adaptación más adecuada de dichos debates a la actualidad puede encontrarse en los experimentos con repositorios distribuidos basados en GitLab que representan Framagit (Didry, 2016) o LaForgeEdu, albergado y promovido por el Ministerio de Educación Nacional francés para toda la comunidad educativa del país⁹⁶.

⁹⁶ Véase: <https://docs.forge.apps.education.fr/>

5.3. Privacidad y ofuscación selectiva para un procomún de datos a través de Decidim

5.3.1. Privacidad por diseño

El proyecto Decidim tiene un firme compromiso con la confidencialidad de los datos personales, el cual consta en su mencionado contrato social, de obligado cumplimiento para toda institución, grupo social o miembro que instale o haga uso de la plataforma. De esta manera, en el punto cuatro del contrato se explicita que:

Se garantizará en todo momento la confidencialidad y privacidad de los datos personales que las personas puedan proporcionar para participar en cualquiera de las funcionalidades o posibilidades de participación que la plataforma proporcione. Los datos personales no se transferirán, en ningún caso, a terceros. Tampoco se utilizarán más allá de lo estrictamente necesario para el registro de usuarios y mejoras en la usabilidad de la plataforma. Siempre que la tecnología de la plataforma lo permita, la expresión de las preferencias políticas o la voluntad en los procesos de toma de decisiones seguirá siendo inaccesible incluso para el administrador de la plataforma o el servidor o servidores que la alojan. (Contrato social de Decidim, s.f., punto 4).

He aquí una constatación de la afirmación de los impulsores de la plataforma (Barandiaran *et al.*, 2024, p. 73) de que la protección de la privacidad de las participantes es un principio de diseño en Decidim. De esta manera, la configuración por defecto de la plataforma permite a las usuarias navegar en una instancia determinada sin estar registradas, así como realizar comentarios y hacer propuestas bajo el seudónimo que ellas elijan, todo ello con el objetivo de asegurar la accesibilidad de la actividad en la plataforma y nutrir la participación y la inteligencia colectiva.

Sin embargo, desde los inicios surgieron dudas sobre cómo mantener este derecho a la privacidad, compaginándolo con la necesidad de verificar, por ejemplo a la hora de las votaciones, que a cada persona registrada le correspondía un único voto (Barandiaran, 2017). Dicho de otra forma, las participantes debían poder permanecer pseudoanónimas a la vez que eran verificadas. Para llevar esto a cabo, en Decidim se mantienen los datos personales que identifican a una usuaria como portadora de derechos separados de su nombre de usuaria y del identificador de la base de datos en Decidim.

He aquí la razón de que, como he explicado anteriormente, una vez que te registras como participante,

puedas verificar tu identidad de diferentes maneras. Es importante recalcar aquí que esto suele implicar proporcionar información personal como prueba de quién eres. Dicha información se revisa y se compara con un registro de personas (como en el caso del censo en una ciudad) para asegurarse de que coincide con los datos de la participante. Sin embargo, tu información personal necesaria para la verificación no se almacena, solo se usa momentáneamente para estos fines.

Para que esto sea posible, Decidim almacena un *hash* mediante un método de cifrado que transforma registros de datos y caracteres de longitud arbitraria en resúmenes criptográficos compuestos de valores compactos y fijos que no se pueden revertir a la información de entrada— de un identificador personal junto con un código secreto que solo conoce el servidor que almacena los *hashes*. De esta manera, cuando necesitas autenticarte en la plataforma e introduces tu identificador personal pertinente, este no es comprobado con una copia almacenada del mismo (por ejemplo, una contraseña comprobada en un almacén de contraseñas en texto claro) sino que es pasado por una función *hash* criptográfica de una sola vía (no reversible sin invertir muchos decenios o siglos en ello). Como resultado, se obtiene una misma cadena de caracteres cifrados que, a continuación, basta confrontar con una base de datos disociada donde se guardan los *hashes* de todos los usuarios registrados hasta dar con el resumen criptográfico que coincida con el generado al darte de alta por primera vez. Al fin y al cabo, se trata de rescatar aquella búsqueda de «un fenómeno digital con las mismas propiedades que una firma escrita» que emprendieron los pioneros de la criptografía de clave pública, Diffie y Hellman (1976, p. 649): «Debe ser fácil para cualquiera reconocer la firma como auténtica, pero imposible producirla si no es el legítimo signatario. Llamaremos a cualquiera de estas técnicas *autenticación unidireccional*. [U]na verdadera firma digital debe ser reconocible sin ser conocida».

5.3.2. Plan de Privacidad de Decidim

Con el propósito de mejorar el tratamiento de los datos y la privacidad de las usuarias del primer Decidim —todavía centrado en la plataforma desarrollada para el Ayuntamiento de Barcelona— en diciembre de 2016 la empresa Eticas Consulting, dedicada al análisis de los factores que influyen en el desarrollo y uso de la tecnología vinculados a cuestiones sociales, legales y éticas, presentó el *Plan de Privacidad de Decidim Barcelona*.

Con el fin de diseñar dicho plan, la consultora llevó a cabo una Evaluación de Impacto sobre Datos Personales (EIPD) a través del análisis de la plataforma, el uso de diferentes cuestionarios y el análisis de la normativa vigente. En tal tarea, Eticas (2016, pp. 18-19) siguió una metodología basada en fuentes de investigación secundarias como la netnografía, esto es, el estudio y navegación por la plataforma así

como la consulta de documentación propia de la organización, como el Plan de Desarrollo Decidim Barcelona v.1.0⁹⁷, elaborado por la Concejalía de Participación y Distritos del Ayuntamiento de Barcelona. Junto a ello esta labor se apoyó en la celebración de diversas reuniones con actores clave vinculados directamente con el desarrollo de la plataforma. Así como el empleo de fuentes de investigación primarias para obtener información sobre cómo funciona la plataforma, cómo se mueven los datos y cómo participan las usuarias tales como: para evaluar cómo se usan los datos personales, se envió a actores clave un formulario genérico sobre la cuestión. También se distribuyeron cuestionarios simples para entender otros aspectos importantes en lo referente a protección de servicios y aplicaciones *web*, correo electrónico, y otras medidas. Además, para conocer la opinión de las personas usuarias, se repartieron encuestas anónimas en el evento Metadecidim celebrado en el MACBA los días 25 y 26 de noviembre de 2016.

Una cuestión muy relevante sobre la que hacían especial énfasis tiene que ver con el momento de registro de una nueva participante. La cuestión radica en que, una vez vas a realizar tu registro, desde la plataforma te solicitan que elijas un nombre de usuario que no tiene por qué corresponder con tu nombre real. Es, por tanto, decisión de la persona que se registra elegir si su alias será o no potencialmente asociable a su identidad, lo que puede generar futuras cuestiones que comprometan su privacidad, tal y como explica Éticas (2016, p. 24):

no es lo mismo registrarse como “JosepTorrent1976” que como “anonimo223”. Esta cuestión no está sólo relacionada con la publicación de comentarios en la plataforma, sino además con el hecho de que los nombres de usuario estén indexados mediante la existencia de un buscador en el apartado de “visualizaciones”. El incremento de la actividad de un usuario puede recaer en el enriquecimiento de las posibilidades de perfilar su comportamiento. [...] En resumen, la combinación entre posibilidades de identificación de un usuario/a y rastreo de su actividad en la plataforma, puede generar efectivamente la posibilidad de crear perfiles (relacionables con opiniones de carácter político) y llevar a cabo seguimientos de la actividad de dicho usuario/a.

Dado que esto es decisión de la persona que se registra, la consultora instaba a la plataforma a informar sobre las consecuencias de la elección de uno u otro nombre de participante.

Por último, con el fin de fomentar la privacidad, se aconsejaba distinguir de manera clara entre las dinámicas de participación perceptibles en la página *web* y los recursos capaces de crear sistemas de

⁹⁷ Véase: <https://github.com/AjuntamentdeBarcelona/decidim-doc-plannedesarrollo/blob/master/plan-de-desarrollo.md>

información organizados e indexables, como bases de datos y archivos de datos abiertos. Siempre que fuese factible, se instaba a realizar procesos de disociación en los archivos que incluyesen información y listados que reflejan la actividad de la plataforma. Esto implicaba reevaluar la indexación de contenidos en buscadores, dado que podían provocar situaciones de reidentificación que perjudicasen la privacidad de las participantes.

5.3.3. El proyecto DECODE y el caso del piloto Democracia Digital y Datos Comunes (DDDC)

Enmarcados en un escenario de creación e implementación de normativas en la UE en torno a la seguridad de las comunicaciones y la privacidad de los datos, como el RGPD analizado en el Capítulo 3, entre los años 2016 y 2018 las urbes más importantes de Europa también buscaron construir nuevas habilidades estratégicas en el ámbito de la gobernanza y administración de datos, promoviendo la importancia de potenciar la privacidad en beneficio de sus habitantes (Bria y Morozov, 2018). Dentro de este interés por los citados temas de privacidad, derechos digitales y soberanía de los datos, se destacaron significativas oportunidades para que los gobiernos municipales interviniesen en la protección de los intereses de los ciudadanos, incluyendo la salvaguarda de las infraestructuras de datos públicos o basados en bienes compartidos (Bria, 2018).

De esta manera, a través del concepto de “*data commons*” (que traduzco como “procomún de datos”), se establecía el valor de los datos para obtener beneficios colectivos y compartidos (Monge *et al.*, 2022, p. 9). La creación de dicho procomún de datos requería de un conjunto de nuevos protocolos que regulasen el uso compartido de los mismos, respaldados por nuevos acuerdos contractuales tanto con los ciudadanos como con los proveedores de servicios (Monge *et al.*, 2022, p. 14).

El proyecto DECODE

Bajo esta idea nació el DEcentralised Citizen Owned Data Ecosystem, conocido como DECODE⁹⁸, un proyecto de ámbito europeo concebido y coordinado por Francesca Bria (Monge *et al.*, 2022, p. 12) y gestionado por Nesta, una organización benéfica del Reino Unido. Financiado por el Programa Horizonte 2020 de la UE con un total de 5 millones de euros, esta iniciativa fue desarrollada entre enero de 2017 y diciembre de 2019 por diferentes agentes (entre tecnólogos, sociólogos y desarrolladores, instituciones y universidades, entre otros) que implementaron programas piloto en dos ciudades europeas: Barcelona y Amsterdam. Con este proyecto se buscaba crear herramientas de *software* abierto que brindasen a las personas la capacidad de controlar y compartir datos personales

⁹⁸ Véase: <https://decodeproject.eu/index.html>

según sus propios términos.

De manera más detallada, según su *Libro Blanco* (Roio *et al.*, 2018, p. 6), DECODE fue un proyecto experimental que buscaba ofrecer alternativas prácticas a la forma en que gestionamos nuestros datos personales e interactuamos en Internet, a través del desarrollo de tecnologías de uso sencillo que permitieran a las personas controlar sus datos personales, dándoles la capacidad de decidir cómo se comparten. De esta manera, el proyecto centraba sus esfuerzos de investigación y desarrollo en nociones novedosas de confianza y privacidad que se pudiesen poner en práctica en nuevos marcos de gobernanza y modelos económicos innovadores basados en los bienes comunes digitales.

A través de los citados proyectos piloto desarrollados en Ámsterdam y Barcelona, y con la coordinación de Francesca Bria en calidad de Directora de Tecnología e Información (CTIO, por sus siglas en inglés) de la capital catalana, DECODE exploró cómo construir una economía digital donde los datos generados y recopilados por los ciudadanos, el IoT y las redes de sensores estuviesen disponibles para un uso comunitario más amplio, con las protecciones de privacidad adecuadas. Su objetivo era sentar las bases de un nuevo enfoque de los datos, mediante el cual *startups*, ONGs, PYMES, cooperativas y comunidades locales los aprovecharan para crear aplicaciones y servicios que respondiesen a sus necesidades y a las de la comunidad en general. Bajo esta visión, las ciudades tenían un papel fundamental como custodios de estos nuevos derechos digitales de los ciudadanos. De esta manera, según su página *web*⁹⁹, entre Barcelona y Ámsterdam se desarrollaron cuatro programas piloto:

El primero, corresponde al desarrollo de la democracia digital y los datos comunes. En este programa participaron el Ayuntamiento de Barcelona y la plataforma Decidim, la cual integró un módulo DECODE que permitía firmar peticiones de forma anónima, mientras respetaba los requisitos de autenticación unidireccional (Diffie y Hellman, 1976) que precisaba la plataforma para llevar a cabo ciertas acciones. Este nuevo sistema para peticiones ciudadanas ofrecía a las personas una capacidad de decisión de una manera más granular sobre sus datos, mejoraba la privacidad —a través de la aplicación también llamada DECODE—, permitía compartir y visualizar datos —a través del panel de control de otra aplicación denominada BarcelonaNow (BCNOW)— y mantenía los estándares de transparencia, gracias a la tecnología de contabilidad distribuida (DLT, por sus siglas en inglés) de DECODE. El programa piloto también abrió un proceso deliberativo y participativo sobre la política y la economía de los datos, y sobre cómo Barcelona podría convertirse en una ciudad democrática a través del procomún de datos.

⁹⁹ Véase: <https://decodeproject.eu/pilots.html>

De esta manera, Calleja-López (2018, pp. 44-45) explica que las tecnologías DECODE comprenden un conjunto complejo de herramientas e infraestructuras digitales compuesto por una cartera digital, una DLT, una red de nodos y un panel de control. Veamos algunas características básicas de cada una:

Para empezar, la cartera digital de DECODE, cercana a las clásicas propuestas minimalistas de «cartera virtual» (Lessig, 2006/2009, pp. 98-101), consistía en una aplicación móvil que servía como interfaz para el almacenamiento y la gestión de datos de forma segura, además de funcionar como punto de acceso a la infraestructura DECODE. Por su parte, la DLT se componía de un conjunto de datos digitales replicados, compartidos y sincronizados que se distribuyen geográficamente en múltiples sitios, países o instituciones, con una administración igualmente distribuida. Es en esta arquitectura de *software* distribuida donde se registraron las reglas concretas (los llamados contratos inteligentes) y las operaciones de datos durante el proceso de firma en el piloto. Esta tecnología permitía que las firmas se almacenasen, auditasen y contasen, y también que se gestionase la información demográfica compartida. En definitiva, funcionaba como un registro público y entre pares de las reglas y las operaciones que tenían lugar durante el proceso de firma. Por otro lado, la red DECODE era un conjunto de nodos que albergaban la DLT de DECODE, los elementos de interacción con la cartera digital y las distintas piezas de *software* que se empleaban.

El segundo programa piloto que se desarrolló en la ciudad de Barcelona fue el relacionado con la gobernanza de datos de ciencia ciudadana. En este programa, los residentes utilizaron sensores ambientales, ubicados dentro de sus casas y en su vecindario, que registraban información como los niveles de ruido y la contaminación ambiental. La tecnología DECODE les permitió compartir estos datos cifrados de forma anónima con sus comunidades y en sus propios términos. El piloto llevó a cabo sesiones para capacitar y apoyar a las participantes, ayudándoles a configurar y usar los sensores para recopilar y analizar datos que influirían en la toma de decisiones a escala municipal. El programa abordó los desafíos técnicos de recopilar y almacenar un flujo de datos captados por los ciudadanos, al mismo tiempo que permitió a los mismos controlar qué información se compartía con quién y bajo qué condiciones. Esta iniciativa se llevó a cabo en colaboración con las organizaciones comunitarias de Barcelona Ideas for Change¹⁰⁰ y FabLab Barcelona¹⁰¹.

Vinculada a estos dos primeros programas aparece la mencionada aplicación BCNOW, que a través de un panel interactivo vinculado a Decidim permitía agregar y combinar de forma sencilla una serie de datos generados por los ciudadanos. BCNOW tenía como objetivo que los datos no solo estuviesen

¹⁰⁰Véase: <https://ideasforchange.com/>

¹⁰¹Véase: <https://fablabbcn.org/>

disponibles para los ciudadanos y que estos pudiesen compartirlos de manera responsable, sino que también fuesen útiles para otros propósitos, al proporcionar un entorno visual poblado de interfaces interactivas para la exploración y visualización de datos.

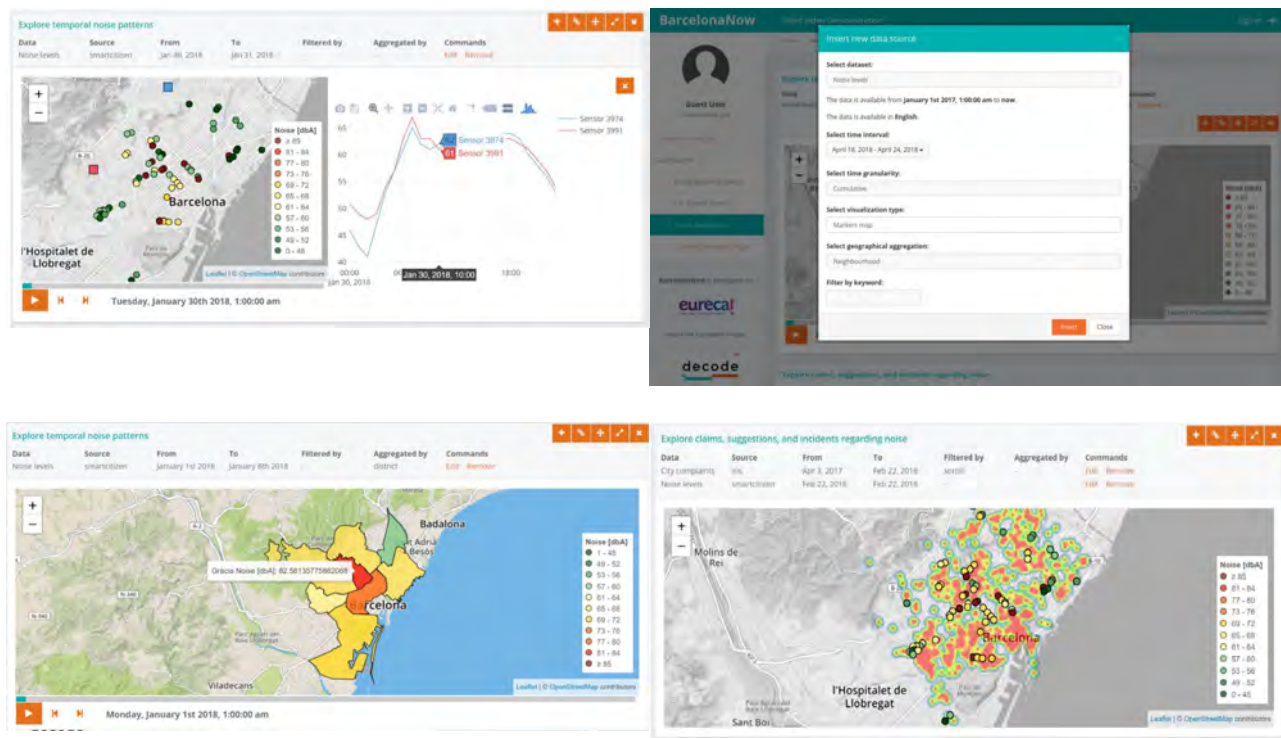


Figura 76. Capturas de pantalla del proyecto BCNOW. Fuente: Marras y Laniado, 2018.

De esta manera, los usuarios podían crear paneles personalizados, mover complementos entre ellos, y seleccionar el nombre de la fuente de datos que visualizar y otros parámetros adicionales. Dicho panel estaba concebido para integrar datos públicos de fuentes del Ayuntamiento de Barcelona, como los datos de los sensores Sentilo¹⁰² y los datos de bicicletas compartidas de los datos abiertos del municipio, con algunas fuentes externas, como los datos extraídos de Airbnb (Marras y Laniado, 2018, párr. 12-21).

De haber tenido esta iniciativa la continuidad deseada pero no alcanzada, el Ayuntamiento de Barcelona planeaba ampliar el catálogo de datos existente con nuevas fuentes de datos públicos y con los datos privados de los usuarios de la infraestructura DECODE (Bass *et al.*, 2018, p. 60).

Por su parte, en la ciudad de Ámsterdam se llevó a cabo un tercer programa piloto de verificación de edad con datos del censo municipal. Este dio a los ciudadanos acceso a información personal almacenada en la base de datos municipal y les permitió compartirla en un contexto diferente, tanto

¹⁰²Véase: <https://www.sentilo.io/>

online como *offline*. En el piloto, los participantes utilizaron la tecnología DECODE de credenciales basadas en atributos para demostrar su edad, lo que les permitía certificar que tenían más de 16 o 18 años sin tener que compartir otra información como su identidad completa o su número de la Seguridad Social.

El último programa piloto tuvo que ver con GebiedOnline¹⁰³, una plataforma virtual de barrios surgida en Ámsterdam en 2012. En sus inicios, el acceso a GebiedOnline se gestionaba mediante correo electrónico/contraseña o inicio de sesión de Facebook, lo que creaba dependencias no deseadas y problemas de seguridad. La junta directiva y la comunidad de Gebiedonline querían que su plataforma fuese de código abierto, inclusiva y permitiera a sus usuarios tener una capacidad de decisión de una manera más granular sobre los datos que compartían con la plataforma y con otros usuarios de la comunidad. Para lograrlo, el proyecto piloto creó y probó una función que permitía el acceso a la plataforma mediante las citadas credenciales basadas en atributos, ofreciendo varias entre las que cada comunidad podía decidir cuál aceptar.

Democracia Digital y Datos Comunes (DDDC): la intersección entre DECODE y Decidim.

El proyecto piloto Democracia Digital y Datos Comunes (DDDC) estaba orientado a implementar experimentalmente las propuestas del mencionado DECODE, esto es, a desarrollar tecnologías y herramientas que permitiesen sistemas sociotécnicos (ya sean de carácter político o económico) que diesen a las personas una mayor capacidad de decisión sobre sus datos, al tiempo que habilitasen usos que proporcionasen más beneficios colectivos a partir de ellos (Calleja-López, 2018, p. 10).

Según las entrevistas realizadas en un estudio de caso sobre el DDDC (Monge *et al.*, 2022, p. 13) uno de los desafíos clave durante el proceso de creación de Decidim fue que la plataforma no recogiera las características demográficas de los participantes con el objetivo de proteger su privacidad.

Sin embargo, esta decisión provocaba que resultase difícil saber quiénes participaban y los posibles sesgos que podían estar dándose si solo ciertos grupos o personas contribuían al desarrollo de los procesos en la plataforma. La solución que este piloto ofrecía era que, dado que DECODE desarrollaba una nueva tecnología de cifrado y almacenamiento, esto permitiría que las personas que estaban navegando o debatiendo pudiesen compartir sus características demográficas, pero mantuviesen su anonimato. Además, si las participantes lo deseaban, la plataforma podría recopilar, de manera agregada, información demográfica (distrito, edad y género) sobre quienes votaban, la cual luego podría usarse para mejorar los procesos de la misma.

¹⁰³Véase: <https://gebiedonline.nl/>

Además de perseguir una participación más respetuosa de la privacidad, el proyecto DDDC buscaba una serie de objetivos: en primer lugar, integrar la tecnología DECODE con la plataforma digital de democracia participativa Decidim con el fin de mejorar los procesos que involucrasen peticiones ciudadanas electrónicas, aportando mayor seguridad, privacidad, transparencia y enriquecimiento de datos. En segundo lugar, habilitar un espacio deliberativo en torno a políticas públicas, gobernanza y economía de los datos que con la meta de promover un mayor control ciudadano sobre los datos y su explotación en modelos orientados al mencionado procomún de datos. Y por último, se buscaba experimentar con la construcción y utilización de un banco común de datos generados sobre la marcha, para mejorar la inclusión del propio proceso participativo (DECODE, 2019, p. 16).

De esta manera, el proyecto DDDC buscó aumentar la participación de la comunidad en el ecosistema de gobernanza de datos de la ciudad mediante la colaboración con comunidades y ciudadanía, sector público y privado, así como actores provenientes de la academia. Fruto de este modelo de innovación abierta a lo largo de su desarrollo, 223 participantes emitieron 118 votos, publicaron 77 propuestas, 86 comentarios y 2 peticiones, y celebraron 8 reuniones (Monge *et al.*, 2022, p. 13).

Para Calleja-López (2018, p. 54), este proyecto piloto desplegaba dos grandes hilos conductores: la democracia digital y el procomún de datos. El primero estaba orientado a llevar a Decidim hacia un modelo de infraestructura más distribuido, que pasase de la democracia participativa a la democracia digital, y donde las personas tuviesen una mayor capacidad de decisión tanto personal como colectiva sobre sus datos. En cuanto al segundo hilo, complementaba al anterior orientándose a explotar el potencial de Decidim para avanzar la visión del proyecto DECODE de formas alternativas de gobernanza y economía de datos en una dirección democratizadora.

La ejecución del piloto implicó la instalación del *software* Decidim complementado con la tecnología DECODE en el sitio de Democracia Digital y Procomún de Datos (dddc.decode.project.eu¹⁰⁴), todo lo cual permitió la circulación de información, la deliberación, el intercambio de datos y la toma de decisiones colectivas. En cuanto a los pasos que dicha ejecución implicó para las participantes, fueron los siguientes: en primer lugar, se les invitó al evento de lanzamiento el 18 de octubre de 2018, el cual incluyó una presentación y un taller y vino precedidos de un simposio más reflexivo (los días 16 y 17 de octubre). A partir de ese día, las personas pudieron registrarse e iniciar sesión en el DDDC siguiendo el proceso habitual del *software* Decidim: una cuenta de correo electrónico era suficiente para realizar todas las actividades (proponer, comentar, etc.) excepto en la etapa de toma de decisiones que se realizaba al final del proceso participativo, en la que se hacía uso del sistema DECODE.

104 Véase: <https://web.archive.org/web/20200529063834/https://dddc.decodeproject.eu/>

Según Calleja-López (2018, p. 55), durante las primeras semanas del proceso se pidió a las participantes que rellenasen una encuesta que, junto con la actividad en la plataforma durante el proceso participativo y los datos compartidos en el paso de toma de decisiones al final del mismo, constituyó el conjunto de datos del DDDC. También podían obtener información, hacer propuestas y discutir la forma de las políticas de datos y constituir experimentalmente un conjunto de datos comunes. Durante el proceso, el citado panel de BCNNOW ayudó a visualizar los tipos de datos que se agregaban a través de la encuesta socio-demográfica y las interacciones en la plataforma, todo lo cual fue la base para acabar tomando decisiones sobre los asuntos en cuestión.

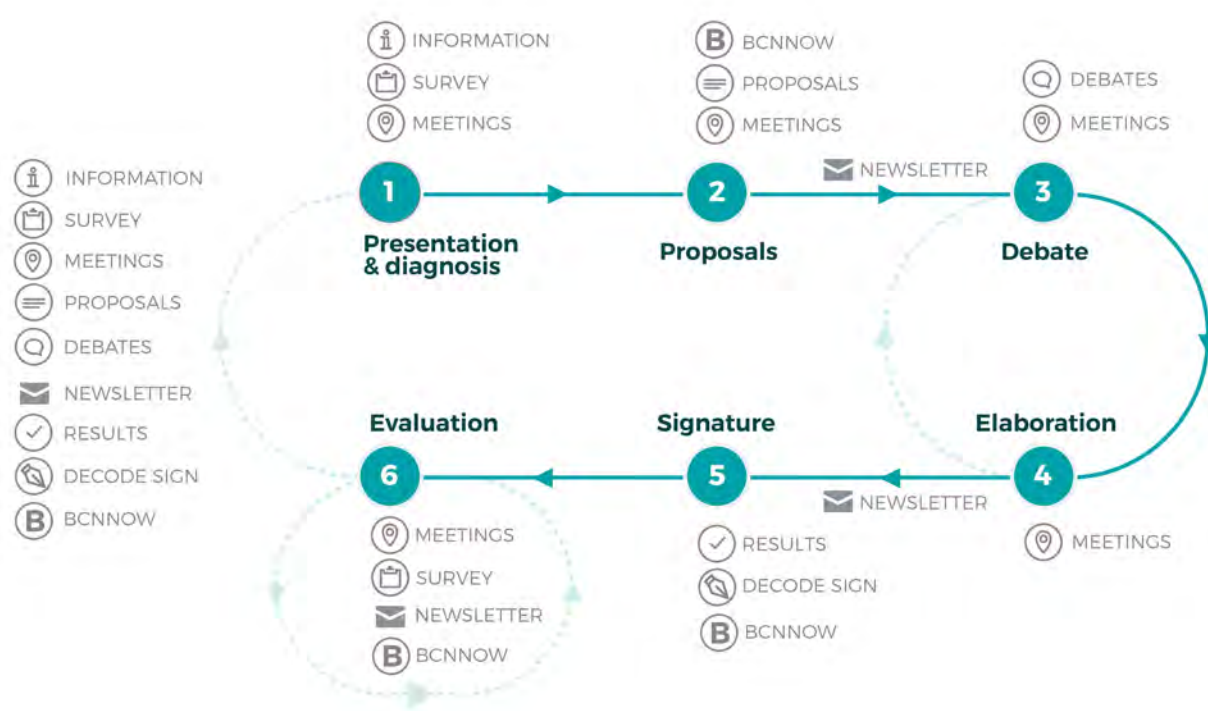


Figura 77. Resumen del proceso DDDC. Fuente:

<https://web.archive.org/web/20200529063721/https://dddc.decodeproject.eu/processes/main/>

La conexión de los diversos componentes DECODE y Decidim se logró a través de un flujo integrado, llevado a cabo por la entidad sin ánimo de lucro Alabs¹⁰⁵ (Calleja-López *et al.*, 2020, 1h16m15s), que estaba en funcionamiento durante el paso final de firma de la petición del proceso participativo. Tal y como detalla Calleja-López (2018, pp. 45-46) el proceso era el siguiente:

En primer lugar, la administradora de Decidim creaba una nueva petición en la instancia de Decidim. En este proceso, se llamaba al conector de decodificación y se creaba un nuevo objeto de petición en la

¹⁰⁵Véase: <https://www.alabs.org/>

DLT, que devolvía a Decidim un enlace a este objeto y se asociaba con la petición.

Tras esto, la participante accedía a la petición a través del sitio *web* de Decidim. Al elegir firmar una petición con DECODE, la participante era dirigida a la aplicación DECODE, donde en función del ID de la petición, se recuperaba la siguiente información de la API de Decidim: el título de la petición, la descripción, los atributos obligatorios y opcionales y la URL para adquirir un atributo obligatorio.

Mientras tanto, en la misma aplicación, se informaba a la participante de qué petición estaba firmando y qué información suya se solicitaba. Si a la participante le faltaba un atributo obligatorio (por ejemplo, residencia verificada), se la derivaba al emisor de credenciales externo. Este servicio verificaba su idoneidad para recibir una credencial (a modo de *token* o identificador que certificase que estaba autorizada a participar en el piloto o que era residente de la ciudad), la cual no se compartía con Decidim.

Una vez que todos los requisitos estaban completados, la participante podía firmar la petición con un Sí/No, los atributos obligatorios y cualquier atributo opcional que eligiese compartir. Esta información se combinaba con el estado de la petición en la DLT, y la aplicación generaba una transacción que actualizaba el recuento en dicho registro distribuido. La naturaleza de este contrato inteligente garantizaba tanto que no se trasmitiesen datos de identificación personal (sino solo agregaciones) como que la transacción y la opción Sí/No fueran imposibles de rastrear hasta la participante, ya que la aplicación se comunicaba con la DLT a través de Tor y la opción Sí/No era indescifrable para revelar la opinión o preferencia de la participante. Por otro lado, los posibles ataques de canal lateral¹⁰⁶ eran bloqueados porque la petición se contaba utilizando encriptación homomórfica¹⁰⁷, de modo que el total de cada recuento de firmas no se conocía hasta el final del proceso, aunque se podía verificar su integridad. Después de la petición, el conector de decodificación descifraba los totales finales y devolvía los resultados a la instancia de Decidim, imposibilitando a partir de entonces realizar más firmas, ya que la DLT rechazaba cualquier otra transacción.

Por último, el panel de control podía entonces cargar datos de la API de Decidim, así como resultados

¹⁰⁶«En seguridad informática, un ataque de canal lateral (*Side-channel Attack*) es cualquier ataque que se basa en la información obtenida por la implementación de un sistema informático, en lugar de en las debilidades de los propios algoritmos implementados, por ejemplo, los ataques de canal lateral se basan en el hecho de que, al funcionar los sistemas de cifrado, producen efectos físicos, y la información derivada de esos efectos puede dar pistas sobre los sistemas. En la mayoría de los casos, los ataques de canal lateral están diseñados para exfiltrar información sensible, incluidas las claves de cifrado, midiendo la coincidencia de las salidas del hardware. En concreto, estos ataques utilizan uno de estos efectos para obtener información adicional sobre los secretos de los algoritmos utilizados» (Profesional Review, 2022, párr. 2).

¹⁰⁷«El cifrado homomórfico, también llamado encriptación homomórfica por su traducción del inglés (*homomorphic encryption*), es una técnica que permite realizar operaciones matemáticas sobre datos cifrados sin necesidad de descifrarlos. Esta propiedad hace que sea posible preservar la privacidad y confidencialidad de los datos» (Gutiérrez Ruiz, s.f. párr. 7)

Una de las principales causas tiene que ver con los resultados en las elecciones municipales de Barcelona de 2019, en las que, pese a que Barcelona en Comú renovó su mandato, la pérdida de votos que sufrió hizo que para ello tuviesen que llegar a un acuerdo con el Partido Socialista Catalán (PSC), el cual asumió las competencias del área digital del Ayuntamiento. Esto tuvo implicaciones para la agenda digital lanzada en 2015, pues para Calleja-López (citado en Monge *et al.*, 2022, p. 16) la narrativa estratégica del consistorio pasó de la soberanía digital al humanismo digital, esto es de una narrativa potencialmente abierta a la política radical a una vinculada a una ética más tibia, de la centralidad de las asociaciones público-comunes a la de las asociaciones público-privadas, y de la crítica y la imaginación socioeconómicas sistémicas a los llamados limitados al cambio social. Otro añadido a esto es que, tras haber completado su mandato, Francesca Bria, coordinadora del proyecto, abandonó su puesto de



Según Monge *et al.* (2022, p. 16), pese a que DECODE fue ampliamente mencionado como una alternativa viable tanto por divulgadores como por responsables políticos y académicos, una serie de circunstancias tanto intrínsecas como externas al proyecto hizo que su piloto DDDC no llegase a implantarse definitivamente.

Una de las principales causas tiene que ver con los resultados en las elecciones municipales de Barcelona de 2019, en las que, pese a que Barcelona en Comú renovó su mandato, la pérdida de votos que sufrió hizo que para ello tuviesen que llegar a un acuerdo con el Partido Socialista Catalán (PSC), el cual asumió las competencias del área digital del Ayuntamiento. Esto tuvo implicaciones para la agenda digital lanzada en 2015, pues para Calleja-López (citado en Monge *et al.*, 2022, p. 16) la narrativa estratégica del consistorio pasó de la soberanía digital al humanismo digital, esto es de una narrativa potencialmente abierta a la política radical a una vinculada a una ética más tibia, de la centralidad de las asociaciones público-comunes a la de las asociaciones público-privadas, y de la crítica y la imaginación socioeconómicas sistémicas a los llamados limitados al cambio social. Otro añadido a esto es que, tras haber completado su mandato, Francesca Bria, coordinadora del proyecto, abandonó su puesto de

CTIO de la ciudad (Monge *et al.*, 2022, p.17).

Por último, la incorporación y escalabilidad de la tecnología pilotada a través de DECODE también enfrentó algunos desafíos. Para Calleja-López, la falta de énfasis en las ideas que sostenían el proyecto y la escasez de tiempo afectaron a su escalabilidad:

Teníamos casi todas las piezas juntas: comunidades de personas que todavía están en contacto y están haciendo muchos proyectos; teníamos la visión; de hecho, también teníamos un prototipo de la tecnología. Teníamos el elemento clave que era la conexión dentro de la ciudad y alguien que estaba absolutamente comprometido con esto... pero no pudimos cerrar finalmente el círculo y hacerlo completamente estable... Creo que cosas como financiación adicional y que Francesca (o alguien similar a ella) se quedara otro mandato eran condiciones necesarias para estabilizar el modelo DECODE (citado en Monge *et al.*, 2022, p.17).

Pablo Aragón (citado en Monge *et al.*, 2022, p.17), otra de las personas involucradas en el proyecto, dio dos posibles razones adicionales por las que el piloto desarrollado a través de DECODE no se integró completamente en Decidim: «O una falta de compromiso político o una necesidad de mayores recursos, o ambas». Otros, como Andrés Pereira de Lucena (citado en Monge *et al.*, 2022, p.17), uno de los desarrolladores de Decidim, encontraron que la tecnología desarrollada bajo DECODE planteaba algunos desafíos de usabilidad:

El problema con la tecnología desarrollada bajo DECODE era que, debido a cómo opera *blockchain*, los participantes tenían que usar una aplicación móvil externa y descubrimos que esto era demasiado engorroso, y lo que queríamos tener son menos pasos para el proceso de votación para permitir la escalabilidad y una mejor experiencia de usuario...

A pesar de estos desafíos, la experiencia de Barcelona ya ha influido en la estrategia y la política de la UE en materia de datos (Monge *et al.*, 2022, p. 18), hasta el punto que la Comisión Europea ha declarado que utilizará sus poderes de convocatoria y financieros para «reforzar la “soberanía tecnológica de Europa para una economía ágil en materia de datos”» (EU Data Strategy 2020, citado en Monge *et al.*, 2022, p. 18). Este documento también hace referencia expresa a DECODE como una de las herramientas innovadoras que permite a los ciudadanos compartir sus datos al tiempo que protege sus derechos, y declara la necesidad de seguir invirtiendo en entornos que permitan que esas innovaciones prosperen (Monge *et al.*, 2022, p. 18).

5.4. Debates acerca de la privacidad y la protección de datos en Metadecidim

Como avancé antes, la comunidad que integra Metadecidim está conformada por personas y organizaciones que emplean y/o desarrollan el *software* Decidim y que se organizan en la plataforma homónima en torno a diferentes secciones: la primera se titula “participa” y se compone de una serie de “procesos” vinculados a mejorar la plataforma, con lugares para proponer nuevas funcionalidades, notificar errores o traducir a otros idiomas los documentos y componentes de la plataforma. Por otro lado, emplean los espacios “asambleas” para realizar encuentros de la comunidad y organizar diferentes grupos de trabajo, así como para aglutinar todas las actividades relativas a su organización en “cómo nos organizamos”. Mediante el uso de espacios de “jornadas” promocionan y organizan los *Decidim Fest* anuales y recopilan la información expuesta en ellos. También organizan otro tipo de encuentros en torno a diferentes temáticas, cuentan con un espacio de noticias y un canal externo de mensajería instantánea.

A través de una búsqueda sobre temas relacionados con la privacidad, el tratamiento de los datos personales o el RGPD en la plataforma de Metadecidim, concretamente en la sección de “propuestas de nuevas funcionalidades”, he encontrado un total de 12 que resumo en la siguiente tabla:

Título	Fecha	Enlace Metadecidim	¿Propuesta implementada?	Desarrollador	Versión disponible	Enlace Github
Cumplir con el Reglamento General de Protección de Datos (RGPD) de la UE	16/04/18	https://meta.decidim.org/processes/roadmap/f/122/proposals/12416	Sí	Codi Tramuntana	0.13	https://github.com/decidim/decidim/issues/3320
RGPD / Portabilidad de datos - Metadatos de autorizaciones de usuario	24/08/19	https://meta.decidim.org/processes/roadmap/f/122/proposals/14756	No			
Notificaciones del censo CSV o autorizaciones automáticas	20/09/19	https://meta.decidim.org/processes/roadmap/f/122/proposals/14798	No			
RGPD / Derecho al olvido - Metadatos de autorizaciones de usuario	10/10/19	https://meta.decidim.org/processes/roadmap/f/122/proposals/14850	No			
Opciones de privacidad del usuario y capacidad para desactivar perfiles públicos	24/02/21	https://meta.decidim.org/processes/roadmap/f/122/proposals/16247	No			
RGPD - Derecho al olvido - Capacidad de los administradores para eliminar cuentas de usuario	25/02/21	https://meta.decidim.org/processes/roadmap/f/122/proposals/16249	No			

Cumplimiento del RGPD: eliminación automática de cuentas de usuarios inactivos	19/01/22	https://meta.decidim.org/processes/roadmap/f/122/proposals/16922	Sí	Open Source Politics	Módulo externo	https://github.com/OpenSourcePolitics/decidim-module-cleaner
Mejorar el área de texto de consentimiento de la Política de privacidad con un resumen	30/12/99	https://meta.decidim.org/processes/roadmap/f/122/proposals/16971	Sí	Platoniq	0.28	https://github.com/decidim/decidim/pull/10166
Política de privacidad para seres humanos		https://meta.decidim.org/processes/roadmap/f/122/proposals/16972				
RGPD - Derecho a oponerse al tratamiento de datos personales	23/10/23	https://meta.decidim.org/processes/roadmap/f/122/proposals/17588	No			
Procesos de archivado y anonimización [comodidad administrativa + trazabilidad + RGPD]	17/05/24	https://meta.decidim.org/processes/roadmap/f/122/proposals/17728	No			
Compatibilidad de la plataforma con el RGPD	08/01/25	https://meta.decidim.org/processes/roadmap/f/122/proposals/17958	No			

Tabla 8. Resumen de las propuestas de nuevas funcionalidades relacionadas con la privacidad y/o la protección de datos.

Fuente: Elaboración propia a partir de búsquedas en la plataforma <https://meta.decidim.org/>. Recuperado el 8 de enero de 2025.

Si atendemos a aquellas propuestas que han sido implementadas, la primera surge el 16 de abril de 2018, poco más de un mes antes de la implantación del RGPD, y en ella una participante hablaba de la necesidad de realizar una revisión por parte de Decidim para cumplir con el RGPD de la UE, más concretamente en lo que afecta al perfil del participante y a la configuración personal. Esta propuesta fue finalmente desarrollada por la empresa de desarrollo de *software* Codi 'Tramuntana'¹⁰⁸ con la financiación del Ayuntamiento de Barcelona, y, tras ser revisada por el equipo de producto de Decidim, se incluyó en la versión 0.13.

Entre las características que se añadieron con el desarrollo de esta propuesta¹⁰⁹ destacan las funciones relacionadas con el derecho a la portabilidad de datos y el derecho al olvido, la aparición por separado y sin activación automática por defecto en el registro de un nuevo usuario de las opciones de aceptar los términos y condiciones del servicio (ToS por sus siglas en inglés) y de “recibir información”, apareciesen separadas y sin marcar, así como la doble verificación de aceptación para recibir el boletín de noticias. También cabe destacar la implementación de la solicitud a los usuarios de volver a aceptar los ToS si estos se modificaban, lo cual debía notificarse por correo electrónico¹¹⁰.

¹⁰⁸Véase: <https://coditramuntana.com/es>

¹⁰⁹Véase: <https://github.com/decidim/decidim/issues/3320>

¹¹⁰Véase: <https://github.com/decidim/decidim/pull/3494> y <https://github.com/decidim/decidim/pull/3491>

La segunda propuesta también implementada tuvo que ver con la eliminación automática de cuentas de usuarios inactivos para cumplir el artículo 5(e) del RGPD, que explicita que:

[Los datos personales serán] mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); (Reglamento (UE) 2016/679, 2016, Artículo 5(e))

Antes de la implantación de esta propuesta sucedía que, si una participante no utilizaba su cuenta por un periodo superior a, por ejemplo, 12 meses, sus datos se conservaban por defecto para siempre a menos que los eliminase ella misma o solicitase su eliminación, por lo que urgía implementar una función que lo automatizase. Finalmente, Open Source Politics¹¹¹ desarrolló un módulo para implementar la limpieza de los datos obsoletos directamente en la base de datos, de modo que fuera posible detectar las cuentas de participantes que llevaban un tiempo determinado inactivas para eliminarlas, aplicándose lo mismo a las cuentas de administradoras obsoletas.

La tercera propuesta desarrollada aparece en Metadecidim bajo dos planteamientos diferentes pero enfocados al mismo tema, por lo que ambos culminaron con la misma implementación. Dichos planteamientos tenían que ver con la necesidad de simplificar los mencionados ToS para que apareciesen redactados en un lenguaje menos jurídico y más legible por la población general. Para ello, Platoniq¹¹² realizó con financiación del Ayuntamiento de Barcelona una modificación estructural de la página destinada a los ToS para que ésta incluyera resúmenes del texto.

Por otro lado, aunque no aparezca reflejado en Metadecidim, si visitamos el espacio de Github de Decidim¹¹³ bajo las etiquetas de “*team: privacy*” y “*contract: GDPR*” encontraremos también modificaciones relativas a la adaptación de la ventana emergente relativa al uso de *cookies* de la plataforma¹¹⁴ para adaptarla a que las participantes puedan elegir qué *cookies* aceptar y rechazar, diferenciadas entre: esenciales, preferencias, analíticas y de *marketing*. Junto a ello, se incluye que siempre

111 Véase: <https://opensourcepolitics.eu/>

112 Véase: <https://platoniq.net/es/home/>

113 Véase: <https://github.com/decidim/decidim>

114 Véase: <https://github.com/decidim/decidim/pull/9271>

sea posible modificar las preferencias a través de un botón habilitado para ello.

Por último, a lo largo del tiempo reaparece un debate recurrente en torno a la visibilidad de las cuentas de las participantes (las cuales son públicas por defecto) y los posibles riesgos que aparecen si deciden elegir un nombre de usuaria potencialmente asociable a su identidad. Tal y como ya apuntaban en el informe de Éticas (2016), desde Decidim se ha acabado incluyendo un mensaje a la hora de crearte una cuenta que indicaba que con el objetivo de garantizar el anonimato este nombre podía ser cualquiera:

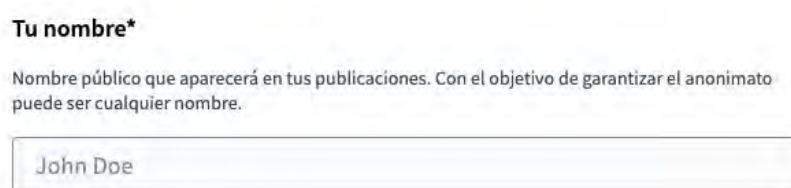


Figura 79. Captura de pantalla del mensaje que aparece a la hora de crear una cuenta en Decidim.

Sin embargo, tal y como he podido observar, en algunas instancias de Decidim este proceso se realiza a través de un sistema de autenticación de terceros, donde el nombre de usuario se completa de manera automática, y la persona usuaria no decide qué nombre público desea tener. Si bien este no es un problema de la plataforma en sí, dado que los perfiles públicos no incluyen información privada (como la dirección de correo electrónico o datos de identidad), y de igual manera, el paso descrito puede subsanarse modificando el alias en el apartado de configuración del participante, esta posibilidad ha generado incomodidad en las instancias donde sucede.

Como solución alternativa, desarrolladores que participan en el proyecto han creado un módulo¹¹⁵ (aún no implementado por la plataforma, por lo que precisa de un mantenimiento con cada actualización) cuya función es proporcionar ciertos controles en la configuración del perfil de la participante que le permitan decidir si quiere aparecer públicamente en la plataforma o no. Dicho módulo también hace que el perfil sea privado por defecto, lo que significa que no se publica información sobre las participantes antes de que hayan dado su consentimiento explícito para publicar dicha información. Bajo este módulo, cuando las participantes deciden permanecer anónimas o “en privado”, toda su información se oculta a la plataforma, incluida la API de Decidim, así como en cualquier página que normalmente mostraría su información, como la página de participante.

¹¹⁵Véase: <https://github.com/mainio/decidim-module-privacy/>

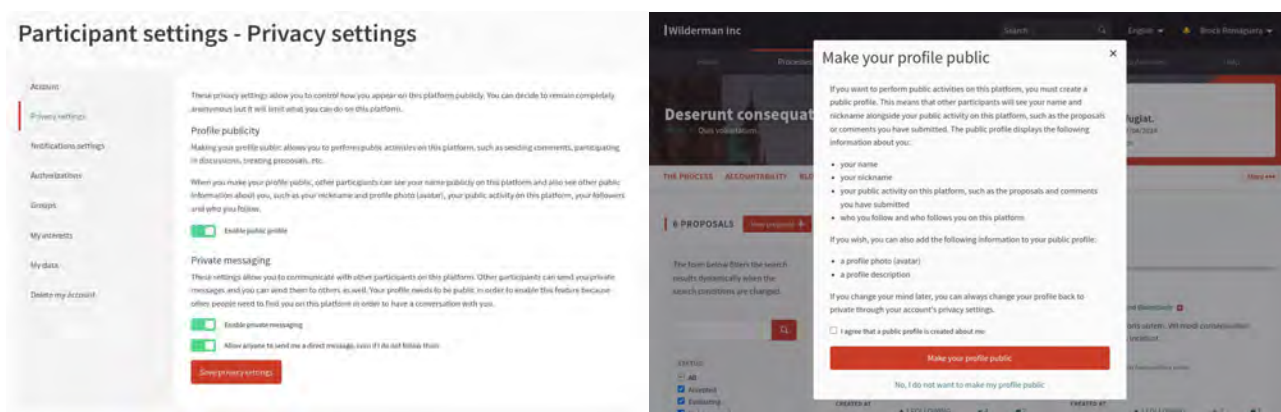


Figura 80. Capturas de pantalla del apartado de configuración de privacidad y mensaje de consentimiento.

Fuente: <https://github.com/mainio/decidim-module-privacy/?tab=readme-ov-file>

5.5. Contribuciones de Decidim al procomún

Cierro aquí esta sección, pero antes de pasar a detallar en las próximas páginas nuestra experimentación con Decidim en la UMA, me gustaría concluir enfatizando las contribuciones que esta plataforma digital de democracia participativa realiza al procomún tal y como lo definí en el apartado 2.5.3.

Así, si entendemos el procomún como «libertad para operar bajo restricciones simétricas» (Benkler, 2014, p. 70) con el requisito de «imbuir de co-participación todos los niveles, desde la producción hasta la toma de decisiones colectivas» (Lloredo Alix, 2020, p. 230), mi interpretación de Decidim a la luz de las cinco prácticas características del *software* libre deja patente su originalidad: a las actuales «patologías» generadas por la «participación algorítmica basada en *big data*» (Kelty, 2019b, p. 256), Decidim contrapone la emergencia de comunidades democráticas donde «la participación en un público recursivo se diseña para producir personas que sean instancias de ese colectivo, no individuos aislados a quienes se agregue en un todo» (Kelty, 2019b, p. 255).

Además, esta interpretación de Decidim (y Metadecidim) nos permite situarla en la citada batalla por la ecología institucional del entorno digital examinando capa a capa su contribución al paradigma del procomún, tal y como sintetizo en la tabla incluida al final.

De este modo, en las secciones 5.1 y 5.2 me he centrado en los componentes más reconocibles de las capas física (esto es, su infraestructura generalmente público-común), lógica (esto es, su apuesta por el *software* libre) y de contenido (el recurso a licencias libres para los diversos tipos de documentación) de Decidim.

A partir de aquí, las secciones 5.3 y 5.4 asumen los debates sobre la profundidad de recursión adecuada que plantea Kelty para indagar la conexión entre la salvaguarda de la privacidad y la concepción de un procomún de datos (democráticos) basado en la capa de contenido de Decidim. De este modo, constato que desde la privacidad por diseño de la plataforma hasta el ambicioso (e inconcluso) proyecto DECODE nos encontramos ante un proceso coherente que cabe concebir como “ofuscación selectiva” tal y como explican Brunton y Nissenbaum (2011, párr. 42) con una significativa alusión a los debates legislativos en la UE:

El fin teórico de la ofuscación selectiva se ha delineado desde una perspectiva legislativa como el acto de ofuscar los datos frente a determinados usuarios o a la reconstrucción de actos individuales, y en las recomendaciones de Gloria González Fuster para la limitación del procesamiento de datos en la UE, como el acto de limitar los datos a un procesamiento

primario: es decir, estructurar los datos de modo que puedan evaluarse para el propósito declarado, al cual los sujetos de los datos dan su consentimiento, pero no para análisis no contemplados (González Fuster, 2009). Bajo esta lógica, los datos recopilados para, por ejemplo, un estudio de salud pública serían adecuados al proceso usado para dicho estudio, difíciles de usar para otros procesos de minería de datos de salud pública, e imposibles de reutilizar para cualquier otro propósito.

En definitiva, sostengo que el marco histórico y conceptual del paradigma de la ofuscación que expuse en el Capítulo 4 podemos retomarlo en el caso de Decidim, no tanto como una resistencia directa y expresiva frente a la vigilancia digital, sino como una táctica constructiva de tratamiento de datos personales alternativo y seguro para potenciar la participación democrática a través de una privacidad habilitadora.

Cercamiento		Procomún
Capa física (1) <i>Transporte</i>		Banda ancha y redes inalámbricas en <i>alianza público-común</i>: Aprovechamiento de la banda ancha y redes inalámbricas de instituciones públicas, tanto gubernamentales como académicas.
	Centralización en servidores corporativos: - <i>Microsoft Azure</i> . Al emplear la forja Github, propiedad de Microsoft Corporation desde 2018, como plataforma de desarrollo del código y control de versiones de Decidim. - <i>Google Cloud</i> . Al integrar YouTube, propiedad de Alphabet, para reuniones en línea e incrustación de videos. - <i>AWS</i> . Al integrar Twitch, propiedad de Amazon, para reuniones en línea e incrustación de videos.	Distribución de servidores en <i>alianza público-común</i>: Alojamiento (de <i>Decidim</i> y de sus posibles plataformas integradas, como <i>Peertube</i> y <i>Etherpad</i>) en servidores de instituciones públicas, tanto gubernamentales como académicas. Distribución de servidores basada en el procomún: Alojamiento en servidores de instituciones basadas en el procomún, como (Co)incidim ¹¹⁶ y Som Energía.
Capa lógica (1) <i>Estándares</i>		Estándares abiertos e interoperables: Para datos, APIs u otras interfaces, OpenID, RSS, OStatus, etc.
Capa lógica (2) <i>Software</i>		Software libre: -Licencia <i>AGPLv3</i> para el código de Decidim. - <i>Ruby on Rails</i> como lenguaje libre de programación y marco de desarrollo <i>web</i> del lado del servidor.
Capa de contenidos (1) <i>Licencias</i>		Licencias libres: - <i>Creative Commons BY-SA 4.0</i> para textos ¹¹⁷ , imágenes, diseños... - <i>ODbl v.1.0</i> para datos; - <i>GNU FDL v.1.3</i> para documentación.
Capa de contenidos (2) <i>Servicios integrados</i>	Servicios integrados privativos: Integración con YouTube o Twitch para reuniones en línea e incrustación de videos.	Servicios integrados libres: -SMTP, para servidor de correo. - <i>Etherpad</i> , para textos colaborativos. - <i>Jitsi</i> , para videollamadas cifradas. - <i>Openstreetmaps</i> , para ubicaciones. - <i>Peertube</i> , para reuniones en línea e incrustación de videos P2P.
Capa de contenidos (3) <i>Tratamiento de datos</i>		Adaptación al RGPD (2018) ¹¹⁸ Publicación en formatos abiertos: CSV, JSON, PDF, etc. Apertura a visitantes sin cuenta Ofuscación de datos personales en <i>alianza privacidad-procomún</i>: -«Reconocible sin ser conocida»: Autenticación unidireccional criptográfica (<i>hashing</i>) para pseudonimato susceptible de verificación. -DECODE (proyecto piloto): Cartera digital, DLT a través de Tor, red de nodos, interfaz de visualización BCNOW y cifrado homomórfico para transmisión de recuentos.

Tabla 9. Panorámica de la ecología institucional de Decidim basada en las 3 capas que distingue Benkler (2006/2015, p. 449). Fuente: Elaboración propia

¹¹⁶Véase: <https://journal.platoniq.net/es/wilder-journal-1/learnings/coincidim-using-decidim-in-citizen-movements/>

¹¹⁷Véase el propio *libro blanco* de Decidim (Barandiaran *et al.*, 2024): <https://tecnopolitica.net/en/content/decidim-technopolitical-network-participatory-democracy-philosophy-practice-and-autonomy>

¹¹⁸Véase: <https://github.com/decidim/decidim/issues/3320>

6. Decidimos Educación Inclusiva

6.1. Movimiento Quererla es Crearla y proyectos de investigación por la educación inclusiva

Con la intención de contextualizar cómo surgió la plataforma participativa *Decidimos Educación Inclusiva* (<https://decidimoseducacioninclusiva.uma.es/>) considero conveniente comenzar explicando quiénes la conforman. De esta manera, encontramos en primer lugar al movimiento social por la educación inclusiva: Quererla es Crearla (en adelante QeC), un grupo de personas pertenecientes a diferentes colectivos de profesionales vinculados con la educación (docentes, orientadores/as, técnicos de la administración educativa, investigadores/as universitarios, etc.) así como familias y estudiantes de diferentes lugares, no solo de la geografía española, sino también de América Latina, todas ellas conectadas por la decisión de hacer las escuelas, y por extensión las sociedades donde se enmarcan, más inclusivas.

Por otro lado, al presentar la plataforma es crucial señalar de inicio que está sufragada por el Proyecto de Investigación *Narrativas emergentes para la construcción de escuelas inclusivas* perteneciente a mi universidad, la UMA, con financiación del Ministerio de Ciencia e Innovación. El *software* se encuentra instalado en una máquina virtual que se ejecuta en un conglomerado (*cluster*) de servidores modelo HPE Synergy 480 Gen 10 que se encuentran ubicados en el Centro de Proceso de Datos del Servicio Central de Informática (SCI), en el Edificio de los Servicios Centrales de Apoyo a la Investigación (SCAI) de la Universidad de Málaga (UMA).

Es importante indicar asimismo que el proyecto antes mencionado es una continuación de otro anterior, *Narrativas emergentes sobre la escuela inclusiva desde el modelo social de la discapacidad. Resistencia, resiliencia y cambio social* desarrollado entre 2018 y 2022 también con financiación del Ministerio de Ciencia, Innovación y Universidades de España. Si bien es cierto que fruto de este proyecto surgió el movimiento Quererla es Crearla, este movimiento trasciende los ámbitos de investigación de ambos proyectos, conformando una base de crecimiento y aprendizaje horizontal entre las personas investigadoras y las protagonistas de las acciones que se realizan bajo QeC, tal y como afirman los investigadores principales de ambos proyectos (Calderón y Rascón, 2022, p. 44):

[E]ntendemos que la investigación educativa puede construir saber y resistencia con la gente común para provocar el ansiado cambio, abandonando la lógica de la gestión científica para acoger el cambio educativo como movimiento social (Rincón, 2019). Particularmente valioso resulta investigar junto a activistas, que “con independencia de la radicalidad de sus manifestaciones públicas, todos marcharían bajo la bandera del ‘Nada

sobre nosotros, sin nosotros” (Lafuente, 2013). Se trata de la ciencia común, de producir conocimiento entre todos, que no es lo mismo que para todos (Lafuente & Estalella, 2015): el mundo común no reclama más expertos, ni alcaldes. Cuando la gente genera conocimiento valioso, contrastado y útil, y lo hace en común, construye un mundo deseable, más justo y hospitalario.

6.1.1. Quererla es Crearla¹¹⁹

Como he comentado anteriormente, Quererla es Crearla (QeC) es el nombre bajo el cual un grupo de personas y colectivos se ha organizado para defender colectiva y colaborativamente la educación inclusiva. Su denominación proviene de una campaña comunicativa homónima por la educación inclusiva que surgió a raíz de la serie de “Conversaciones sobre la escuela (inclusiva)” (Calderón y Rascón, 2020) que puso en marcha Ignacio Calderón en mayo de 2020, las cuales fueron retransmitidas primero en directo y posteriormente publicadas en su perfil de YouTube. Con esta paradójica apertura de un espacio dialógico virtual en pleno confinamiento por la pandemia de la COVID-19, se invitaba a pensar sobre la realidad que vivían las escuelas en esos momentos de clausura y sobre a qué escuelas se desearía volver tras su reapertura. A estas sesiones se apuntaron más de 200 personas de muy diversas procedencias, razón por la que se dividieron los encuentros por colectivos (familias, estudiantes, profesionales, investigadoras/es y políticas/os).

En medio de estas conversaciones se produjo una emergencia propiamente narrativa: al poco de constituirse en España a comienzos de 2020 el gobierno de coalición PSOE-UP, la entonces Ministra de Educación, Isabel Celaá, anunció que el primer proyecto de ley en someterse al Parlamento sería la reforma de la Ley Orgánica que regía el sistema educativo español (la LOMCE de 2013). Ante este anuncio, las madres activistas que habían participado en la conversaciones citadas salieron de ellas con la clara determinación de hacerse escuchar en el debate parlamentario para que la educación inclusiva no volviera a quedar relegada en la futura LOMLOE.

Para ello se optó por un tono y un discurso afirmativo, sin entrar en el marco de la segregación escolar, responder a las posibles provocaciones o caricaturizar a su vez a quienes piensan distinto; asertivo en cuanto a los derechos de las personas con discapacidad, pues ésta era la fuente de las exigencias al Gobierno para la LOMLOE; y esperanzador, intentando atraer a las personas afectadas por la apertura

¹¹⁹Este apartado forma parte de una ponencia invitada presentada junto con Florencio Cabello Fernández-Delgado el 15 de mayo de 2024 en el V Congreso Internacional sobre Movimientos Sociales y TIC Move.net, celebrado en la Facultad de Comunicación de la Universidad de Sevilla, titulada *Cómo rodar un movimiento: el proceso de creación del documental “Educación inclusiva: Quererla es crearla”*. <https://hdl.handle.net/10630/38009>

de horizontes de inclusión escolar, y no por emociones tristes. Con estas claves comunicativas y la experiencia de años de sufrimiento, lucha e iniciativas personales de difusión, estas familias sintieron que había llegado el momento de coordinarse para llegar aún más lejos.

Pero no se trataba solo de denunciar la escasa efectividad de muchas leyes educativas en España que a menudo dejan en papel mojado el derecho a una educación inclusiva si no existe una reclamación cotidiana a pie de escuela. Tampoco se pretendía ejercer de *lobby* que se ciñera a los códigos y plazos legislativos de la LOMLOE, por más relevante que ésta fuera. Por consiguiente, lo que considero más decisivo en el germen de la campaña QeC fue el propósito originario de trascender las reivindicaciones estrictamente legales para desencadenar un proceso de “concientización” (Freire, 1985, pp. 123-125; 160-161) respecto a dos aspectos inseparables: la capacidad colectiva de construcción de esa «objetividad feminista [que] trata de la localización limitada y del conocimiento situado, no de la trascendencia y el desdoblamiento del sujeto y el objeto» (Haraway, 1991/1995, p. 324); y la potencia política de esa (re)unión de activistas para poner tal conocimiento al servicio de la transformación de la realidad escolar.

En este sentido, podemos afirmar que la concepción de la campaña QeC se ajusta a las siete claves que para Barranquero (2007, p. 118) caracterizan las iniciativas edu-comunicativas para el cambio social:

En primer lugar, se ha subrayado que la prioridad en esta campaña es «generar un proceso de transformación colectiva» más allá de los productos mediáticos que emanen de ella; para cumplir tal prioridad, la campaña busca «que las familias implicadas se apropien del proceso», en lugar de delegar en personal experto (académico, legislativo, comunicativo...); en tercer lugar, lejos de pretender *trending topics* o apariciones fugaces en los medios, la campaña hace hincapié en la necesaria «pertinencia cultural» de las acciones que se diseñen, en coherencia con la atención a la diversidad cultural y sociopolítica del contexto en que se inserta.

Las características cuarta y quinta van emparentadas, pues si la campaña enfatiza el interés de intervenciones apegadas al terreno que generen una «participación distribuida en lo local», nunca pierde de vista la necesidad de un «trabajo en red», que permita vincular entre sí experiencias similares desplegadas en contextos diversos; en cuanto a la «selección de medios tecnológicos», se apuesta siempre por su adecuación al contexto (en nuestro caso, por ejemplo, muchas madres eran ya muy activas en Twitter, Instagram y Facebook, y esas fueron las plataformas de redes sociales donde abrimos perfiles de la campaña) y se rechaza que acaben convertidos en fines en sí mismos; finalmente, y en coherencia con lo afirmado arriba, la campaña contempla desde el principio una «trascendencia a

medio y largo plazo» que posibilite una transformación duradera de las condiciones de vida de las activistas y sus hijos.

Con la coordinación de una de las madres activistas, en mayo de 2020 arrancaron las reuniones con el cometido esencial de encontrar un título para la campaña que apelara al debate sobre la LOMLOE, pero que también lo trascendiera. Tras varios debates, finalmente optamos por “Quererla es Crearla”, una fórmula que aludía elusivamente a la educación inclusiva al tiempo que incidía en la emergencia sentida por las activistas de que partidos y entidades que en esas semanas decían quererla, se comprometieran a crearla.

A renglón seguido, se decidió que, si la campaña quería cumplir con las claves definidas en su concepción, especialmente con la búsqueda de alianzas con otros movimientos por la justicia social, lo más propicio sería lanzarla desde el anonimato. Con ello también aspirábamos a evitar que la atención hacia la campaña acabara enfocándose en las personas que la impulsaban, y en las situaciones de discriminación que vivían en comparación con otras. Junto a ello, la polarización del debate parlamentario y mediático que se imponía en general en el contexto pandémico, agudizada en lo tocante a la educación inclusiva, desaconsejaba la sobreexposición de algunas madres que ya venían padeciendo numerosas inectivas contra sus publicaciones personales (o incluso académicas) en *blogs* y plataformas de redes sociales.

En coherencia con todo lo anterior, establecimos como eje fundamental de la campaña el mensaje de que, lejos de cualquier apelación cínica al “realismo” para desacreditar la educación inclusiva, esta constituye una demanda plenamente democrática. En este sentido, si bien esta reivindicación afecta de entrada al alumnado con discapacidad, su alcance se extiende a otros estudiantes marcados por su género, etnia, procedencia, clase social, etc. En síntesis, la clave de la campaña radicaba en (re)ubicar la educación inclusiva en el marco de los avances democráticos imprescindibles para una sociedad más igualitaria y justa. Para ello hicimos hincapié en su vinculación con los derechos humanos universales (más concretamente, en la Convención de la ONU sobre los Derechos de las Personas con Discapacidad de 2006, ratificada por España en 2007) y con otras luchas pasadas y presentes en clave de lo que Nancy Hartsock (1975, p. 76) denominaba «entrelazamiento» (*«interlocking»*, en el original) de las opresiones del patriarcado, el supremacismo blanco y el capitalismo, y años después se ha dado en llamar con Kimberlé Crenshaw (1991) «interseccionalidad».

Con vistas a desarrollar este planteamiento de campaña, nos propusimos una doble combinación: la que articula la denuncia de los abusos a tales derechos universales con la visibilización de alternativas

efectivas que ya practican la inclusión escolar; y la que liga la afirmación razonada de argumentos, dictámenes y declaraciones oficiales que respaldan dichos derechos con una apelación más emotiva orientada a legitimar y ampliar la lucha por la inclusión vinculándola con otras similares más reconocidas socialmente. En esta línea, la primera tarea fue crear una página *web*¹²⁰ de la campaña que sirviese de referencia sobre sus reivindicaciones básicas, pero también de repositorio de todo el conocimiento científico, académico y vital que se había generado de forma distribuida en los últimos años en el movimiento por la educación inclusiva. No se trataba de inventar nada nuevo, sino más bien de que las familias y el personal académico hiciéramos un esfuerzo conjunto de inventariar toda la documentación que cargaba de razones (y de afectos) al movimiento.

En este punto, todas las familias expresaron su deseo de producir un primer video-manifiesto corto que fijara su posición en el debate sobre la LOMLOE y permitiera responder en clave afirmativa y esperanzadora al cuestionamiento del pleno derecho a la educación de las personas con discapacidad. Este vídeo¹²¹ se lanzó el 14 de octubre de 2020 para incidir en la tramitación parlamentaria de la LOMLOE que arrancaba ese mismo día y, más allá, sirvió de presentación de la campaña y de su *web*. A continuación, planteamos el lanzamiento para principios de 2021 de un segundo vídeo¹²² de corte más emotivo para denunciar las experiencias negativas que vive el alumnado con discapacidad que ya está en la escuela ordinaria, decidiéndose muy pronto que la soledad sería la protagonista de esta segunda pieza.

A partir de aquí, desde el proyecto investigador coordinamos la selección de materiales de la página *web*, para lo cual contamos con la ayuda de las familias con más bagaje jurídico y de colaboradores académicos que respondieron amablemente a nuestra solicitud. Una vez recopilado dicho material, acordamos con las familias una estructura de contenidos muy sintética basada en otras cuatro afirmaciones en primera persona del plural:

- Queremos: Esta sección contiene lo que podría denominarse el manifiesto de la campaña.
- Sabemos: Este apartado remite al “amplísimo corpus de conocimiento e investigación” al que se alude en el citado manifiesto como apoyo para las reivindicaciones de carácter más político y jurídico. En ella se pueden encontrar tanto libros, capítulos de libros y artículos como monografías sobre educación inclusiva, pasando por una serie de informes y guías oficiales

¹²⁰Véase: <https://creemoseducacioninclusiva.com>

¹²¹Véase: <https://youtu.be/ze1K3X5-NTY> Para la versión alojada en nuestro Peertube, véase: <https://creemoseducacioninclusiva.uma.es/w/kkog8Ks67Uitw6kVuQrSgB>

¹²²Véase: <https://youtu.be/uEPZ38BdiYE> Para la versión alojada en nuestro Peertube, véase: <https://creemoseducacioninclusiva.uma.es/w/oRjxcdGyLczao1fXWabNCJ>

sobre modelos y experiencias de educación inclusiva que ya funcionan en distintas partes del mundo.

- Defendemos: En esta sección, la campaña pone a disposición de familias, profesionales, partidos políticos, medios de comunicación y público en general la variedad de convenciones, declaraciones, ratificaciones y textos legislativos que, empezando por la ONU y acabando por el Estado español, reconocen la educación inclusiva como un derecho fundamental universal.
- Creamos: Este último epígrafe abarca un conjunto de secciones dedicadas a cada uno de los vídeos cortos producidos, a materiales escritos en forma de guía, así como a información sobre el documental que rodamos bajo la dirección de la cineasta Cecilia Barriga y sobre el modo de organizar proyecciones públicas del mismo.

Estimo fundamental detenerme aquí en presentar el documental mencionado. Titulado “Educación Inclusiva: Quererla es Crearla” (2022)¹²³, esta obra colaborativa surgió con el objetivo promover la educación inclusiva y el cambio social, destacando el activismo de las personas con discapacidad y sus entornos. En esta línea, el documental se proponía contribuir a encontrar, desarrollar y promover nuevas perspectivas sobre las discapacidades y los entornos educativos desde el punto de vista de quienes trabajan para la defensa de los derechos humanos.

A la hora de conceptualizar esta película, una de las primeras cuestiones que tuvimos que decidir estaba relacionada con determinar quiénes serían los protagonistas de la historia, dónde encajaría cada cual y hasta dónde podríamos llegar en nuestro rodaje. De este modo, desde el principio se procuró dotar del mayor protagonismo posible a las familias activistas por la educación inclusiva de manera que devinieran sujetos investigadores en lugar de quedar reducidos a objetos de investigación (Freire, 1982).

Esta apuesta por el protagonismo de las familias implicadas tanto en la campaña como en el documental no se detuvo siquiera en la fase de montaje, ya que en este se tuvieron en cuenta las diferentes visiones tanto de quienes protagonizan la obra como del equipo investigador, siempre bajo la dirección técnica y artística de la directora. Para ello, desarrollamos una serie de visionados colectivos (tanto presenciales como virtuales) de los diferentes cortes de la película, tras los cuales fuimos consensuando los momentos y escenas que reflejaban más claramente lo que buscábamos transmitir. Igualmente, fueron las personas protagonistas, en coordinación con el equipo investigador, las encargadas de la transcripción del documental y su posterior adaptación para el subtítulo en castellano de la obra.

¹²³Véase: <https://creemoseducacioninclusiva.com/documental-quererla-es-crearla/>

El estreno del documental tuvo lugar el 21 de octubre de 2022 a las 17:00h en el Auditorio Sabatini del Museo Reina Sofía, con la presencia de la Ministra de Educación del Gobierno de España, Pilar Alegría, de la junta directiva del museo y del equipo al completo de producción de la película. Desde aquel día, la obra ha quedado a disposición de todo colectivo que desee organizar un pase grupal en su territorio¹²⁴.

Para hacer dicha difusión libre y ecológicamente consciente, recurrimos a la plataforma distribuida de archivo y reproducción audiovisuales *PeerTube*, creada por la organización francesa Framasoft y definida como «*software* libre para recuperar el control de tus vídeos» (Peertube, s.f.). Entre las virtudes de *PeerTube*, destaca su apuesta por la arquitectura distribuida P2P (del inglés *peer-to-peer*, o entre pares, donde cada nodo de la red actúa a la vez como cliente y como servidor) como modo de reducir la carga de los servidores centrales (implicando a los nodos conectados al visionado para que compartan su ancho de banda de subida con el resto de espectadores) y, con ello, reducir a su vez la demanda de energía y sus emisiones contaminantes asociadas, especialmente de CO₂ (Mills, 2013, pp. 38-40).

En paralelo al camino que ha ido recorriendo el documental, multitud de compañeras y compañeros de QeC han ido trazando diversas acciones en favor de la escuela inclusiva, muchas de ellas recogidas también dentro de la pieza audiovisual. El primero que quisiera destacar es el inmenso trabajo del grupo de Estudiantes por la Inclusión, coordinado por la investigadora Luz Mojtar-Mendieta, en el desarrollo de una guía sobre educación inclusiva en institutos de secundaria. Elaborada para el INTEF (Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado) en el marco de sus Guías LADA (La Aventura del Aprender), las cuales reúnen a colectivos sociales e instituciones educativas para elaborar un documento de facilitación de proyectos colaborativos entre adolescentes. La citada guía, titulada *Cómo hacer inclusiva tu escuela* (Calderón *et al.*, 2021), es fruto de una serie de reuniones desarrolladas a lo largo de un año con 16 jóvenes de diversas clases sociales, capacidades, nacionalidades, etnias y géneros, entre otros, que participaron en un proceso de Investigación Acción Participativa Juvenil para analizar y reconstruir colectivamente sus realidades, conformando un grupo de resistencia (Mojtar-Mendieta *et al.*, 2025).

Desde sus primeros encuentros hasta ahora este grupo se ha ido consolidando como un referente en el activismo por la educación inclusiva. Buena prueba de ello son la multitud de charlas y cursos de formación para profesionales educativos que estos estudiantes realizan a escala local y regional y los reconocimientos que en esos mismos ámbitos vienen recibiendo sus integrantes¹²⁵. Con todo, en los

¹²⁴Véase: <https://creemoseducacioninclusiva.com/creamos/el-documental-se-mueve/>

¹²⁵Véase: <https://creemoseducacioninclusiva.com/creamos/estudiantes-por-la-inclusion/>

últimos tiempos la proyección de Estudiantes por la Inclusión ha rebasado con mucho dichas escalas: para empezar, en 2023 recibieron el Premio "Youth Teams in Education Research" (YTER), otorgado por la American Educational Research Association (AERA), el cual implicaba su selección como participantes del Congreso anual que la AERA celebró en Chicago el mismo año junto con otros 12 equipos de estudiantes de secundaria de EEUU y Canadá¹²⁶; junto a ello, otra delegación pronunció un discurso¹²⁷ en la sede de la ONU de Nueva York el 21 de marzo de 2024 como ganadores de uno de los premios anuales otorgados por la organización *Down Syndrome International*, el cual reconoció explícitamente el enfoque y composición interseccionales de este equipo¹²⁸.

Otro colectivo importante de QeC, surgido del WorkshopOrienta organizado en Málaga en 2018 y de las citadas Conversaciones sobre la escuela inclusiva de 2020, es el de orientadores y orientadoras de diferentes partes del territorio que trabajan para generar un nuevo modelo de Evaluación Psicopedagógica orientado a la inclusión¹²⁹. Entre los diversos materiales que han producido destacan tres en particular: un documento de mínimos para una Evaluación Sociopsicopedagógica Inclusiva denominado *Lineas Rojas*¹³⁰; otro documento para justificar la fundamentación de voto particular contrario a la escolarización fuera del aula ordinaria¹³¹; y la guía para una evaluación psicopedagógica inclusiva, que estará disponible próximamente.

En el transcurso del primer proyecto de investigación también se puso en marcha en el CEIP La Parra de Almáchar (Málaga) una Comunidad de Aprendizaje (CdA) que se vio enriquecida con un proceso de Investigación-Acción Participativa (IAP) cuyo objetivo fue mejorar la convivencia dentro del centro y con su entorno. De esta manera, la totalidad del alumnado y el profesorado seleccionó, diseñó e implementó un plan de acción integral de cara a identificar las barreras de aprendizaje y fomentar la participación de todo su alumnado sin excepción. Fruto de este trabajo se desarrolló una guía sobre *Cómo hacer una investigación-acción participativa*, también publicada por el Ministerio de Educación y Formación Profesional, para que otras escuelas y comunidades escolares puedan desarrollar sus propios procesos de crecimiento para la inclusión¹³², y se sentaron las bases para extrapolar este proceso a otros centros dentro del territorio español así como en América Latina, como veremos más adelante.

Por último, bajo este gran paraguas de QeC encontramos a diversas, sobre todo madres, activistas por

126 Véase: <https://www.uma.es/facultad-de-ciencias-de-la-educacion/noticias/estudiantes-por-la-inclusion-premio-aera-chicago-2023>

127 Véase: <https://creemoseducacioninclusiva.uma.es/w/hoCipAbhyycdfYtVAXFxuB>

128 Véase: <https://www.ds-int.org/world-down-syndrome-awards>

129 Véase: <https://creemoseducacioninclusiva.com/creamos/una-orientacion-para-la-educacion-inclusiva/>

130 Véase: <https://creemoseducacioninclusiva.com/2024/10/lineas-rojas/>

131 Véase: <https://creemoseducacioninclusiva.com/2024/10/orientacion-escolar-y-derechos-humanos/>

132 Véase: <https://creemoseducacioninclusiva.com/creamos/una-escuela-trabajando-por-sus-suenos/>

la equidad, la inclusión educativa y los derechos de las personas etiquetadas por la discapacidad, que desarrollan acciones no solo por sus criaturas sino para toda la sociedad. Algunas de ellas se agruparon bajo un colectivo denominado “Radikales Desadaptadas” para elaborar la obra *Cómo disentir. Una guía (o compañía)* (2024)¹³³, en la que comparten sus experiencias frente a injusticias que viven en el día a día.

A su vez, estas activistas han desarrollado diversas acciones en plataformas de redes sociales, algunas de las cuales han alcanzado gran trascendencia, como la campaña *#YnoPasaNada*¹³⁴ desarrollada Belén Jurado para agrupar y denunciar las vulneraciones del derecho a la educación que han sido normalizadas en la cotidianidad de las escuelas. La serie de ilustraciones elaboradas por Ricardo Clemente sobre las *#excusas* a las que se enfrentan las familias cuando abogan por la educación inclusiva en sus escuelas han sido luego adaptadas a diferentes prendas de ropa para llevar el mensaje más lejos de las pantallas¹³⁵. Algunas de ellas incluyen además códigos QR que remiten a información detallada que desmonta esas falsas creencias como que «la inclusión está muy bien pero no hay recursos»¹³⁶.

Más recientemente, otra “radical desadaptada”, Paula Verde, ha impulsado la campaña – *favores + derechos*¹³⁷ a raíz de la privación por parte del centro escolar de su hijo de los recursos necesarios para su educación (Sotelino, 2024). Esta campaña derivó en una concentración convocada por *Foanpas*, la federación de madres y padres de alumnado de Vigo y comarca, y la asociación de directores de colegios públicos, *Adicopuvi*, exigiendo a la Xunta de Galicia más recursos para una educación inclusiva (La Voz de Galicia, 2024).

6.1.2. Proyecto de investigación “Narrativas emergentes para la construcción de escuelas inclusivas”

Como avancé arriba, el proyecto de investigación *Narrativas emergentes para la construcción de escuelas inclusivas*, del que formo parte actualmente, busca enfrentar las dificultades que tienen los sistemas educativos en todo el mundo para adaptarse a cambios sociales, tecnológicos y culturales, por lo que se reconoce la necesidad internacional de hacer que las escuelas sean más acogedoras e inclusivas. En este sentido, he de enfatizar la continuidad de este proyecto con el anterior, que bajo el título *Narrativas emergentes sobre la escuela inclusiva desde el modelo social de la discapacidad. Resistencia, resiliencia y cambio social* contribuyó al nacimiento del movimiento Quererla es crearla analizado en la sección 6.1. Surgido en 2018 del cuestionamiento de por qué algunas personas no obtienen resultados satisfactorios o son

133 Véase: <https://creemoseducacioninclusiva.com/creamos/como-disentir/>

134 Véase: <https://creemoseducacioninclusiva.com/creamos/y-no-pasa-nada/testimonios-y-no-pasa-nada/>

135 Véase: <https://www.latostadora.com/shop/quererlaescrearla/#shop>

136 Véase: <https://creemoseducacioninclusiva.com/pero-no-hay-recursos/>

137 Véase: <https://www.instagram.com/p/DANzAMGuhPg/?hl=es>

excluidas del sistema educativo, este primer proyecto buscaba mejorar el sistema educativo desde una perspectiva inclusiva, desde el convencimiento de que de esta manera se contribuía a crear a una sociedad más equitativa y justa. Como he señalado, con este propósito se aglutinó la participación de diversos actores de la comunidad educativa y activista para generar diversos materiales que se utilizan actualmente en universidades, escuelas y cursos de formación para profesionales, contribuyendo a transformar las políticas educativas y hacerlas más inclusivas.

Si este trabajo inicial demostró la capacidad del equipo investigador para avanzar en el conocimiento y contribuir al desarrollo escolar en España, el nuevo proyecto amplía sus objetivos y límites geográficos para abordar el desafío de la educación inclusiva también en América Latina, expandiendo allí la generación de conocimiento pedagógico y la implementación de políticas inclusivas basadas en las voces de la comunidad, siempre en colaboración con activistas sobre el terreno. Sobre esta base, el proyecto fue seleccionado en la Convocatoria de 2022 de Proyectos de Generación de Conocimiento del Ministerio de Ciencia e Innovación del Gobierno de España para perseguir los siguientes objetivos:

Objetivos generales:

1. Localizar y documentar narrativas iberoamericanas sobre inclusión educativa que se originan en colectivos en desventaja con el fin de difundirlas y reconocer su valor.
2. Conocer y comprender las concepciones educativas, experiencias y prácticas profesionales implicadas en los procesos de inclusión escolar desarrolladas por docentes y equipos de orientación.
3. Elaborar y difundir recursos que visibilicen y alimenten nuevas concepciones sobre la diversidad y que articulen propuestas para promover la construcción de comunidades educativas inclusivas.
4. Promover la transformación de políticas, culturas y prácticas en escuelas de España y América Latina, orientándolas a la inclusión y la equidad a través de metodologías participativas.

Objetivos Específicos:

1. Documentar nuevas narrativas sobre la diversidad y la inclusión emanadas de personas implicadas en el reconocimiento de los derechos humanos.
2. Documentar a través de historias de vida, narrativas y análisis interseccionales que permitan recoger las experiencias de inclusión escolar desarrolladas por docentes, familias, estudiantes y equipos de orientación.

3. Conocer y profundizar las concepciones educativas de profesionales escolares involucrados en el movimiento por los derechos humanos.
4. Comprender los procedimientos de colaboración que utilizan las personas estudiadas en sus procesos de resistencia y su posible relación con la resiliencia.
5. Difundir nacional e internacionalmente los recursos elaborados en el marco del proyecto de investigación precedente, así como los de nueva creación.
6. Elaborar recursos narrativos, audiovisuales y artísticos que favorezcan miradas más complejas y profundas acerca de la realidad humana, la desigualdad y las diferencias desde una perspectiva interseccional.
7. Desarrollar un diagnóstico participativo de la situación de la inclusión escolar en España y América Latina, desde la experiencia de miembros de los distintos colectivos que conforman la comunidad educativa.
8. Contribuir a la democratización de las escuelas, fomentando el uso de metodologías participativas en los centros educativos que impliquen a profesionales, estudiantes y familias, y faciliten el proceso de hacer sus escuelas más inclusivas.
9. Promover la construcción de redes de colaboración y activismo para la inclusión.
10. Desarrollar programas de formación sobre inclusión a partir de las narrativas emanadas de los colectivos objeto de estudio.
11. Examinar y contrastar la legislación educativa internacional y supranacional, sus lógicas y sus posibles contradicciones con las propuestas de educación inclusiva.

6.1.3. Por qué un Decidim para Quererla es Crearla

Las razones que nos han llevado a implementar la plataforma Decidim examinada en el Capítulo 5 para desarrollar diferentes actividades dentro de nuestro último proyecto de investigación y del movimiento QeC son fruto de una voluntad de coherencia intelectual y política con nuestra metodología y posicionamiento investigador. En este sentido, la primera razón parte de la apuesta del proyecto por trabajar en favor de la educación inclusiva de forma colectiva y participativa:

Queda por delante impulsar luchas que den salida a una situación de evidente acoso social y educativo, que permitan la construcción de nuevos proyectos de vida. Pero, de vida

comunitaria; no podemos volver a incurrir en el error de focalizarnos en lo individual. Eso es precisamente lo que propone el proyecto de hacer las escuelas inclusivas: sacar del pozo de lo individual el problema, porque ese ejercicio condena las diferencias (Calderón y Rascón, 2022, p. 44).

La segunda razón, de índole más metodológica, tiene que ver con la intención por parte del grupo de poner en marcha una serie de procesos de IAP en diferentes escuelas de Latinoamérica y España, haciendo uso de los materiales construidos previamente y de otros recursos producidos *ad hoc*. Así, la denominada *Red Internacional de Escuelas por la Inclusión y la Equidad*¹³⁸ comenzó en mayo de 2024 y a ella se han sumado 29 centros, 19 pertenecientes al territorio español, 4 de México, 3 de Colombia, y otros 3 en Costa Rica, Brasil y Chile. Con ellas se desarrollan diferentes reuniones telemáticas de coordinación de la implantación de estas IAPs así como de seguimiento de las tareas que han de cumplimentar los centros entre cada reunión. Este importante crecimiento en el número de participantes, sumado a limitaciones como la diferencia horaria y de disponibilidad o la obvia incapacidad de trasladarnos físicamente a los centros con tanta facilidad como en el caso de la anterior IAP en el CEIP *La Parra*, requería una planificación y organización marcadamente *online* que, sin sustituir a los necesarios encuentros presenciales en cada territorio, facilita en gran medida la tarea.

Por otro lado, estamos hablando de un proyecto de investigación muy maduro y prolífico, de cuyo amplio bagaje he dado cuenta a lo largo de estas líneas. Así, en su edición anterior se llegaron a ver implicadas cerca de 500 personas entre las diferentes actividades realizadas (Calderón y Rascón, 2022, p. 48), por lo que contamos con un relevante respaldo de personas comprometidas en mayor o menor medida en QeC. Bajo estas circunstancias, contar con una plataforma virtual propia de participación nos permitiría trascender las limitaciones de una página *web* estática (por lo demás muy nutrida) y, sobre todo, de los perfiles en diferentes plataformas de redes sociales comerciales. Se trataba, pues, de explorar las posibilidades que Decidim nos ofrecía de sustentar y ampliar estas relaciones ya establecidas, animando a las personas implicadas tanto a asumir un papel más activo como a tomar distancia cuando no dispusieran del tiempo necesario, pero siempre con la oportunidad de ponerse al día mediante la consulta sencilla de la agenda de reuniones de los distintos procesos, de los resúmenes y actas de encuentros anteriores, etc.

Además, la oportunidad de aglutinar las diferentes conversaciones, encuentros, debates, actas y propuestas que se dan en el movimiento en un mismo espacio virtual facilita en gran medida la tarea de

¹³⁸Véase: <https://creemoseducacioninclusiva.com/creamos/red-escuelas-por-la-inclusion/>

documentación, así como la difusión de las decisiones y acciones de QeC a otras personas. A su vez, Decidim da la posibilidad de limitar el acceso y la visibilidad al público en general de, por ejemplo, un encuentro, otorgando acceso sólo a las personas registradas en la plataforma e incluso solo a ciertas participantes dentro de las registradas, por lo que brinda espacios seguros para que se den ciertas conversaciones o toma de decisiones.

La última cuestión que considero conveniente destacar aquí es que desde que planteamos las primeras campañas de QeC, un aspecto constitutivo de nuestra labor ha sido trasladar al movimiento por la educación inclusiva los debates democráticos sobre «la profundidad de recursión adecuada» (Kelty, 2008/2019a, p. 384), en consonancia con lo examinado en el Capítulo 5. De ahí que, en la medida de lo posible, todas nuestras creaciones audiovisuales, incluyendo el largometraje *Educación inclusiva: Quererla es crearla* (2022), en todas sus versiones y con todos sus materiales asociados¹³⁹, se han difundido según la filosofía del «copyleft» (Stallman, 2002/2004, pp. 92-93). De este modo, la adopción de la licencia libre *Creative Commons Reconocimiento-Compartir Igual 4.0* para la publicación de todas nuestras obras supone el expreso consentimiento previo para que quienes las vean puedan copiarlas, compartirlas y adaptarlas para cualquier finalidad con la sola condición de citar su autoría y mantener esas mismas libertades en las eventuales obras derivadas.

En estrecha relación con ello, al inicio del capítulo avancé que nuestro propósito de difundir nuestras obras del modo más ecológico posible nos ha llevado a la pionera (al menos en la universidad española) instalación de una instancia de la plataforma de vídeo *PeerTube* en los servidores del SCI de la UMA. Así, frente a la tendencia a que las obras audiovisuales producidas desde el sector público acaben confinadas en las llamadas “nubes” de las grandes corporaciones, con los consiguientes perjuicios de privacidad y de contaminación ecológica (Pitron, 2021), la organización Framasoft ofrece *PeerTube* como un modo de reducir la carga de los servidores, al implicar a quienes ven un vídeo en la cesión de ancho de banda de subida para su difusión al resto. Junto a ello, al abrir nuestro servidor de *PeerTube* en la UMA los vídeos que colgamos en él pueden ser encontrados a través del buscador de cualquier otro servicio de *PeerTube*, según una lógica federada fiel a la interoperabilidad original de Internet y alejada de los jardines amurallados de las grandes plataformas privativas.

¹³⁹Véase: <https://creemoseducacioninclusiva.com/documental-quererla-es-crearla/>

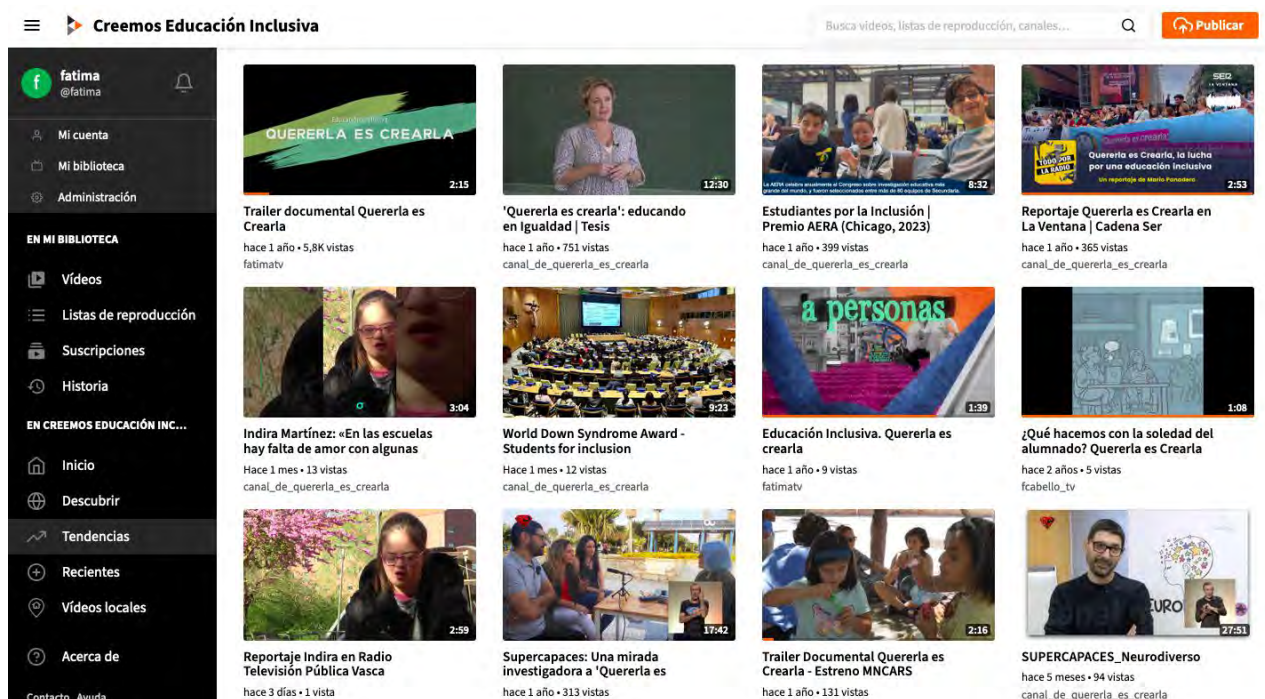


Figura 81. Captura de pantalla del Peertube de QeC: <https://creemoseducacioninclusiva.uma.es/>

Siguiendo la misma lógica recursiva, recuerdo aquí mi análisis de Decidim como una plataforma basada en el procomún, sintetizado en la Tabla 9 del Capítulo 5: en la capa física, no depende de servidores centralizados extractivistas de datos (y, como hemos visto, suele alojarse en servidores públicos de instituciones como ayuntamientos o universidades); en la capa lógica, está construida íntegra y colaborativamente con *software* libre con licencia: *Affero GPLv3*³⁴; y en la capa de contenido, se vale de las licencias *Creative Commons By-SA* para texto, imágenes, diseño y demás materiales y *Open Access Database Licence* para los datos (Barandarian *et al.*, 2024, pp. 4-5).

Además, Decidim es una infraestructura “multi-usuario” que, como tal, se presta a la instalación de varias instancias en un único servidor garantizando su funcionamiento independiente. Ello permite impulsar el desarrollo de un modelo de servicio basado en Decidim en el que diferentes instituciones, organizaciones y proyectos pueden operar una única instalación que dé soporte a múltiples sitios activos, lo que reduce los costes de gestión y mantenimiento, a la vez que proporciona un mejor mantenimiento a estas instancias de Decidim (Barandarian *et al.*, 2024, p. 76). En este sentido, el hecho de que hayamos instalado la plataforma Decidim de QeC en los servidores del SCI de la UMA ofrece a otros grupos y proyectos universitarios la posibilidad de instalar sus propias instancias, cumpliendo así con el fomento del *software* público como servicio (pSaaS, por sus siglas en inglés) (Barandarian *et al.*, 2024, p. 76) y, más allá, de las alianzas público-comunes que Decidim defiende.

A la vista de este conjunto de razones emanadas de la investigación sobre Decidim expuesta en el Capítulo 5, el 9 de mayo de 2024 operé el paso de la observación participante a la IAP al solicitar presentar la plataforma a mis compañeras y compañeros en una reunión híbrida (presencial en la UMA pero incorporando virtualmente a otras colegas de España y América Latina) del proyecto de investigación. A raíz de dicha presentación, abrimos la deliberación sobre si queríamos embarcarnos en la ambiciosa tarea de instalar y poner a punto esta infraestructura democrática de gran alcance para que los diferentes agentes que creemos y creamos educación inclusiva (con especial atención a los de América Latina) diéramos un nuevo “salto recursivo”. Tras el visto bueno del equipo comencé, junto con Florencio Cabello, las diferentes tareas que requerían su puesta a punto, las cuales detallaré a continuación.

Por último, quisiera mencionar cómo este desarrollo de la nueva plataforma ha ocasionado una evolución en las citadas secciones de la página *web* de QeC, de “queremos”, “sabemos”, “defendemos” y “creamos”, a que ahora también “decidimos” educación inclusiva.

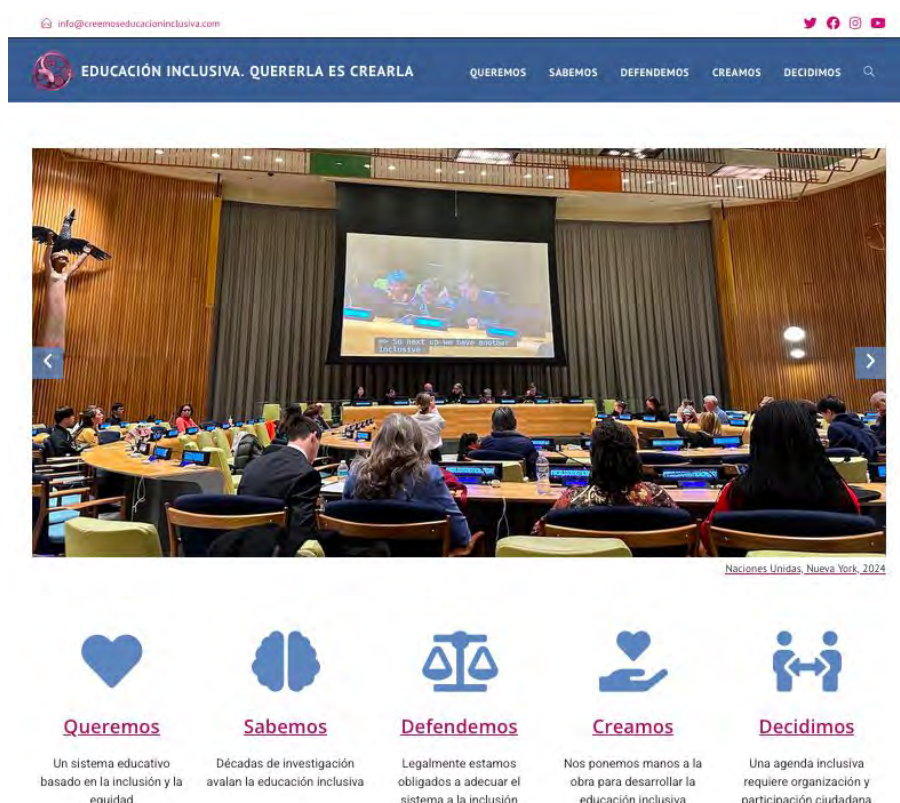


Figura 82. Captura de pantalla de la página de inicio de <https://creemoseducacioninclusiva.com/> Recuperado el 20 de febrero de 2025.

6.2. Cómo hacer un Decidim para Quererla es Crearla

Como avancé en la tabla 9 al final del Capítulo 5, Decidim es una plataforma construida íntegra y colaborativamente con *software* libre, concretamente con Ruby on Rails¹⁴⁰, un lenguaje de programación que permite a cualquier persona crearla y configurarla para ser utilizada como una red política para la participación democrática. Para quien maneje ese lenguaje de programación su instalación no debe resultar difícil, y desde Decidim aportan la información necesaria para llevarlo a cabo¹⁴¹. Sin embargo, dado que esto no siempre es así, alrededor del proyecto han surgido diferentes empresas que ofrecen servicios de instalación y asesoramiento en torno a la plataforma. En nuestro caso, para su instalación tuvimos la muy valiosa ayuda del equipo de Pokecode¹⁴².

Instalar un Decidim requiere una serie de requisitos técnicos: para empezar, es necesario contar con un servidor con 2 núcleos y 4GB de RAM mínimo; si además se instala a través de un Docker¹⁴³, desde Pokecode recomiendan al menos 100GB de espacio de memoria. También requiere de un proveedor SMTP capaz de enviar correos electrónicos en nombre de Decidim, amén de un certificado SSL y un nombre de dominio. A través de una serie de solicitudes de servicio (y alguna que otra visita presencial), Florencio Cabello trasladó al amable equipo del SCI estos y otro requisitos para la instalación. Tras realizar estos ajustes y proveer desde el SCI a los compañeros de Pokecode de la preceptiva clave pública para acceder a la máquina virtual, finalmente la plataforma se lanzó el 14 de junio de 2024 y todo su código y documentación se encuentra disponible en el siguiente repositorio específico de Github¹⁴⁴.

De entre los diferentes espacios (iniciativas, procesos, asambleas, consultas y jornadas) y componentes de Decidim que describí al inicio del Capítulo 5, entendimos que, al menos de entrada, resultaba más sencillo partir de aquéllos a los que sabíamos que le daríamos un uso desde el principio. Es por ello que tanto los espacios “iniciativas” como “consultas” no forman parte de *decidimoseducacioninclusiva.uma.es* en el momento en el que escribo estas líneas.

Por otro lado, debido a la vocación de internacionalización de nuestro proyecto de investigación y del propio movimiento QeC, precisamos poder ofrecer la plataforma en diferentes idiomas, por lo que actualmente se puede navegar en castellano, inglés, francés, portugués, así como en catalán, euskera y gallego.

140Véase: <https://rubyonrails.org/>

141Véase: <https://docs.decidim.org/en/v0.29/index.html>

142Véase: <https://pokecode.net/>

143Véase: <https://www.docker.com/>

144Véase: <https://github.com/openpoke/decidim-inclusiva>



Figura 83. Captura de pantalla de la caja de idiomas del pie de página de <https://decimoseducacioninclusiva.uma.es/>

Una vez definidas estas cuestiones, llegaba el momento de enseñar a utilizar la plataforma a nuestras compañeras. Como nos encontramos en una fase muy preliminar del proyecto todavía, de momento hemos seguido lo que podríamos considerar una estrategia diseminada.

De hecho, a la hora de formar a futuras administradoras, es cierto que ciertas cuestiones tienen una lógica consecutiva (esto es, si no marco esta casilla, no aparecerá tal acción disponible), pero otras requieren una traslación de la lógica con la que opera la plataforma a las necesidades específicas de nuestro grupo, tal y como ilustraré en el punto 6.3.2. con un caso concreto. Es por ello que, lejos de clases magistrales, el (continuo) proceso de formación y aprendizaje en el que estamos todas inmersas se está desarrollando de la siguiente manera: en primer lugar tuvimos una serie de reuniones Florencio y yo para resolver y también entender el porqué de ciertas acciones dentro de los diferentes espacios. Fruto de este aprendizaje Florencio elaboró un *Manual básico de administración de interfaz Decidim-QeC* (v0.28) para que otras compañeras pudiesen consultarlo.

Tras esto, algunas compañeras tanto del grupo de investigación como de QeC tuvimos una primera reunión en formato híbrido, es decir, algunas estaban presentes y otras accedieron a la reunión, por primera vez, a través de nuestra propia instancia *decimoseducacioninclusiva.uma.es*. En este encuentro presenté la estructura del Decidim de QeC, y recorrí los procedimientos de alta como participantes y *admins*, así como los “Espacios” básicos desplegados y sus respectivos componentes (incluido el de “Encuentros”, desde el que recursivamente convocamos y desarrollamos esta misma reunión). Igualmente deliberamos ciertas cuestiones relativas a qué asambleas constituiríamos o hasta qué punto debería ser un encuentro público o privado. En esta misma fecha, Florencio e Indira Martínez de Illarduya, compañera de Estudiantes por la inclusión, acordaron realizar una serie de encuentros de formación abiertos a través de la plataforma para profundizar en su aprendizaje¹⁴⁵.

¹⁴⁵Véase: <https://decimoseducacioninclusiva.uma.es/assemblies/nos-organizamos/f/5/meetings>

EDUCACIÓN INCLUSIVA. QUERERLA ES CREARLA

Buscar

Ayuda Encuentros Actividad Cuenta

¡Bienvenida a la Comunidad Quererla es Crearla!

Participa

Quererla es Crearla Asambleas Jornadas Procesos Contacta

Bienvenida a la plataforma participativa Decidimos Educación Inclusiva.

Construyamos una sociedad más abierta, transparente y colaborativa.
Únete, participa y decide.

¿Cómo participo en un proceso?

Encuentros
Averigua dónde y cuándo puedes participar en encuentros públicos.

Debates
Debate y discute, comparte tus opiniones y enriquece los temas relevantes.

Propuestas
Haz propuestas, apoya las existentes y promueve los cambios que desees ver.

Más información sobre Decidimos Educación Inclusiva

Jornadas activas

Ver todas las conferencias

Workshop Cataliza 2024-Barcelona
25 oct 2024 → 26 oct 2024

Las AMPAS como aceleradoras de una educación inclusiva
20 jul 2024 → 21 jul 2024

Congreso ION 2024 - Paraguay
04 jul 2024 → 06 jul 2024

WorkshopCrearla: Construyendo colectivamente para impulsar la escuela inclusiva
22 oct 2022

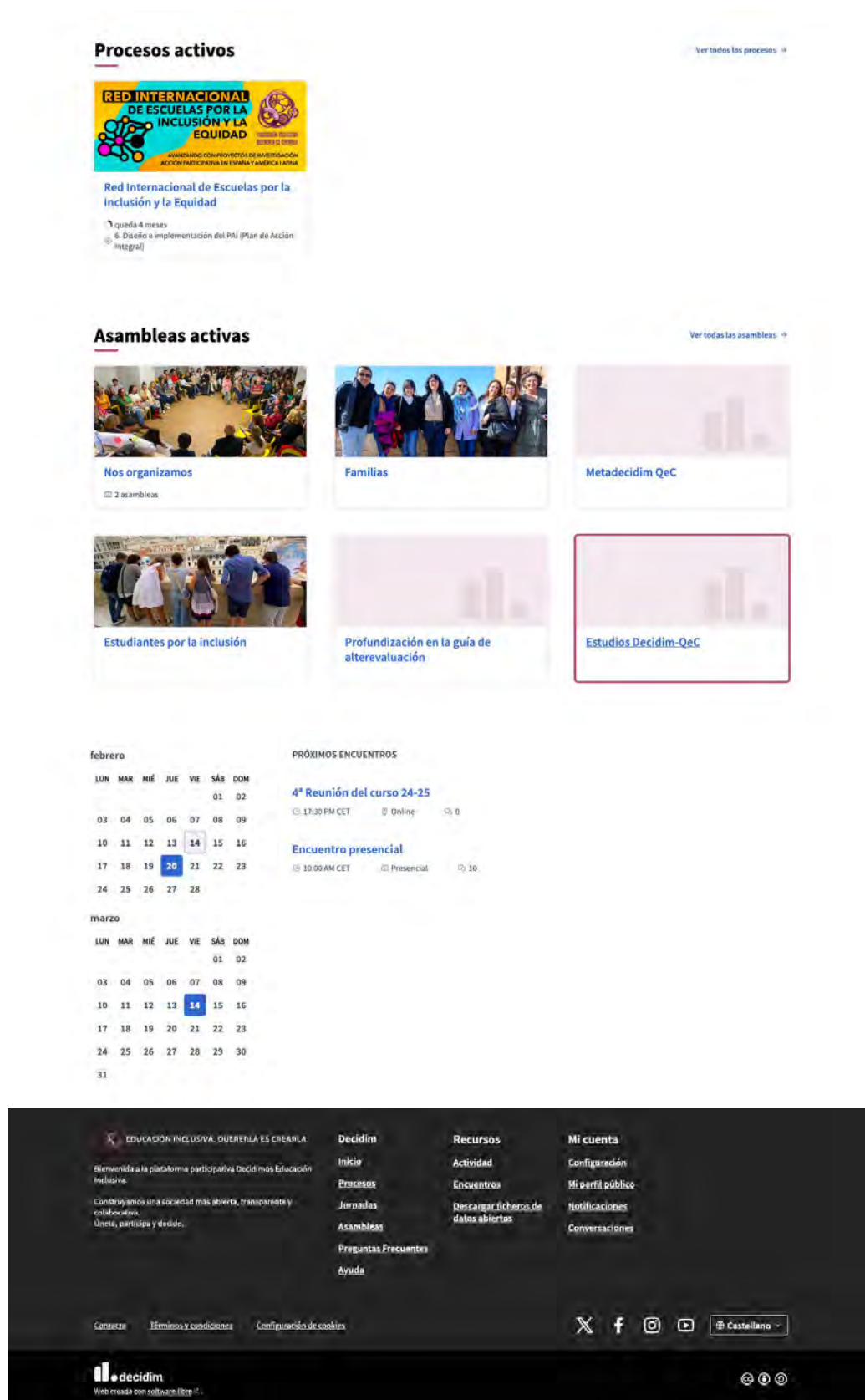


Figura 84. Captura de pantalla de la página de inicio de <https://decidimoseduccioninclusiva.uma.es/> Recuperado el 14 de febrero de 2025.

6.3. Cómo nos organizamos

Tal y como comenté a lo largo del Capítulo 5, la plataforma se diseñó en un principio para favorecer la participación ciudadana en la toma de decisiones del Ayuntamiento de Barcelona. Al pensar su diseño como medio comunicativo y deliberativo entre una administración y su ciudadanía, Decidim está construida a partir de esta lógica que, aunque tiene una alta capacidad de modulación, en ocasiones hemos tenido que “traducir” a nuestra diversas necesidades operativas como comunidad.

Si bien actualmente nos encontramos en una fase inicial en el desarrollo nuestra instancia, por lo que no puedo descartar que en el futuro sufra una o varias modificaciones, estimo oportuno adelantar algunas cuestiones relativas a cómo hemos articulado en este tiempo la plataforma, así como desglosar nuestra organización del *workshop* internacional que celebramos en Barcelona a finales de octubre de 2024 a través de ella.

6.3.1. Cómo hemos articulado la plataforma

Desde que lanzamos la plataforma el 14 de junio de 2024 hasta el momento en el que escribo estas líneas¹⁴⁶, contamos con 673 participantes, 13 de ellas con la función de administradoras, se han realizado 65 encuentros, se han escrito 225 comentarios y se han redactado 13 propuestas entre sus diferentes espacios.

Dentro de estos “espacios”, habilitados tanto de manera pública como privada, se han puesto en marcha tres “procesos”, entre los que destaca la *Red Internacional de Escuelas para la Inclusión y la Equidad*.

También hemos constituido 11 “asambleas”, de las cuales son de acceso público las siguientes: *Nos organizamos*, que incluye dentro de ella dos “sub-asambleas” (*Estudios Decidim-QeC* y *Metadecidim QeC*); *Estudiantes por la inclusión*; *Familias*; *Quererla es Crearla Mediterrànea* (para coordinar las actividades que afectan a Cataluña, Baleares, Comunidad Valenciana, Murcia y Andalucía); *Crear redes de apoyo*; y *Orientación* y *Quererla es Crearla Noroeste* (donde se coordinan diferentes actividades circunscritas a Galicia, Asturias y León).

A partir de aquí hemos celebrado dos “jornadas”, aunque he de matizar que en la plataforma incluimos otras dos (el *Workshop Crearla 2022: Construyendo colectivamente para impulsar la escuela inclusiva* y el *Congreso ION 2024 Paraguay*) a título exclusivamente informativo y para facilitar su vinculación con futuros procesos que puedan ponerse en marcha.

Aclarado esto, las primeras jornadas desarrolladas a través de esta plataforma fue *Las AMPAS como*

¹⁴⁶Recuperado el 20 de febrero de 2025.

*aceleradoras de una educación inclusiva*¹⁴⁷, celebrada el 20 y 21 de julio en Arcos de la Frontera (Cádiz, España). En ella se utilizó esta plataforma para realizar reuniones previas donde discutir la propuesta inicial con diferentes agentes involucrados y, posteriormente, debatir sobre el borrador del programa del evento. Resulta relevante señalar que tras este evento se inició el citado proceso *Construcción de la Guía: El cambio educativo desde las AMPAS*. En segundo lugar, encontramos el *Workshop Cataliza 2024 – Barcelona*, celebrado los días 25 y 26 de octubre en el Hub Social de la Fundación Bofill y en el cual me detendré en el próximo apartado debido a su relevancia para nuestra plataforma.

6.3.2. Primera gran prueba: el *Workshop Cataliza 2024*

Desde el comienzo del estudio que sustenta *Quererla es Crearla*, nuestro grupo de investigación ha estado organizando eventos participativos que han ayudado a enfocar nuestros esfuerzos de manera conjunta y coordinada: así, en 2018 tuvo lugar en Málaga el *Workshop Orienta*¹⁴⁸; en 2020 se llevaron a cabo de forma virtual las ya mencionadas *Conversaciones sobre la escuela (inclusiva)*; y en 2022 nos reunimos en Madrid en torno al *Workshop Crearla*¹⁴⁹. Sin tratarse de un evento aislado, el encuentro que tuvo lugar en Barcelona en 2024 representa, sin embargo, la primera vez en que poníamos en práctica la participación híbrida a través del Decidim de QeC que detallaré a continuación.

Cabe recordar aquí que una de las actividades propuestas por los investigadores principales para la Convocatoria de 2022 de Proyectos de Generación de Conocimiento del Ministerio de Ciencia e Innovación del Gobierno de España era el desarrollo de un *workshop* internacional en el que participasen familiares, profesionales y estudiantes para abordar la experiencia de la escolarización de niños y niñas y la desigualdad escolar. Con él se pretendía fomentar un encuentro de trabajo a través de la comunicación igualitaria de estos colectivos con el objeto de realizar una evaluación de la experiencia de la escolarización en España y América Latina. Igualmente este *workshop* buscaba iniciar una serie de líneas estratégicas para trabajar coordinadamente en los diferentes territorios por la transformación necesaria de las escuelas. En suma, para nuestro equipo este tipo de encuentros constituye un marco inmejorable para el desarrollo del resto de la investigación y para la movilización de un grupo internacional de activistas que generen propuestas de trabajo, con especial énfasis en el impulso del mencionado colectivo Estudiantes por la inclusión.

A partir de esta propuesta, desde el proyecto de investigación establecimos que en 2024 el *Workshop*

147Véase: <https://decidimoseduccioninclusiva.uma.es/conferences/AMPASaceleran>

148Véase: <https://creemoseducacioninclusiva.com/2024/10/workshop-orienta/>

149Véase: <https://creemoseducacioninclusiva.com/2024/10/workshop-crearla/>

*Cataliza*¹⁵⁰ debería ser ya ese encuentro internacional entre familias, estudiantes y profesionales y otros agentes comunitarios para impulsar el movimiento por la educación inclusiva. De este modo, la continuidad del trabajo participativo, organizado y sistemático que QeC venía desarrollando desde hace más de seis años podría apoyar la construcción de una Red Internacional de escuelas por la inclusión y la equidad, dirigida a facilitar y acelerar el proceso de transformación de los sistemas educativos de España y América Latina para hacerlos más inclusivos.

Sobre la base de pensar y construir globalmente para actual localmente en la creación de un movimiento social por la educación inclusiva, organizamos con QeC y el departamento de Teoría e Historia de la Educación, Pedagogía Social y M.I.D.E el citado *Workshop Cataliza* los días 25 y 26 de octubre de 2024, de 9:00 a 20:30 horas, en el Hub Social de la Fundació Bofill en Barcelona.

Conscientes del valor de lo que hemos ido construyendo, así como del momento singularmente importante que atravesamos, este encuentro tenía dos grandes cometidos: por una parte, acompañar a la *Red Internacional de Escuelas por la Inclusión y la Equidad* en sus primeros pasos para avanzar en la transformación de sus realidades; por otra, seguir desarrollando el movimiento social por la educación inclusiva en España y en América Latina. Más concretamente, formulamos así, los objetivos del *Workshop Cataliza*:

- Facilitar y acelerar el proceso de transformación de políticas, culturas y prácticas educativas en escuelas de España y América Latina, orientándolas a la inclusión y la equidad a través de metodologías participativas.
- Constituir un espacio para el desarrollo de la Red Internacional de escuelas por la Inclusión y la Equidad.
- Conocer y comprender las concepciones educativas, experiencias y prácticas profesionales implicadas en los procesos de inclusión escolar.
- Aprender de los saberes del alumnado, las familias y los y las profesionales, favoreciendo que todos los miembros de la comunidad educativa puedan contar sus experiencias escolares y sus propuestas de mejora.
- Identificar, desarrollar y compartir los mecanismos de colaboración utilizados en los diferentes centros educativos.

Para llevar esto a cabo, el *Workshop Cataliza* se estructuró en dos jornadas de trabajo intensivo, la

¹⁵⁰Véase: <https://decidimoseduccioninclusiva.uma.es/conferences/workshopcataliza>

primera centrada en apoyar a la red de escuelas y la segunda en vertebrar el movimiento social. Dadas las diferencias horarios con América Latina, las mañanas de cada uno de estos días estuvieron destinadas a los y las participantes de España y las tardes, al *Workshop* Internacional. Independientemente de esta previsión, todos los participantes podían participar en cualquier sesión, según este esquema: el viernes 25 de octubre, la sesión de la mañana se dedicó fundamentalmente a trabajar con la Red de Escuelas de España, mientras que la sesión de la tarde se dedicó al trabajo con la Red Internacional de Escuelas, con énfasis en América Latina. El sábado 26 de octubre por la mañana avanzamos en el estado y agenda del Movimiento Social por la Educación Inclusiva en España, y por la tarde nos dedicamos a generar líneas de trabajo para el avance del Movimiento Social Internacional. En síntesis, los días se distribuyeron de la siguiente forma:

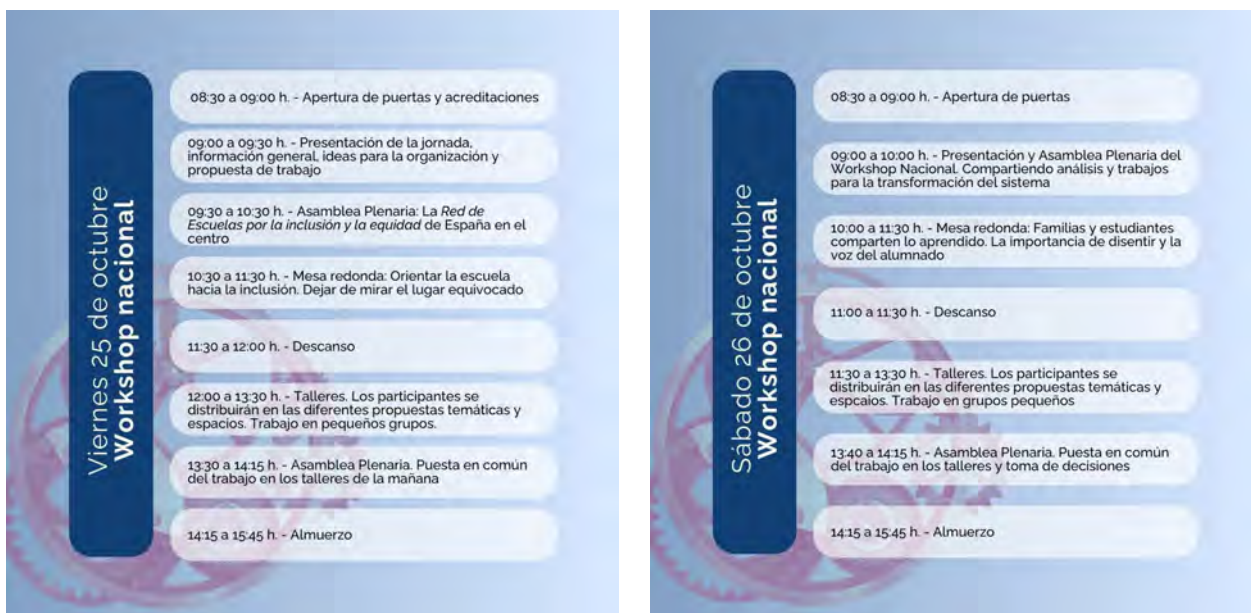




Figura 85. Horarios del Workshop Cataliza 2024. Fuente: elaboración propia para las redes sociales de Quererla es Crearla

Dado que se trataba de un evento de carácter internacional, previmos que muchas personas, pese a su interés por participar, no podrían estar presencialmente en Barcelona esos días. Particularmente para todas aquellas personas que participasen desde América Latina, en las semanas antes de la celebración del *Workshop* hicimos una convocatoria de vídeos en los que pedíamos que esbozasen su historia, un dolor y una alegría asociados a la escuela. No buscábamos historias edulcoradas, sino narrativas reales que contasen lo bueno y lo malo que estaban viviendo en relación con la educación escolar. Esta convocatoria recibió una gran respuesta y pudimos contar con casi 40 testimonios de diferentes países (Colombia, Venezuela, Chile, Uruguay, Argentina, México, Paraguay, Brasil y Perú), todos ellos disponibles en la instancia de *Peertube* de QeC¹⁵¹, también instalada y mantenida en colaboración con el SCI de la UMA.

¹⁵¹Véase: <https://creemoseducacioninclusiva.uma.es/w/p/3mPiV1usXD4wVFgMq7eDRN>



Figura 86. Videos testimonios de América Latina para QeC.

Fuente: <https://creemoseducacioninclusiva.com/creamos/workshopcataliza/>

A su vez, y gracias a Bitlab¹⁵², durante el evento establecimos la infraestructura necesaria para retransmitir las sesiones plenarias en *streaming* a través de nuestra instancia de *Peertube*, para que pudiesen ser seguidas por las personas interesadas dentro y fuera de nuestras fronteras. Como complemento de lo anterior (sobre todo para disponer de un *chat* en directo que no nos permitía nuestro *Peertube*) y específicamente para facilitar la participación remota en los talleres en grupos pequeños, habilitamos diferentes videoconferencias sobre la instancia de *Jitsi Meet* que ofrece *Guifi.net*¹⁵³. También se utilizó el *hashtag* #WorkshopCataliza en plataformas de redes sociales para que las personas que siguiesen los debates y el trabajo asambleario pudieran compartir imágenes y comentarios etiquetados del evento.

Pero para que todo esto pudiese suceder, lo primero que debíamos gestionar con las asistentes eran las inscripciones al *workshop*. Si bien en el caso del *Workshop Crearla* de 2022 en Madrid, solo había un tipo

¹⁵²Véase: <https://www.bitlab.cat/es/>

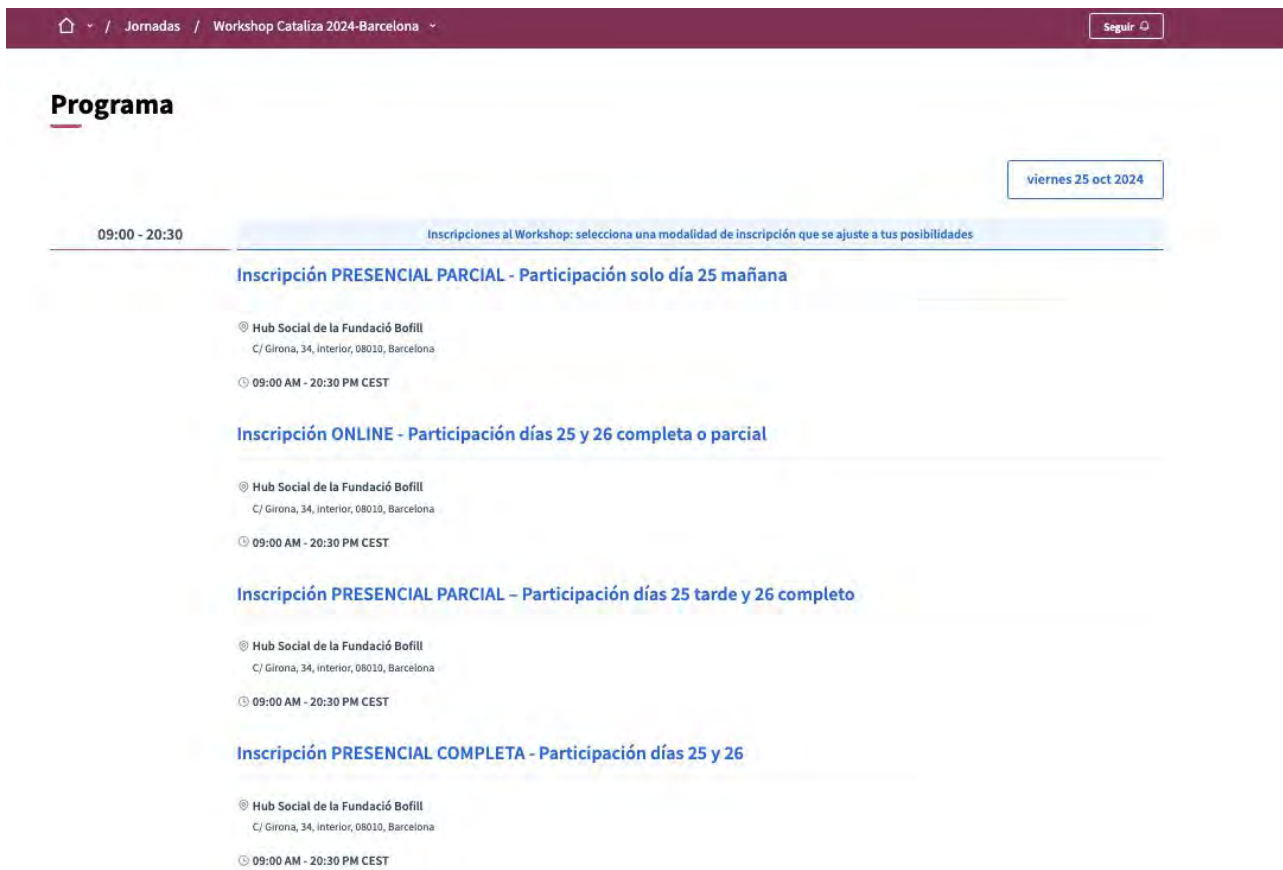
¹⁵³Véase: <https://meet.guifi.net/>

de inscripción y las realizamos a través de una encuesta en el servicio libre y cifrado *Cryptpad*, para Barcelona, debido a las distintas formas de participación y las diferentes temáticas que se abordarían, decidimos que lo más sencillo para nuestras asistentes era habilitar cuatro tipos de inscripciones diferentes en nuestra plataforma *decidimoseduccioninclusiva.uma.es*.

Esta última opción nos llevó a abordar la primera adaptación de Decidim a nuestras necesidades. La cuestión que planteo aquí es que, si bien el mencionado espacio “Jornadas” da la opción de gestionar las inscripciones a través de una configuración predeterminada, desde la organización del evento necesitábamos recopilar una serie de datos sobre las asistentes para poder coordinarlo adecuadamente. Lamentablemente, dicha configuración predeterminada no incluye la opción de realizar una serie de preguntas a quien desea inscribirse, por lo que, para no tener que enviar tras la inscripción a cada participante una encuesta que podrían no contestar, decidimos que lo más conveniente era realizar las citadas inscripciones creando diferentes “encuentros” para cada una, dado que las inscripciones a ellos sí permiten incluir una encuesta previa.

Con este método, además, perseguíamos simplificar la tarea de registrarse por primera vez en la plataforma para futuras actividades. No en vano, para apuntarte al *workshop* primero debías tener una cuenta en *decidimoseduccioninclusiva.uma.es*, algo relativamente sencillo de completar —ingresar un correo electrónico y una contraseña— si la asistente ya estaba motivada a rellenar el resto de campos para participar en el encuentro. Además, contamos con la inestimable ayuda de nuestra compañera Indira Martínez de Illarduya, que elaboró un detallado tutorial sobre cómo realizar esta acción¹⁵⁴. Gracias a todo ello, puedo afirmar que esta adaptación de Decidim a las inscripciones del *WorkshopCataliza* resultó una forma muy fructífera de introducir a nuestros colaboradores en el funcionamiento de la plataforma.

¹⁵⁴Véase: <https://creemoseducacioninclusiva.uma.es/w/tQrdZ2tFTtrEqEzVETE8b7>



Programa

viernes 25 oct 2024

09:00 - 20:30 Inscripciones al Workshop: selecciona una modalidad de inscripción que se ajuste a tus posibilidades

Inscripción PRESENCIAL PARCIAL - Participación solo día 25 mañana

Hub Social de la Fundació Bofill
C/ Girona, 34, interior, 08010, Barcelona

09:00 AM - 20:30 PM CEST

Inscripción ONLINE - Participación días 25 y 26 completa o parcial

Hub Social de la Fundació Bofill
C/ Girona, 34, interior, 08010, Barcelona

09:00 AM - 20:30 PM CEST

Inscripción PRESENCIAL PARCIAL - Participación días 25 tarde y 26 completo

Hub Social de la Fundació Bofill
C/ Girona, 34, interior, 08010, Barcelona

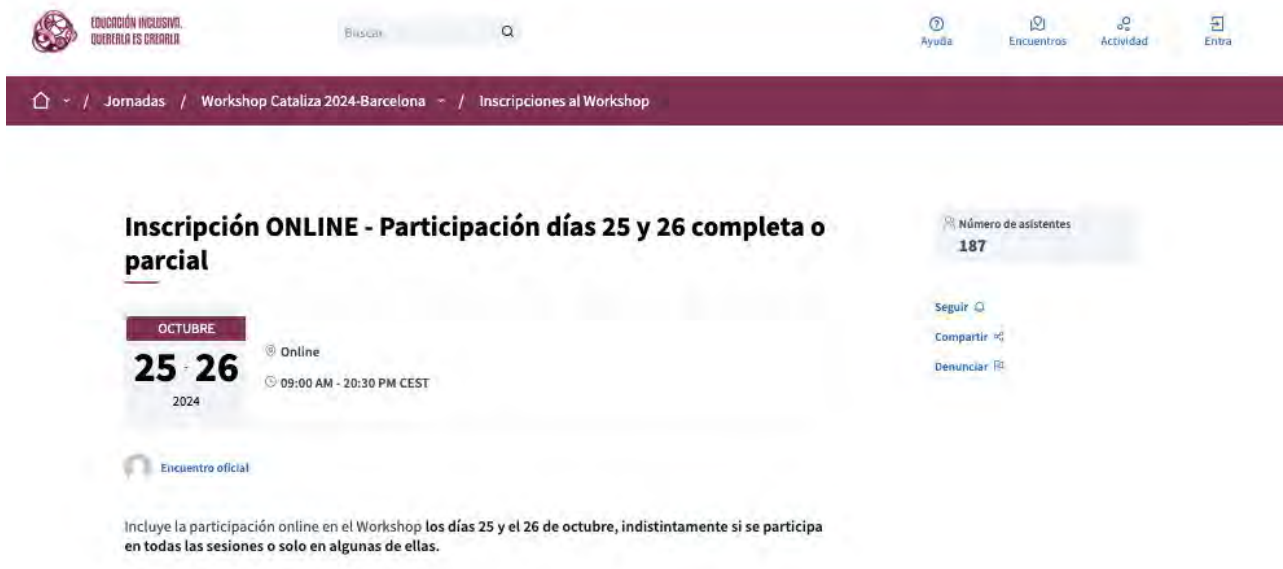
09:00 AM - 20:30 PM CEST

Inscripción PRESENCIAL COMPLETA - Participación días 25 y 26

Hub Social de la Fundació Bofill
C/ Girona, 34, interior, 08010, Barcelona

09:00 AM - 20:30 PM CEST

Figura 87. Captura de pantalla de los diferentes tipos de inscripción en el *Workshop Cataliza*.



EDUCACIÓN INCLUSIVA. QUIERELA ES CREARLA

BUSCAR

Ayuda Encuentros Actividad Entra

Home / Jornadas / Workshop Cataliza 2024-Barcelona / Inscripciones al Workshop

Inscripción ONLINE - Participación días 25 y 26 completa o parcial

Número de asistentes: 187

Seguir

Compartir

Denunciar

OCTUBRE

25 - 26 2024

Online

09:00 AM - 20:30 PM CEST

Encuentro oficial

Incluye la participación online en el Workshop los días 25 y el 26 de octubre, indistintamente si se participa en todas las sesiones o solo en algunas de ellas.

Figura 88. Captura de pantalla de a inscripción *online* en el *Workshop Cataliza*.

De cara al desarrollo del evento, dada la citada diferente naturaleza de las actividades que tendrían lugar en él, también nos valimos del espacio “encuentros” para plasmarlas a modo de “programa”¹⁵⁵. Esto nos permitía a su vez generar diferentes enlaces para acceder *online*, desgranar los vídeos del encuentro en función del tema que tratar y, lo que finalmente reconocimos como más importante, subir instantáneamente las actas de cada charla, taller o asamblea en cada cierre de encuentro, lo que nos permitía reunir y ofrecer en tiempo real la documentación de cada uno de los actos¹⁵⁶.

Con vistas a calibrar la envergadura del evento, apunto aquí que, entre asistentes presenciales y *online*, llegamos a contar con más de 300 participantes. En este sentido, he de incidir en que esta combinación de actividades, encuentros presenciales e híbridos, mesas redondas, charlas y asambleas, sumado a los *streamings* y las participaciones *online* a través de videoconferencias pudo llevarse a cabo gracias a la adecuación del espacio prestado por la Fundació Bofill y al maratoniano trabajo de todos los colaboradores de nuestra organización: el equipo del Sindicato Popular de Vendedores Ambulantes de Barcelona¹⁵⁷, los citados realizadores de Bitlab, La Llacana¹⁵⁸ y los intérpretes de lenguaje de signos de Entre Signos¹⁵⁹. Igualmente incalculable fue la ayuda de todas aquellas personas que participaron tanto desde el equipo de investigación como desde QeC en moderar, dinamizar y, lo más importante, tomar actas de cada encuentro.

155Véase: <https://decidimoseduccioninclusiva.uma.es/conferences/workshopcataliza/program/9>

156Véase como ejemplo: <https://decidimoseduccioninclusiva.uma.es/conferences/workshopcataliza/f/9/meetings/58>

157Véase: <https://manteros.org/>

158Véase: <https://lallucana.com/>

159Véase: <https://www.entresignos.com>

6.4. Reflexiones sobre un proceso en marcha

Como indicaba en el punto 1.4.4., el ciclo continuo de reflexión y actuación que ha caracterizado la realización de este proyecto no se puede presentar aquí como concluido, ya que el estudio que la sustenta tiene una duración que supera la redacción de este trabajo. Lo que sí puedo adelantar en estas páginas es un conjunto de reflexiones (aún incipientes) sobre la migración de QeC a Decidim que vengo coordinando desde mediados de junio de 2024 y que, si bien superó satisfactoriamente su primera gran prueba en octubre de ese mismo año con la celebración del *Workshop Cataliza*, aún debe atravesar nuevas producciones hasta prestarse a extraer conclusiones.

Mi primera reflexión tiene que ver con este *workshop*, concretamente con los frutos recogidos de la apuesta por Decidim como plataforma de participación y documentación. En este sentido, puedo afirmar que gracias a los vídeos facilitados por Bitlab y a las transcripciones llevadas a cabo por la empresa ACCIUMRed¹⁶⁰, completados con las actas recogidas en el Decidim de QeC, hemos podido extraer los temas y debates clave que surgieron del *Workshop Cataliza* como base para futuras acciones tanto del movimiento QeC como del proyecto. Se cumple así nuestra intención de valernos de Decidim como una plataforma recursiva sobre la que coger impulso para llevar más lejos nuestro trabajo por la educación inclusiva.

La segunda reflexión, acaso debería describirla más bien como tarea pendiente. Y es que si he destacado que la reconfiguración de las inscripciones en Decidim ha sido muy fructífera para introducir a nuevos colaboradores en la plataforma, ello implica ahora un nuevo salto: la decisiva importancia de continuar con los proceso de formación de las compañeras para que cada vez seamos más los agentes impulsores de actividades dentro de la plataforma.

Aquí volvemos una vez más a los debates sobre «la profundidad de recursión adecuada» (Kelty, 2008/2019a, p. 384) a los que aludí en el Capítulo 5, pues para mí es crucial trasladar a cada vez más participantes de QeC esa capacidad de adaptación de las herramientas disponibles a las funciones que específicamente necesiten desde cada entidad y territorio, sobre todo para favorecer más las conversaciones dentro de *decidimoseducacioninclusiva.uma.es* y hacer de ella el punto de encuentro *online* de España y América Latina en torno a la educación inclusiva.

De hecho, una reflexión que probablemente compartimos todos aquellos que colaboramos en movimientos y activismos de diversa índole es cómo favorecer dicha participación o, al menos, cómo

¹⁶⁰Véase: <https://acciumred.com/>

generar los espacios y momentos para que nuestras compañeras se animen a ello. Si bien la plataforma Decidim está diseñada para este fin, algo que nos enseñó rodar el documental *Educación inclusiva: Quererla es Crearla* (2022) es que siguen siendo imprescindibles esos espacios de encuentro físicos donde poder compartir nuestras experiencias. De ahí nuestra necesidad de seguir moviéndonos y fomentando esas reuniones cara a cara, ahora apoyadas en una plataforma donde poder convocarlas, difundirlas y registrar nuestras conversaciones y debates para que otras se puedan sumar a ellas.

Conclusiones

Conclusiones

A lo largo de este trabajo he dedicado muchas líneas a intentar desmontar ciertas creencias que están firmemente arraigadas en relación a varios conceptos vinculados al tema de esta tesis. Motivada por una concepción crítica de la historia —gracias en parte al trabajo de Silvia Federici, así como a los escritos de David Graeber y David Wengrow, entre otros— vi necesario detenerme a describir de dónde provienen y la razón por la cual percibimos de la manera que lo hacemos cuestiones relacionadas con la vigilancia, la privacidad y el tratamiento dispensado a los datos personales dentro de un sistema extractivista.

Esto resulta importante porque, tal y como apunta Paola Ricaurte (2023, p. 57), «el extractivismo en términos de desarrollo tecnológico está asociado además con la construcción de narrativas, discursos e imaginarios» que persiguen imponer un relato y un futuro únicos, así como la idea de que no se puede vivir fuera de tal sistema y, por tanto, la acción colectiva no es viable.

De esta manera, si nos retrotraemos a algunos ejemplos históricos, sobre todo de Europa y América, observamos cómo el poder de distintos gobiernos se ha mantenido mediante la vigilancia de su población. Para tal fin, el establecimiento de la escritura resultó fundamental, ya que facilitó la supervisión de un volumen mayor de personas y justifica por qué las insurrecciones populares a menudo comenzaban por destruir los registros de deudas y posesiones. La llegada de la imprenta permitió difundir el poder administrativo, aunque la vigilancia moderna, en el siglo XIX, también se expandió con la militarización y la industria. Todo ello nos lleva a entender que, a pesar de que la vigilancia no es algo nuevo, sí ha evolucionado gracias a técnicas de registro cada vez más avanzadas.

También hemos visto que, en el transcurso de la época moderna, la vigilancia fue superponiéndose a la coerción física y el espectáculo en el mantenimiento del orden, y cómo la mayor facilidad de la población para desplazarse a otros territorios supuso que los Estados aumentasen su capacidad de control, primero de los grupos marginales para después extenderlo a la población general. A ello vino a sumarse posteriormente la expansión de la organización burocrática, evidente tanto en los ejércitos modernos y en los sistemas de organización del Estado, como en la empresa capitalista. A su vez, la ampliación de los derechos de la ciudadanía ligada a la emergencia de los Estados de bienestar implicó un mayor seguimiento y registro de la población, que a menudo se traducía en un escrutinio exacerbado de los colectivos históricamente más vulnerables.

Al final del siglo XX, la expansión de las tecnologías microelectrónicas aumentó la capacidad de vigilar, por lo que hoy en día ésta ha cambiado y es más fluida y flexible, aunque he de remarcar que aún coexiste con formas tradicionales de control. Con todo, este nuevo tipo de «vigilancia post-panóptica» (Bauman y Lyon, 2013, pp. 61-84) se basa en la movilidad y conectividad, donde las tecnologías y redes de información son más relevantes que las instituciones, por lo que la vigilancia ahora funciona a distancia, gestionando flujos de datos y clasificando a las personas. Esta cibervigilancia se caracteriza por el seguimiento predictivo de comportamientos a través de algoritmos, generando desventajas para muchos, al tratar a las personas como datos.

A lo largo del texto he señalado también cómo las corporaciones han cooperado con los sistemas de vigilancia de los Estados, reforzando el complejo militar-industrial hacia un «complejo militar-digital» ante el que advertía McChesney (2014, pp. 158-171).

Por otro lado, y en nombre de la seguridad, las personas nos hemos acostumbrado a ser observadas y localizadas en ciertos espacios, lo que ha llevado a una pérdida de nuestra privacidad. A su vez, hemos trasladado nuestra presencia cada vez más a un mundo digitalizado en el que imperan la «datificación» y el «dataísmo» (van Dijck, 2014), esto es, la creencia en que se puede cuantificar objetivamente el comportamiento humano y la confianza plena en quienes manejan dichos datos. Esto tiene repercusiones en, por ejemplo, cómo uno de los métodos más importantes para generar riqueza en las empresas que operan en Internet es la monitorización de sus usuarios y la extracción de sus datos personales, todo ello sobre la base de que en el momento en que volcamos parcelas de nuestra vida en la Red asumimos que en ella hay una ausencia de privacidad real.

Sin embargo, lejos de estas interesadas proclamas que dan por finalizada la posibilidad de que exista dicha privacidad, también hemos constatado cómo ésta debería dejar de ser vista como una cuestión individual. En efecto, a lo largo de esta tesis subyace el alegato de que la privacidad resulta importante no solo como un valor que protege a las personas de abusos, sino también porque vivir en una sociedad que defiende la privacidad de manera colectiva protege a su vez otros valores igual de importantes como la igualdad, la justicia y la democracia.

A partir de dicho alegato, la taxonomía de la privacidad de Solove me ha permitido presentar sistemáticamente los dilemas relacionados desde «un enfoque descriptivo de abajo a arriba de los tipos de problemas de privacidad que se abordan en diversos debates» (Solove, 2009, p. 172), aunque debemos tener en cuenta que estos problemas no son inmutables. Con todo, la principal función de este enfoque es cambiar las discusiones teóricas sobre la privacidad, moviéndolas de una concepción

unificada a centrarse en los diversos problemas que se generan en torno a ella, lo que proporciona más claridad a la hora de abordar los riesgos de la pérdida de privacidad.

De manera resumida podemos decir que la privacidad es un derecho fundamental porque su valor está vinculado al bienestar colectivo. Aunque es importante señalar que al proteger la privacidad individual no se debe perjudicar a la sociedad; de hecho, su valor debe justificarse por los beneficios sociales que aporta. De esta manera, no se trata de un valor absoluto y superior al resto: vivimos en comunidad, lo que hace que nuestro bienestar esté conectado con el de los demás.

En última instancia, el valor de la privacidad debe entenderse por su contribución a la sociedad, incluso si a menudo se argumenta su valor en términos de derechos individuales. En consecuencia, la privacidad no ha de contemplarse solo como una defensa contra el control social, sino como una protección socialmente construida contra varios problemas, todos ellos cruciales para la autonomía, seguridad, igualdad y justicia. Por todo ello se torna de especial necesidad considerar los contextos específicos para evaluar la privacidad y los intereses en conflicto en cada situación.

Aquí es donde estimo que el concepto de «privacidad como integridad contextual» de Nissenbaum (2004) resulta uno de los más adecuados, ya que en él se reconoce la importancia de preservar este derecho en diversos contextos sociales, asumiendo que diferentes entornos requieren distintos niveles de privacidad y que las normas en torno a ella pueden variar según el contexto específico. Para mantener la integridad contextual, pues, las personas deben ser conscientes de las expectativas y normas de un entorno particular y ser capaces de gestionar estos límites eficazmente.

Por otra parte, hemos visto cómo a medida que las personas nos integramos cada vez más en la vida en línea, los dispositivos conectados se vuelven parte de nuestra vida diaria, lo que provoca que nuestra percepción social y de nosotros mismos cambie. Dichos cambios afectan cómo vivimos y formamos nuestras identidades en la era digital. Aquí es importante entender que no solo percibimos a los demás a través de datos, sino que nosotros mismos podemos llegar a vernos en esos términos. En este sentido, Haggerty y Ericson (2000) introdujeron el concepto de «doble de datos» para describir el interés por el control de fragmentos de datos personales, especialmente en lo que ello implica de que el cuerpo se divida en flujos de información para ser analizados. Este doble de datos, si bien no representa a la persona, puede influir en su vida cotidiana y, en algunos casos, puede llegar a prevalecer sobre su propia palabra.

Otra cuestión analizada es cómo anhelamos y utilizamos todos estos dispositivos que hemos mencionado. Si bien deseamos mantenernos en Internet, descargar aplicaciones y acceder a nuestras

redes sociales, ello se justifica a menudo por un interés vinculado al consumismo y a lo que Hochschild (2013) llama el «yo subcontratado»: cuando el yo se subcontrata, el mercado influye en la vida íntima y la vida social se organiza en torno a estos servicios, lo que lleva al desarrollo de aplicaciones y sitios *web* que ofrecen cada vez más trasladar y compartir detalles personales a entornos mercantilizados.

En esta misma línea, el concepto de «confesión maquínica» (Raunig, 2015/2023, pp. 145-146) apunta a una voluntad de postración ante unas plataformas digitales transformadas en «confesionario social» donde se vuelca el ansia por la «autodisección». De este modo, las personas se exponen a múltiples formas de vigilancia de las que, sin dejar de resentirse, pueden llegar a disfrutar. De ahí que la circulación de datos represente una consecuencia lógica de cómo se reestructura la vida social a través de un mercado dirigido a crear un ambiente donde compartir detalles personales se vuelva común.

Esta vigilancia a través de los datos o «*dataveillance*», término acuñado por Roger Clarke (1988), describe la supervisión de las actividades de una persona mediante la observación de su rastro de datos. Actualmente, esto abarca no solo compras con tarjeta de crédito y solicitudes de seguros sociales, sino también llamadas telefónicas, datos biométricos y el rastro que uno deja en Internet. Si bien usualmente hablamos de “recopilación de datos” para referirnos a cómo se obtiene la información, tal expresión puede resultar engañosa, ya que sugiere que los datos son frutos que se ofrecen de manera natural a la recolección.

Frente a ello, hemos expuesto cómo los datos requieren no poca mediación para ser extraídos. En este sentido, Gitelman y Jackson (2013) afirman que la creencia de que los datos parecen existir antes que los hechos, siendo la base de lo que sabemos sobre nosotros y cómo nos comunicamos, puede llevar a la suposición de que constituyen algo transparente, evidente. Así pues, lejos de la idea de que los datos se “recopilan”, “almacenan” y “procesan”, y de que la interpretación viene solo al final, estas autoras sugieren que la recolección y gestión de datos requieren interpretación desde el principio. En suma, los datos deben ser “generados” para existir, debiendo descartarse como un oxímoron cualquier concepción de la preexistencia de datos en bruto.

Por otra parte, nuestro doble de datos no solo se conforma a partir de textos y videos que producimos conscientemente, sino también de lo que Zuboff (2019/2020) llama «texto en la sombra», que es la información adicional que nuestros dispositivos generan al interactuar en la Red. También conocido como metadatos (esto es, datos sobre datos), dicho “texto”, incluye registros de actividad de nuestros dispositivos (como las llamadas que hacemos y el tiempo que pasamos viendo videos) y es creado automáticamente, sin que tengamos control sobre él. No en vano, Edward Snowden (2019) ya advertía

que nuestros dispositivos emiten comunicaciones constantemente, sin importar si lo deseamos.

En este sentido, si bien la mayoría de las personas tiende a pensar en la vigilancia de forma simple (esto es, concentrándose en el contenido de los mensajes), Snowden recuerda que el contexto de transmisión de datos es indisociable al contenido del mensaje, y advierte de que una concepción que reduzca la privacidad al contenido es la excusa perfecta para quienes argumentan que recopilar metadatos no es vigilar. Frente a ello, en esta tesis he enfatizado cómo el contenido de nuestras comunicaciones puede exponernos menos que los patrones de conducta revelados a través de los metadatos. Recordemos al respecto el ejemplo desarrollado a lo largo del punto 2.4., donde el dato de geolocalización recogido por una aplicación de control de ciclo menstrual puede suponer una prueba determinante, al agregarlo al resto de información sobre un embarazo, de si una persona se trasladó de un Estado restrictivo de EEUU a otro más permisivo con la intención de someterse a un aborto.

¿Cómo entendemos entonces nuestra relación con los datos y con cómo son captados por diferentes organizaciones a través de la vigilancia? Hemos visto con Kienscherf (2022) que hay dos grandes fuentes de valor en la mercantilización de los datos personales: su producción por los usuarios y el valor agregado por las plataformas, las cuales actúan sobre la actividad del usuario de maneras más cercanas a la expropiación que a la explotación. Por su parte, Ricaurte (2023) relaciona dicha expropiación con el «extractivismo de datos personales», que implica el despojo de recursos y formas de vida de las comunidades. De este modo, el extractivismo de materias primas que repasamos en el punto 1.1. se complementa con un extractivismo de comportamientos y relaciones mediadas por la tecnología digital, influenciando nuestra relación con el mundo.

Repasados y situados estos términos, resultaría sesgado simplemente aceptar un relato que se acerca a lo que Mattelart (1979, p. 9) señalaba como una «contrafascinación del poder», puesto que desde el comienzo de este trabajo, al discurso de cómo se conforma la autoridad y el control a través de la vigilancia le ha seguido el relato de cómo se entiende y se enfrenta ésta desde la ciudadanía, en lo que Foucault (1978/1998, p. 116) resumía con la afirmación de que «donde hay poder hay resistencia».

Pero llegados a este punto, conviene fijarnos también en cómo Ricaurte (2023, pp. 48-49) explica las resistencias, o como ella las denomina las «tecnorresistencias», al extractivismo de datos personales:

[E]ntiendo las tecnorresistencias como prácticas de reexistencia, es decir, formas de acción e intervención que buscan poner en marcha maneras dignas de existir en el mundo (Albán, 2013). [...] [Estas] resistencias pueden ser rupturas éticas, estéticas, políticas, es decir, alternativas materiales y epistémicas que dan cuenta de las diferencias ontológicas del

ser/saber/sentir/hacer/vivir-en-el mundo. En ese sentido, la resistencia es reexistencia (Albán, 2013) y puede adquirir múltiples formas: el juego, el arte, la recodificación o reescritura o la digna rabia, como lo mencionan las comunidades indígenas desde el Movimiento Zapatista que, como política oposicional, emerge de una conciencia diferencial (Sandoval 2004, p. 87).

Es aquí donde radica el objetivo principal que me propuse para este trabajo: analizar las tácticas de resistencia y reexistencia al extractivismo de datos que surgen desde la ciudadanía, esto es, aquélla que debe moverse en un espacio que no le es propio, pero que aun así inventa diferentes respuestas desde diferentes «posicionamientos» (Hartsock, 1983a; 1983b). Y todo ello con el fin de escapar del conocido como “efecto nocebo” (“dañaré” en latín) al que la epistemología de la citada “contrafascinación del poder” nos incita. Entendido como opuesto al conocido “efecto placebo”, con él me refiero a la sugestión de un daño (aquí la desconfianza y la sensación de que no hay nada que hacer) a través de un procedimiento azaroso. Frente a dicho efecto nocebo, solo cabe una inmunidad colectiva que parta, como propone Rebecca Solnit (2009, p. 49), de las mejores tendencias que afloran en medio del desastre:

Aceptando que las naturalezas humanas son varias, modeladas a partir de la cultura y las circunstancias —que cada uno de nosotros contiene multitudes—, puede que el desastre nos demuestre no quiénes somos siempre, o quiénes somos de forma general, sino quiénes podríamos ser y tendemos a ser en tales circunstancias.

En suma, en esta tesis he procurado explorar aquellas «tecnoresistencias» valiéndome de la propuesta de Michel de Certeau (1990, p. 46) de unos «modos de hacer» que combinan tres elementos clave: «una ética de la tenacidad» (que apela al inconformismo), una «estética de golpes» (que abre las invenciones técnicas al camuflaje y la sorpresa) y «un estilo de intercambios sociales» que, no obstante, puede persistir mucho mejor de lo que concebía el autor francés si, como propone Cabello (2019, p. 37), lo ubicamos en las coordenadas del procomún, esos “lugares comunes” donde preservar y recrear el legado de «operaciones de artistas» sin lugar propio (Certeau, 1990, p. 46).

Semejante reivindicación del procomún, que Peter Linebaugh (2008/2013, pp. 62-63) verbaliza como «hacer común», no solo resuena con la crítica histórica al extractivismo (y, más específicamente, a los “cercamientos” de ayer y de hoy), sino también con la clásica denuncia de Brunton y Nissenbaum (2011, párr. 12-16) sobre las «asimetrías de poder y saber» en este ámbito:

Primero, la asimetría de poder: rara vez podemos escoger si somos o no controlados, qué pasa con la información sobre nosotros y qué nos pasa a nosotros debido a ella. [...] Segunda, e igualmente importante, es la asimetría epistémica: a menudo no somos plenamente conscientes del control, y no sabemos lo que será de la información producida por dicho control, ni dónde acabará ni lo que puede hacerse con ella. [...] En cuanto personas cuyos datos son recopilados, lo que sabemos de la situación es problemático, y lo que no sabemos es sustancial.

Frente a esta formulación de las amenazas de la vigilancia digital, la definición de Yochai Benkler (2014, p. 70) del procomún como «libertad para operar bajo restricciones simétricas, disponible para una clase de usuarios abierta o indefinida» adquiere un nuevo sentido si lo trasladamos al campo que nos ocupa como base para un alegato a favor de la confluencia entre privacidad y procomún (de datos).

Tal confluencia entronca con argumentos conocidos de dos referentes de la cultura libre ya citados: por un lado, con la defensa de Lessig (2006/2009, pp. 371-372) de la plena coherencia de abogar por la libre circulación de obras creativas y científicas al tiempo que se articulan limitaciones a la difusión de datos personales; por otro, con la apuesta por la «autonivelación» que Keltz (2008/2019a, p. 72) atribuye a los públicos recursivos y que sostengo que cabe interpretar más allá del *software* libre:

Y es en su intento de hacer que el terreno de juego se autonivele donde plantan cara y se resisten a las formas de poder que tratan de nivelarlo en beneficio de una u otra parte: Estados, gobiernos, empresas o grupos profesionales. Es importante comprender que los *geeks* [...] desean inventar modos de dotar al terreno de juego de un cierto tipo de capacidad de acción, efectuada a través de la capacidad de acción de muchos seres humanos diferentes, pero revisada mediante su estructura y apertura técnica y legal. [...] Se trata de una ética de la justicia entreverada con una estética de elegancia técnica y astucia legal.

Finalmente, he destacado cómo Cabello (2019) propone aterrizar las prácticas del procomún en la estructura de tres «capas» (física, lógica y de contenidos) con la que Benkler (2006/2015) dota de coherencia los conflictos característicos de «la batalla por la ecología institucional del entorno digital».

De esta manera, he comenzado relatando el caso de NOYB, paradigma de una respuesta al extractivismo que he denominado “tácticas de la litigación colectiva”, por la que busca que las corporaciones cumplan la legislación de la UE sobre protección de datos, en particular el RGPD y la Directiva sobre privacidad en las comunicaciones electrónicas. De esta manera, NOYB interpone

reclamaciones contra compañías ante las autoridades de protección de datos de la UE o directamente en los tribunales. Con todo, he destacado que el aspecto más distintivo de NOYB es que, bajo un espíritu de los bienes comunes creativos y el conocimiento compartido, decidió publicar la mayor parte de su investigación de forma pública y gratuita a través de su propio *wiki*, el GDPRhub, y de esta manera permitir la modificación y actualización continua de la información con la ayuda de sus colaboradores voluntarios. Por ello puedo afirmar que este grupo de abogados contribuye a la preservación de la privacidad en el entorno europeo al tiempo que construye en las capas lógica y de contenidos un procomún de datos sobre su labor.

Sin embargo, que NOYB pueda operar de la forma que lo hace deriva de que cuenta con un marco legislativo que, antes del actual RGPD, ya reconocía la protección de datos como derecho fundamental desde los comienzos de la UE, tal y como hemos podido ver a lo largo del recorrido histórico por la legislación de la UE en esta materia. A partir de aquí, Lloredo Alix (2020, pp. 232-233) plantea abiertamente el debate sobre qué papel le correspondería al Derecho desde una concepción política de los comunes, a lo que responde de un modo bastante coherente con mi énfasis en la articulación de las tácticas en el marco del procomún:

De lo que se trataría es de resignificar y de emplear tácticamente las instituciones, en favor de la defensa de ciertos bienes comunes, o en aras de construir espacios de producción y reproducción comunitaria. [...] Del mismo modo que veíamos en páginas anteriores respecto a la ciudad, la red, los cuidados o la tierra, el objetivo sería «comunizar» el derecho, extrayéndolo del dominio exclusivo de los expertos —y del monopolio estatal— e inyectándolo de instancias de participación colectiva.

En relación a la presentación de las prácticas de «ofuscación» a la que dedico el Capítulo 4, hemos podido observar que, a pesar de que los múltiples proyectos ilustrativos difieren en ciertos detalles, comparten otros aspectos: en primer lugar, todas critican la tendencia a la datificación impulsada por el procesamiento algorítmico de grandes volúmenes de información; en segundo lugar, las tecnologías de ofuscación empleadas se dirigen a sistemas algorítmicos sobre los que interfieren como un “ruido de fondo”, más allá de que éste sea perceptible (como en los casos de *glamouflaging*) o no (como *AdNauseam* o *Nightshade*) por un observador humano. En definitiva, se trata de cortar las cadenas de suministro del sistema extractivista de datos, tal y como argumenta Harvey:

Esa es la idea: la forma en que se desarrollan los algoritmos ahora requiere una gran cantidad de datos aplicados, que a menudo provienen de fuentes en línea, extraídos de imágenes con licencia *Creative Commons*. Por lo tanto, la idea era: si no se tienen datos y no se pueden crear redes convolucionales, no se pueden entrenar todas estas redes sin millones de imágenes. Entonces, ¿qué pasa si se intenta cortar esa cadena de suministro? Entonces no se puede lograr. Es imposible crear estas redes neuronales sin suficientes datos; si no se tienen los datos, teóricamente, la vigilancia se desvanece (Harvey, comunicación personal, 14 de noviembre del 2023).

En tercer lugar, podemos afirmar que las tecnologías de ofuscación generalmente utilizan la automatización, si bien hablamos de una automatización táctica que busca eliminar su propia necesidad. Otro aspecto relevante es que estos dispositivos se pueden clasificar como tecnologías expresivas en la medida en que «no sólo existen para cumplir una función instrumental, sino también para amplificar perspectivas sociales, culturales o políticas» (Howe, 2015, p. 93). Por último, debemos tener en cuenta que la importancia relativa de los tres objetivos básicos de la ofuscación (protección, subversión y expresión) varía según el campo en que se despliega, de modo que, por ejemplo, en las tácticas empleadas en tiempos de guerra la protección es crucial, mientras que en proyectos artísticos lo que prima es la expresión. En este sentido, Howe detecta tensiones entre ciertos objetivos (de modo que si priorizamos una mayor protección ello puede significar una disminución de expresividad, y viceversa), aunque también señala ejemplos que muestran que ambos pueden coexistir.

En cuanto a las aportaciones al procomún que estos proyectos pueden ofrecer, resultan ampliamente dispares: algunos, como *Fango*, *Skilift* o *Data Pools*, emplean *software* y *hardware* libre, aunque estos proyectos se encuentran disponibles en repositorios de Github, por lo que no todos los componentes de su capa física se hallan estrictamente basados en el procomún, al igual que observamos en el caso de *Adnauseam*.

Otros ejemplos, por el contrario, resultan más restrictivos, destacando sobremanera el caso de Jing-cai Liu y sus compañeros, quienes se apresuraron a desmentir el rumor de que su proyecto *Wearable face protector* estaba siendo empleado por los manifestantes de Hong Kong, recalando que los derechos de autor del producto y del concepto seguían en sus manos. Si bien se confirmó que la relación con Hong Kong era finalmente falso, ello no despeja el debate acerca de la plausible reapropiación tecnológica táctica de proyectos como este que, aunque se desmarquen de vínculos partidistas o causas concretas, no dejan de ser especialmente políticos. De ahí que, por mucho que los autores quieran desvincularse

de los presuntos actos inspirados en su trabajo, realmente no pueden disociar la dimensión expresiva de la ofuscación de obras que, como sucedió en el contexto chino de 2019, movilizaba la imaginación y la acción de los manifestantes de Hong Kong sometidos a algunas técnicas sofisticadas de vigilancia, detección y represión en diferentes esferas como Internet, las calles, los mapas geolocalizados o las plataformas de redes sociales.

En cuanto a los proyectos de Ben Zhao y su equipo, se abre la cuestión aquí de si sería posible trasladar sus esfuerzos por la preservación de los derechos de autor de los artistas hacia, por ejemplo, la protección de la imagen personal de los usuarios de redes sociales que ven cómo sus rostros son empleados para el entrenamiento de modelos de aprendizaje automático de dichas plataformas. La otra peculiaridad destacable de *Glaze* y *Nightshade* radica en el propósito de cada uno y las decisiones estratégicas que los amparan. Así, llama la atención que mientras que *Glaze* ha renunciado a liberar su código bajo la justificación de dificultar la adaptación de los modelos de aprendizaje (Glaze, s.f., párr. 13), *Nightshade* sí ha apostado por el *software* libre, ya que ello permitiría a otros experimentar con ella y crear sus propias versiones. En efecto, sus impulsores sostienen que cuantas más personas lo usen y creen sus propias versiones, más potente se volverá la capacidad de contaminación de imágenes del modelo y mayor será el daño causado por esta vía (Heikkilä, 2023, párr. 5).

Con todo, Howe (2015) puntualiza que los sistemas de ofuscación suelen implicar iniciativas colectivas, a diferencia de los enfoques tradicionales de la privacidad centrados en la protección individual. De hecho, hemos visto que la ofuscación puede proteger incluso a quienes no la utilizan, ya que el ruido añadido puede afectar el valor de los datos recopilados. Con base en esta premisa cabe preguntarnos: ¿es posible institucionalizar la ofuscación de los datos personales? O dicho de otro modo, ¿es posible integrar las tácticas de ofuscación en la privacidad por diseño?

Cuestiones similares a esta se planteaba la profesora de la Facultad de Derecho de Harvard, Aileen Nielsen, durante el tercer *Workshop sobre Ofuscación* celebrado de manera *online* en mayo de 2021, concretamente dentro de una mesa redonda titulada *Obfuscation is dead? Long Live Obfuscation!* (¿La ofuscación ha muerto? ¡Larga vida a la ofuscación!). En ella Nielsen abogaba por una “ofuscación centralizada” que no debiera entrar en conflicto con la opción descentralizada y para cuya explicación retomaba el ejemplo de, efectivamente, la contaminación ambiental y las medidas que debemos tomar para paliarla (de manera individual pero también colectiva).

Nielsen también llamaba la atención hacia las problemáticas del empleo exclusivo de ofuscación descentralizada, temiendo que no ejerza la presión necesaria sobre las estructuras de mercado basada en

el extractivismo de datos, o que siga aportando soluciones solo para una parte de la población — aunque hemos visto que la vocación de la ofuscación es la de ayudar incluso a quien no la emplea. Asimismo ponía el foco sobre las externalidades negativas del empleo de técnicas de ofuscación para fines no legítimos —nótese que este tipo de actividades me guardaré de denominarlas “tácticas”, puesto que en ellas desaparece la acción polemológica que apuntaba Certeau—.

En contraposición, Nielsen sugería la posibilidad de instaurar una ofuscación centralizada en la práctica, nombrando como ejemplos las leyes que sugieren ofuscar por defecto los datos personales. En esta dirección citaba el caso de la UE y, más concretamente, la por entonces aún incipiente legislación sobre las herramientas de IA o la prohibición del uso de sistemas de identificación biométrica remota. Por último, retomaba su propuesta de combinar centralización con descentralización a través de los ejemplos del rastreo digital descentralizado de contactos desde una autoridad centralizada o del RGPD como estructura legal híbrida.

De hecho, al final de este trabajo he apuntado como ejemplo de este modelo el caso del proyecto piloto DECODE, que propone para Decidim una ofuscación selectiva de los datos personales de manera centralizada, esto es, por defecto desde la plataforma. Este procedimiento se enmarca en la actualidad en lo que se ha dado en llamar “privacidad diferencial”, definida así por la profesora de Ciencias de la Computación de Harvard Cynthia Dwork:

[L]a privacidad diferencial garantiza que la eliminación o adición de un solo elemento de la base de datos no afecte (sustancialmente) el resultado de ningún análisis. De ello se deduce que no se incurre en ningún riesgo al unir la base de datos, lo que proporciona un medio matemáticamente riguroso para abordar el hecho de que la información distributiva pueda ser reveladora [...] La privacidad diferencial es, por lo tanto, una garantía *ad omnia*. Además, es una garantía muy sólida, ya que es una propiedad estadística sobre el comportamiento del mecanismo y, por lo tanto, es independiente de la potencia computacional y de la información auxiliar disponible para el adversario/usuario (Dwork, 2008, p. 2).

Esta metodología es empleada por instituciones como la oficina del Censo de EEUU (United States Census Bureau, 2021), la Fundación Wikimedia (Adeleye *et al.*, 2023) y empresas como Apple (Apple, s.f.), y en España la fomenta la propia Agencia Española de Protección de Datos (2021, párr. 4-5) con la siguiente explicación:

La privacidad diferencial [t]iene su fundamento en la Ley de los Grandes Números, un principio estadístico que establece que cuando el tamaño de la muestra crece, los valores promedios que se derivan de la misma se aproximan al valor medio real de la información. De esa forma, la adición a todos los datos de un ruido aleatorio permite compensar estos efectos y producir un valor “esencialmente equivalente”.

El concepto “esencialmente equivalente” no significa que el resultado obtenido sea idéntico, sino que se refiere a que el resultado concreto a partir del análisis que se deriva del conjunto original de datos, y el resultado del conjunto al que se ha aplicado privacidad diferencial son, funcionalmente, equivalentes. Esta circunstancia permite incorporar la “negación plausible” de que los datos de un sujeto concreto estén en el conjunto de datos objeto de análisis. Para ello, el patrón de ruido incorporado a los datos ha de estar adaptado al tratamiento y los márgenes de exactitud que es necesario obtener.

¿Estamos entonces ante una solución aplicable a cualquier circunstancia donde se empleen estadísticas basadas en datos personales? Lo cierto es que, según la citada Dwork (2008, p. 3), la privacidad diferencial no es una garantía absoluta de privacidad pero, pese a todo, resulta adecuada para asegurar que solo se incurra en un riesgo adicional limitado en «las bases de datos socialmente beneficiosas».

Este último apunte sobre “bases de datos socialmente beneficiosas” es lo que quizá nos dé una pista esencial de cuándo resulta oportuno emplear la privacidad diferencial. Y ello porque cuando están en liza fines actuariales o lucrativos los riesgos de discriminación persisten porque, en última instancia, la privacidad diferencial enmascara la identidad de los participantes, sí, pero los sigue englobando dentro de un gran doble de datos descorporeizado —algo más parecido a las máscaras del *Facial Weaponization Suite* de Zach Blas que a un cuerpo digital propiamente dicho— que no nos libra ni de la datificación ni de los sesgos derivados de encasillarnos en un grupo más o menos aventajado según los datos recopilados. La privacidad diferencial no sería una gran solución cuando el fin de esta actividad no está vinculado a un bienestar colectivo, lo que nos lleva de vuelta al temprano énfasis de Helen Nissenbaum (2004) sobre el contexto como clave para determinar la legitimidad del tratamiento de los datos personales.

Una buena forma de condensar esto podemos tomarla de la conocida consigna *cyberpunk* «privacidad para los débiles, transparencia para los poderosos», que recupera Anderson (2022, p. 7) para situar el enfoque ciberpunk en el marco de un activismo de datos que Stefania Milan y Lonneke van der Velden

(2016, citadas en Anderson, 2022, p. 7) definen como una respuesta a la datificación de la vigilancia y la sociedad que aboga por un enfoque práctico y se involucra en (y se apropia de) la vigilancia digital y las tecnologías de datos. A modo de recapitulación, Anderson (2022, pp. 8-9) afirma que:

El eslogan *cyberpunk* «privacidad para los débiles, transparencia para los poderosos» encarna a la perfección la síntesis de las respuestas reactivas y proactivas del activismo de datos a la datificación. Cuando los *cyberpunks* abogan por el uso del cifrado para lograr la privacidad de los débiles, adoptan un enfoque reactivo. Las aplicaciones de mensajería con cifrado de extremo a extremo, las cuentas de correo electrónico cifradas, las redes privadas virtuales (VPN), el navegador *Tor* y *Bitcoin* encarnan el modo defensivo del activismo de datos. De igual manera, cuando los *cyberpunks* abogan por el uso del cifrado para lograr transparencia para los poderosos, adoptan un enfoque proactivo.

Como forma de activismo de datos, la epistemología *cyberpunk* comprende la datificación de las relaciones sociales y responde con estrategias prácticas de resistencia, proactivas y reactivas, ofensivas y defensivas. Como tal, representa una forma de lo que Matthew Zaia (2019) ha denominado conciencia de vigilancia oposicional y participativa. La epistemología *cyberpunk* es oposicional porque cuestiona las relaciones de poder al oponerse a la vigilancia, y participativa porque se involucra con las tecnologías digitales que posibilitan la vigilancia contemporánea, convirtiéndolas en tecnologías de resistencia.

Fomentar una cultura de la privacidad como bien común requiere, por tanto, de un enfoque multifacético que aborde tanto las dimensiones tecnológicas como sociales de la privacidad, al hilo del el esquema de cuatro reguladores —ley, norma social, mercado y arquitectura— de Lessig (2006/2009, p. 207). Así, para promover la privacidad como un procomún y salvaguardar los principios democráticos que emanan de ella resulta necesario que todas las organizaciones colaboren para establecer leyes y políticas que protejan los derechos de privacidad desde una perspectiva colectiva. Esto incluye implementar regulaciones sólidas de protección de datos (o hacerlas cumplir en territorios que ya lo hayan hecho, tarea de NOYB en la UE) que comiencen por la premisa de minimizar su recolección, garantizar la transparencia y la rendición de cuentas sobre su tratamiento, y proporcionar a las personas las herramientas y el conocimiento para controlar su información personal.

En el plano tecnológico, allá donde sea inevitable la recopilación de datos personales, sería conveniente implantar tecnologías seguras que preserven la privacidad por diseño. Hablamos, entre otras, de las

técnicas de autenticación unidireccional criptográfica como garantía de seudonimización en el tratamiento de datos personales que vimos en el caso de Decidim, o la metodología de la privacidad diferencial para realizar estadísticas basadas en dicha información. También se torna importante educar a las personas sobre la importancia de la privacidad digital y fomentar una ética colectiva de respeto por el derecho a la misma. Al construir una ciudadanía consciente de la privacidad, podemos crear una sociedad más resiliente que valore la privacidad como un bien común y trabaje activamente para defenderla como un pilar democrático inmune al extractivismo.

Para poder desarrollar este trabajo de una manera fructífera estimo oportuno que centremos nuestra atención en aquellos territorios con una vasta experiencia en la práctica comunitaria, tal y como ejemplifica la investigadora, lingüista y activista mixe Yásnana Aguilar (2020, párr. 4):

Este trabajo colaborativo de apoyo mutuo tiene un pasado profundo. Para muchos pueblos de México, este se llama *tequio* (del náhuatl *tequitl*) o *faena*, *kol*, o *minga* más al sur del continente. Por medio del *tequio* se han construido escuelas, se han instalado sistemas de agua potable, se han realizado proyectos artísticos y se ha convertido en una estrategia de resolución de las necesidades de la vida cotidiana. Así como la condición abierta del código libre permite un avance conjunto, desde Abya Yala¹⁶¹, el trabajo colaborativo del *tequio* plantea una posibilidad de resistencia y puede dar también una esperanza ante una crisis climática que pone en riesgo la vida humana.

Para Ricaurte (2022, p. 61), el *tequio* no se puede llevar a cabo individualmente, por lo que al ser concebido como una responsabilidad compartida, se puede conseguir un mayor alcance en menor tiempo. A su vez, implica un compromiso a largo plazo, así como la certeza de que con dicha participación existirá un futuro en el que ese trabajo o recursos serán compensados, intensificando así la responsabilidad colectiva de una comunidad hacia cada uno de sus miembros. Este método de trabajo sitúa la acción colectiva como núcleo de un universo de relaciones mutuas que implican un compromiso por la dignidad mediante la consecución conjunta de metas compartidas. Tal y como continúa argumentando Ricaurte (2022, p. 62), si incorporamos estos principios de mutualidad, pluriversalidad y comunalidad al ámbito tecnológico, su percepción no podría separarse de una participación colectiva que involucra a todos los individuos que constituyen la comunidad, donde se establece un objetivo compartido y se responsabiliza a todos ellos. Por ello, Aguilar (2022, párr. 33) nos invita a pensar con el término “tequiologías”, neologismo del concepto de *tequio*, para concebir la

¹⁶¹Abya Yala es el término, en lengua guna de Panamá, con el que se nombraba al continente americano desde antes de 1492.

tecnología desde la mutualidad y el desarrollo colaborativo, apuntando que el *software* libre sería lo más próximo al concepto de *tequio*. Bajo esta concepción, Ricaurte (2022, p. 65) ofrece una conclusión que considero clave compartir como fin de esta reflexión:

Por eso es urgente pensar las tecnologías en relación con las luchas en primera línea en el continuo cuerpo-territorio, porque las opresiones se encuentran interconectadas y los sistemas sociotécnicos son fundamentales en su reproducción. Empezar a reparar los daños implica hacernos corresponsables de las afectaciones y no invisibilizar las luchas de las personas defensoras de la tierra, de los pueblos originarios, las mujeres, las diversidades sexo-genéricas, las trabajadoras precarizadas, que buscan defender el derecho a una vida digna y que nos permiten imaginar otros futuros posibles libres de violencia, tequiológicos.

Conclusions

Throughout this work, I have devoted many lines attempting to dismantle certain deeply held beliefs regarding various concepts linked to the topic of this thesis. Motivated by a critical conception of history —thanks in part to the work of Silvia Federici, as well as the writings of David Graeber and David Wengrow, among others— I felt it necessary to pause and describe where these beliefs come from and why we perceive issues related to surveillance, privacy, and the treatment of personal data within an extractive system the way we do.

This is important because, as Paola Ricaurte (2023, p. 57) points out, «extractivism in terms of technological development is also associated with the construction of narratives, discourses, and imaginaries» that seek to impose a single story and future, as well as the idea that one can not live outside such system and, therefore, collective action is not viable.

Thus, if we look back at some historical examples, especially from Europe and America, we see how the power of various governments has been maintained through surveillance of their populations. To this end, the establishment of writing was fundamental, as it facilitated the supervision of a larger number of people, which explains why popular insurrections often began with the destruction of records of debts and possessions. The arrival of the printing press made it possible to spread administrative power, although modern surveillance, in the 19th century, also expanded with militarization and industry. All of this leads us to understand that, although surveillance is not new, it has evolved thanks to increasingly advanced recording techniques.

We have also seen that, over the course of the modern era, surveillance gradually overlaps physical coercion and spectacle in the maintenance of order. The greater ease for the population to move to other territories meant that states increased their control capacity, first of marginalized groups and then extending it to the general population. This was later accompanied by the expansion of bureaucratic organization, evident both in modern armies and in state organizational systems, as well as in capitalist corporations. In turn, the expansion of citizens' rights linked to the emergence of welfare states entailed greater monitoring and registration of the population, which often resulted in heightened scrutiny of the historically most vulnerable groups.

By the end of the 20th century, the expansion of microelectronic technologies increased the capacity for surveillance. Today, it has changed and is more fluid and flexible, although I must emphasize that it still coexists with traditional forms of control. However, this new type of «post-panoptic surveillance»

(Bauman and Lyon, 2013, pp. 61-84) is based on mobility and connectivity, where information technologies and networks are more relevant than institutions. Therefore, surveillance now operates remotely, managing data flows and classifying people. This cyber surveillance is characterized by the predictive tracking of behavior through algorithms, generating disadvantages for many by treating people as data.

Throughout the text, I have also pointed out how corporations have cooperated with the surveillance systems of states, reinforcing the Military-Industrial complex towards a «Military-digital complex» against which McChesney warned (2014, pp. 158-171).

On the other hand, and in the name of security, people have become accustomed to being observed and located in certain spaces, which has led to a loss of our privacy. At the same time, we have increasingly shifted our presence to a digitalized world dominated by «datafication» and «dataism» (van Dijck, 2014), that is, the belief that human behavior can be objectively quantified and the complete trust placed in those who handle such data. This has repercussions, for example, on how one of the most important methods for generating wealth for companies operating on the Internet is the monitoring of their users and the extraction of their personal data. All of this is based on the fact that the moment we upload parts of our lives to the Internet, we assume that there is a real lack of privacy.

However, far from these self-serving proclamations that dismiss the possibility of such privacy, we have also noted how it should no longer be viewed as an individual issue. Indeed, underlying this thesis is the argument that privacy is important not only as a value that protects individuals from abuse, but also because living in a society that collectively defends privacy in turn protects other equally important values, such as equality, justice, and democracy.

Based on this argument, Solove's privacy taxonomy has allowed me to systematically present related dilemmas from «a bottom-up descriptive account of the kinds of privacy problems that are addressed in various discussions» (Solove, 2009, p. 172), although we must keep in mind that these problems are not immutable. Nevertheless, the main function of this approach is to shift theoretical discussions about privacy from a unified conception to a focus on the diverse problems generated around it, which provides greater clarity when addressing the risks of privacy loss.

In summary, we can say that privacy is a fundamental right because its value is linked to collective well-being. However, it is important to note that protecting individual privacy should not harm society; in fact, its value must be justified by the social benefits it provides. Thus, it is not an absolute, superior value: we live in a community, which connects our well-being to that of others.

Ultimately, the value of privacy must be understood through its contribution to society, even if its value is often argued in terms of individual rights. Consequently, privacy should not be viewed solely as a defense against social control, but as a socially constructed protection against various problems, all of them crucial to autonomy, security, equality, and justice. Therefore, it becomes especially necessary to consider specific contexts when assessing privacy and the conflicting interests in each situation.

This is where I believe Nissenbaum's (2004) concept of «privacy as contextual integrity» is most appropriate, as it recognizes the importance of preserving this right in diverse social contexts, assuming that different environments require different levels of privacy, and that the norms surrounding it may vary depending on the specific context. To maintain contextual integrity, then, people must be aware of the expectations and norms of a particular environment and be able to manage these boundaries effectively.

On the other hand, we have seen how, as people increasingly integrate into online life, connected devices become part of our daily lives, causing our social and self-perceptions to change. These changes affect how we live and form our identities in the digital age. It is important to understand here that we not only perceive others through data, but we can also come to see ourselves in those terms. In this sense, Haggerty and Ericson (2000) introduced the concept of the «data double» to describe the interest in controlling fragments of personal data, especially what it implies when the body is divided into streams of information for analysis. This data double, while not representative of one person, can influence her daily life and, in some cases, can prevail over her own word.

Another issue analyzed is how we crave and use all these devices we have mentioned. While we want to stay online, download apps, and access our social networks, this is often justified by an interest linked to consumerism and what Hochschild (2013) calls the «outsourced self»: when the self is outsourced, the market influences intimate life, and social life is organized around these services, leading to the development of apps and websites that increasingly offer the transfer and sharing of personal details into commodified environments.

Along these same lines, the concept of «machinic confession» (Raunig, 2015/2023, pp. 145-146) points to a desire to prostrate ourselves before digital platforms transformed into social confessionals where the desire for self-dissection is poured out. In this way, people are exposed to multiple forms of surveillance that, while resenting it, they may even come to enjoy. Hence, the circulation of data represents a logical consequence of how social life is restructured through a market aimed at creating an environment where sharing personal details becomes commonplace.

This data surveillance, or «dataveillance», a term coined by Roger Clarke (1988), describes the monitoring of a person's activities by observing their data trail. Currently, this encompasses not only credit card purchases and social security applications, but also phone calls, biometric data, and the trail one leaves on the internet. While we often refer to “data collection” to refer to how information is obtained, this expression can be misleading, as it suggests that data are naturally available for harvesting.

In sharp contrast to this, we have shown how data require considerable mediation to be extracted. In this regard, Gitelman and Jackson (2013) assert that the belief that data seem to exist before facts, being the basis of what we know about ourselves and how we communicate, can lead to the assumption that they constitute something transparent and self-evident. Thus, far from the idea that data are “collected,” “stored,” and “processed,” and that interpretation comes only at the end, these authors suggest that data collection and management require interpretation from the very beginning. In short, data must be “generated” to exist, and any notion of the preexistence of raw data should be dismissed as an oxymoron.

Moreover, our data double is not only made up of texts and videos we consciously produce, but also of what Zuboff (2019/2020) calls «shadow text», which is the additional information our devices generate when we interact online. Also known as metadata (i.e., data about data), this “text” includes activity logs from our devices (such as the calls we make and the time we spend watching videos) and is created automatically, without us having any control over it. Not in vain, Edward Snowden (2019) already warned that our devices constantly emit communications, regardless of whether we want them to.

In this sense, while most people tend to think of surveillance in a simplistic way (that is, focusing on the content of messages), Snowden reminds us that the context of data transmission is inextricably linked to the content of the message, and warns that a conception that reduces privacy to content is the perfect excuse for those who argue that collecting metadata is not surveillance. Against this background, in this thesis I have emphasized how the content of our communications can expose us less than the behavioral patterns revealed through metadata. In this regard, let us recall the example developed throughout section 2.4, where the geolocation data collected by a menstrual cycle tracking app can provide decisive evidence, when combined with other information about a pregnancy, as to whether a person moved from a restrictive US state to a more permissive one with the intention of having an abortion.

Then, how do we understand our relationship with data and the way it is captured by different organizations through surveillance? We have seen with Kienscherf (2022) that there are two major

sources of value in the commodification of personal data: its production by users and the value added by platforms, which act on user activity in ways closer to expropriation than exploitation. Ricaurte (2023) links this expropriation to personal data extractivism, which involves the dispossession of resources and ways of life from communities. In this way, the extractivism of raw materials we reviewed in section 1.1 is complemented by an extractivism of behaviors and relationships mediated by digital technology, influencing our relationship with the world.

Having reviewed and situated these terms, it would be biased to simply accept a narrative that comes close to what Mattelart (1979, p. 9) referred to as a «counter-fascination of power». Since the beginning of this work, the discourse on how authority and control are shaped through surveillance has been followed by the narrative of how it is understood and confronted by citizens, in what Foucault (1978/1998, p. 116) summarized with the statement that «where there is power, there is resistance».

But at this point, it is also worth looking at how Ricaurte (2023, pp. 48-49) explains the resistances, or as she calls it, «techno-resistances», to the extraction of personal data:

I understand techno-resistances as practices of re-existence, that is, forms of action and intervention that seek to put in motion dignified ways of existing in the world (Albán, 2013). [...] [These] resistances can be ethical, aesthetic, or political ruptures; that is, material and epistemic alternatives that account for the ontological differences of being/knowing/feeling/doing/living-in-the-world. In that sense, resistance is re-existence (Albán, 2013) and can take multiple forms: play, art, recodification or rewriting, or dignified rage, as mentioned by indigenous communities from the Zapatista Movement, which, as an oppositional politics, emerges from a differential consciousness (Sandoval 2004, p. 87).

This is where the main objective I set for myself for this work lies: to analyze the tactics of resistance and re-existence to data extractivism that emerge from citizens, that is, those who must navigate a space that is not their own, but who nevertheless invent different responses from different «standpoints» (Hartsock, 1983a; 1983b). And all of this with the aim of escaping the so-called nocebo effect (“I will harm” in Latin) to which the epistemology of the aforementioned counterfascination of power incites us. Understood as opposed to the well-known placebo effect, I refer to the suggestion of harm (here, distrust and the feeling that nothing can be done) through a random process. In the face of this nocebo effect, the only possible solution is a collective immunity that stems, as Rebecca Solnit (2009, p. 49) proposes, from the best tendencies that emerge in the midst of disaster:

if you concede that there are many human natures, shaped by culture and circumstance,

that each of us contains multitudes, then the majority of human natures on display in disaster may not suggest who we are ordinarily or always, but they do suggest who we could be and tend to be in these circumstances.

In sum, in this thesis I have sought to explore techno-resistances by drawing on Michel de Certeau's (1990, p. 46) proposal of arts of practice combining three key elements: an ethic of tenacity (which appeals to nonconformity), an aesthetics of tricks (which opens technical inventions to camouflage and surprise), and a style of social exchange that, however, can persist much better than envisioned by the French author if, as Cabello (2019, p. 37) proposes, we locate it within the coordinates of the commons, those common places where the legacy of artists' operations without their own place can be preserved and recreated (Certeau, 1990, p. 46).

This way of reclaiming to the commons, which Peter Linebaugh (2008/2013, pp. 62-63) verbalizes as “commoning,” not only resonates with the historical critique of extractivism (and, more specifically, of the past and present “enclosures”), but also with Brunton and Nissenbaum's (2011, par. 12-16) classic denunciation of the “asymmetries of power and knowledge” in this area:

First, the asymmetry of power: rarely do we get to choose whether or not we are monitored, what happens to information about us, and what happens to us because of this information. [...] Second, equally important, is an epistemic asymmetry: we are often not fully aware of the monitoring, and do not know what will become of the information produced by that monitoring, nor where it will go and what can be done to it. [...] As people whose data is being collected, what we know of the situation is problematic, and what we do not know is substantial.

In the face of this formulation of the threats posed by digital surveillance, Yochai Benkler's (2014, p. 70) definition of the commons as «freedom-to-operate under symmetric constraints, available to an open, or undefined, class of users», takes on new meaning when applied to the field we are discussing as a basis to make a case for the convergence of privacy and (data) commons.

This convergence aligns with arguments made by two well-known free culture advocates: on one hand, with Lessig's (2006/2009, pp. 371-372) advocacy of the free circulation of creative and scientific works while also recognizing limitations on the dissemination of personal data; on the other hand, with the commitment to «self-leveling» that Kelty (2008/2019a, p. 72) attributes to recursive publics, which I believe can be interpreted beyond just free software:

And it is in the attempt to make the playing field self-leveling that they confront and resist forms of power and control that seek to level it to the advantage of one or another large constituency: state, government, corporation, profession. It is important to understand that geeks [...] wish to devise ways to give the playing field a certain kind of agency, effected through the agency of many different humans, but checked by its technical and legal structure and openness. [...] It is an ethic of justice shot through with an aesthetic of technical elegance and legal cleverness.

Finally, I highlighted how Cabello (2019) proposes grounding common practices in the three-layer structure (physical, logical, and content) with which Benkler (2006/2015) provides coherence to the conflicts characteristic of «the battle for the institutional ecology of the digital environment».

Thus, I began by recounting the case of NOYB, paradigmatic of a response to extractivism that I have termed “collective litigation tactics”, which seeks to force corporations to comply with EU data protection legislation, particularly the GDPR and the ePrivacy Directive. In this way, NOYB files claims against companies before EU data protection authorities or directly in court. All in all, I have highlighted that the most distinctive aspect of NOYB is that, in the spirit of creative commons and shared knowledge, it decided to publish most of its research publicly and freely through its own wiki, the GDPRhub, thus allowing for continuous modification and updating of the information with the help of its volunteer contributors. Therefore, I can affirm that this group of lawyers contributes to the preservation of privacy in the European environment while building a data commons about its work.

However, the fact that NOYB can operate this way stems from the fact that they have a legislative framework that, prior to the current GDPR, already recognized data protection as a fundamental right since the beginning of the EU, as we have seen throughout the historical journey through EU legislation on this matter. On this basis, Lloredo Alix (2020, pp. 232-233) openly raises the debate about what role the law would play from a political conception of the commons, to which he responds in a way quite coherent with my emphasis on the articulation of tactics within the framework of the commons.

The challenge would be to resignify and tactically employ institutions in order to defend certain common goods, or to build spaces for community production and reproduction. [...] Just as we saw in previous pages regarding the city, internet, care, or the land, the objective is a «commoning» of the law, extracting it from the exclusive domain of experts—and state monopoly—, and injecting it with instances of collective participation.

Regarding the presentation of «obfuscation» practices to which I dedicate Chapter 4, we have observed that, although the multiple illustrative projects differ in certain details, they share certain aspects: first, they all criticize the trend toward datafication driven by the algorithmic processing of large volumes of information; second, the obfuscation technologies employed target algorithmic systems, with which they interfere as “background noise”, regardless of whether this noise is perceptible (as in the cases of *glamouflage*) or not (as in *AdNauseam* or *Nightshade*) by a human observer. Ultimately, it is about cutting off the supply chains of the extractive data system, as Harvey argues:

That’s the idea, is that the way that algorithms are developed now requires a large applied data, that data often come from online sources, scrape from Creative Commons license imagery and so the idea was, well if you don't have data and you can't make the convolutional networks, they can't train it all these networks without millions of images. So, what if you try to cut that supply chain? Then you can't do it. It’s impossible to make these neural networks without enough data, if you don't have the data then surveillance evaporates (Harvey, personal communication, November 14, 2023).

Third, we can affirm that obfuscation technologies generally use automation, although we are speaking of a tactical automation that seeks to eliminate its own necessity. Another relevant aspect is that these devices can be classified as expressive technologies to the extent that they exist «not only to serve some instrumental function, but always also to amplify social, cultural or political perspectives» (Howe, 2015, p. 93). Finally, we must bear in mind that the relative importance of the three basic objectives of obfuscation (protection, subversion, and expression) varies depending on the field in which it is deployed. For example, in tactics employed in wartime, protection is crucial, while in artistic projects, expression is paramount. In this sense, Howe detects tensions between certain objectives (so that prioritizing greater protection may mean a decrease in expressiveness, and vice versa), although he also points to examples showing that they can coexist.

As for the contributions to the commons that these projects can offer, they are widely disparate: some, such as *Fangø*, *Skilift*, or *Data Pools*, use free software and hardware, although these projects are available in GitHub repositories, so not all of their physical layer components are strictly based on the commons, as we observe in the case of *Adnauseam*.

On the other hand, other examples are more restrictive. Particularly notable in this regard is the case of Jing-cai Liu and his colleagues, who were quick to deny the rumor that their *Wearable Face Protector* project was being used by Hong Kong protesters, emphasizing that the copyright to the product and

the concept remained with them. While the link to Hong Kong was ultimately confirmed to be false, this does not settle the debate about the plausible tactical technological reappropriation of projects like this one, which are distinctively political even if they distance themselves from partisan ties or specific causes. Hence, however much as the authors wish to disassociate themselves from the alleged acts inspired by their work, they cannot truly dissociate the expressive dimension of the obfuscation of projects that, as happened in the Chinese context of 2019, mobilized the imagination and action of Hong Kong protesters subjected to sophisticated techniques of surveillance, detection, and repression in different spheres such as the Internet, the streets, geolocated maps, or social media platforms.

As for the projects of Ben Zhao and his team, the question here is whether it would be possible to transfer their efforts to preserve artists' copyright to, for example, the protection of the personal images of social media users who see their faces used to train machine learning models on these platforms. The other notable peculiarity of *Glaze* and *Nightshade* lies in the purpose of each and the strategic decisions that support them. Thus, it is striking that while *Glaze* has renounced releasing its code under the justification of making it difficult for learning models to adapt to it (Glaze, n.d., par. 13), *Nightshade* has opted for free software, as this would allow others to experiment with it and create their own versions. Indeed, its proponents argue that the more people who use it and create their own versions, the more potent the model's image contamination capacity becomes, and the greater the damage caused by this approach (Heikkilä, 2023, para. 5).

However, Howe (2015) points out that obfuscation systems often involve collective initiatives, unlike traditional approaches to privacy focused on individual protection. Indeed, we have seen that obfuscation can protect even those not using it, as the added noise can affect the value of the collected data. Based on this premise, we may ask: Is it possible to institutionalize the obfuscation of personal data? Or, to put it another way, is it possible to integrate obfuscation tactics into privacy by design?

Harvard Law School professor Aileen Nielsen raised similar questions during the third Workshop on Obfuscation held online in May 2021, specifically within a roundtable entitled "Obfuscation is dead? Long Live Obfuscation!". In it, Nielsen advocated for a centralized obfuscation that should not conflict with the decentralized option. To explain this, she returned to the example of, indeed, environmental pollution and the measures we must take to mitigate it (individually but also collectively).

Nielsen also drew attention to the problems of the exclusive use of decentralized obfuscation, fearing that it might not exert the necessary pressure on market structures based on data extraction, or that it might continue to provide solutions only for a portion of the population—although we have seen that

obfuscation's purpose is to help even those not using it. She also focused on the negative externalities of using obfuscation techniques for illegitimate purposes—note that I will refrain from considering these types of activities as tactics, since they eliminate the polemological action Certeau pointed out.

In contrast, Nielsen suggested the possibility of implementing centralized obfuscation in practice, citing as examples laws that suggest obfuscating personal data by default. In this regard, she cited the case of the EU and, more specifically, the then-still-nascent legislation on AI tools or the ban on the use of remote biometric identification systems. Finally, she returned to her proposal for combining centralization with decentralization through the examples of decentralized digital contact tracing from a centralized authority, or the GDPR as a hybrid legal structure.

In fact, at the end of this paper, I pointed out as an example of this model the DECODE pilot project, which offers Decidim a selective obfuscation of personal data in a centralized manner, that is, by default from the platform. This procedure currently falls under what has been called “differential privacy”, as defined by Harvard Computer Science professor Cynthia Dwork:

[D]ifferential privacy ensures that the removal or addition of a single database item does not (substantially) affect the outcome of any analysis. It follows that no risk is incurred by joining the database, providing a mathematically rigorous means of coping with the fact that distributional information may be disclosive. [...] Differential privacy is therefore an *ad omnia* guarantee. It is also a very strong guarantee, since it is a statistical property about the behavior of the mechanism and therefore is independent of the computational power and auxiliary information available to the adversary/user (Dwork, 2008, p. 2).

This methodology is used by institutions such as the United States Census Bureau (United States Census Bureau, 2021), the Wikimedia Foundation (Adeleye *et al.*, 2023), and companies such as Apple (Apple, n.d.). In Spain, it is promoted by the Spanish Data Protection Agency itself (2021, par. 4-5) with the following explanation:

Differential privacy is based on the Law of Large Numbers, a statistical principle that establishes that as the sample size grows, the average values derived from it approach the true mean value of the information. Thus, adding random noise to all the data compensates for these effects and produces an essentially equivalent value.

The concept of essentially equivalent does not mean that the result obtained is identical; rather, it refers to the fact that the specific result derived from the analysis of the original

data set and the result of the data set to which differential privacy has been applied are functionally equivalent. This circumstance allows for the plausible denial that a specific subject's data are in the data set under analysis. To achieve this, the noise pattern incorporated into the data must be adapted to the processing and accuracy margins required.

So, are we confronted with a solution applicable to any circumstance where statistics based on personal data are used? The truth is that, according to the aforementioned Dwork (2008, p. 3), differential privacy is not an absolute guarantee of privacy, but it is nevertheless adequate to ensure that only a limited additional risk is incurred in socially beneficial databases.

This last note about «socially beneficial databases» is perhaps what gives us an essential clue as to when it is appropriate to employ differential privacy. And this is because when actuarial or profit-making ends are at stake, the risks of discrimination persist because, ultimately, differential privacy masks the identity of the participants, that is true, but it continues enclosing them within a large, disembodied data double—something more similar to the masks in Zach Blas's *Facial Weaponization Suite* than to a digital body per se—that does not free us from either datafication or the biases derived from pigeonholing us into a more or less advantaged group according to the data collected. Differential privacy would not be a great solution when the purpose of this activity is not linked to collective well-being, which brings us back to Helen Nissenbaum's (2004) early emphasis on context as key to determining the legitimacy of the processing of personal data.

A good way to sum up this can be found in the well-known cypherpunk slogan "privacy for the weak, transparency for the powerful," which Anderson (2022, p. 7) takes up to place the cyberpunk approach within the framework of data activism, defined by Stefania Milan and Lonneke van der Velden (2016, cited in Anderson, 2022, p. 7) as a response to the datafication of surveillance and society. This activism advocates for a practical approach and engages in (and appropriates) digital surveillance and data technologies. To recap, Anderson (2022, pp. 8-9) states that:

The cypherpunk slogan “privacy for the weak, transparency for the powerful” perfectly embodies the synthesis of re-active and pro-active responses of data activism to datafication. When the cypherpunks advocate the use of encryption to achieve privacy for the weak, they are taking a re-active approach to their activism. End-to-end encrypted messaging applications, encrypted email accounts, virtual private networks (VPNs), Tor browser, and Bitcoin all embody the defense mode of data activism. Likewise, when

cypherpunks advocate for the use of encryption to achieve transparency for the powerful, they are taking a pro-active approach to their activism.

As a form of data activism, then, cypherpunk epistemology understands the datafication of social relations and responds with practical pro-active and re-active, offensive and defensive, strategies of resistance. As such, cypherpunk epistemology represents a form of what Matthew Zaia (2019) has called oppositional and participatory surveillance consciousness. Cypherpunk epistemology is oppositional because it contests power relations by going up against surveillance, and it is participatory because it engages the digital technologies that make contemporary surveillance possible, turning those technologies into technologies of resistance.

Therefore, promoting a culture of privacy as a common good therefore requires a multifaceted approach that addresses both the technological and social dimensions of privacy, along the lines of Lessig's (2006/2009, p. 207) framework of four regulators—the law, social norm, the market, and the architecture. Thus, to promote privacy as a commons and safeguard the democratic principles that emanate from it, it is necessary for all organizations to collaborate in order to establish laws and policies that protect privacy rights from a collective perspective. This includes implementing robust data protection regulations (or enforcing them in territories where they are already in place, as NOYB does in the EU) that are built on the premise of minimizing data collection, ensuring transparency and accountability regarding its processing, and providing people with the tools and knowledge to control their personal information.

In the technological realm, wherever the collection of personal data is unavoidable, it would be advisable to implement secure technologies that preserve privacy by design. We discussed, among other things, cryptographic one-way authentication techniques as a guarantee of pseudonymization in the processing of personal data, which we saw in the Decidim case, and the differential privacy methodology for generating statistics based on such information. It is also important to educate people about the importance of digital privacy and foster a collective ethic of respect for the right to it. By building a privacy-aware citizenry, we can create a more resilient society that values privacy as a common good and actively works to defend it as a democratic pillar immune to extractivism.

In order to develop this work in a fruitful manner, I consider it appropriate that we focus on those territories with vast experience in community practice, as exemplified by the Mixe researcher, linguist,

and activist Yásnana Aguilar (2020, par. 4):

This form of collaborative effort has ancient roots. To many peoples in Mexico, it is known as *tequio* (from the Náhuatl *tequitl*) or, farther south, as *faena*, *kol*, or *minga*. Through *tequio*, schools have been built, potable-water systems have been installed, and art has been made. *Tequio* has also become a strategy for meeting everyday needs. Just as the modern-day technology of free, open-source code has enabled collective progress in the digital sphere, the communal labor of *tequio* raises the possibility of resistance in Abya Yala¹⁶² — and survival of the world at large.

For Ricaurte (2022, p. 61), *tequio* can not be carried out individually, so its conception as a shared responsibility enables to achieve a greater scope in less time. In turn, it implies a long-term commitment, as well as the certainty that with such participation there will be a future in which those efforts or resources will be compensated, thus intensifying the collective responsibility of a community toward each of its members. This working method places collective action at the core of a universe of mutual relationships that imply a commitment to dignity through the joint achievement of shared goals.

As Ricaurte (2022, p. 62) continues to argue, if we incorporate these principles of mutuality, pluriversality, and communality into the technological field, their perception could not be separated from a collective participation involving all the individuals that constitute the community, who are then held accountable when establishing shared objectives. For this reason, Aguilar (2022, para. 33) invites us to think with the term *tequilogies*, a neologism drawn from the concept of *tequio*, so as to conceive technology from the perspective of mutuality and collaborative development, pointing out that free software would be the closest thing to the *tequio*. Under this conception, Ricaurte (2022, p. 65) offers a conclusion that I consider key to share as the end of this reflection:

That is why it is urgent to consider technologies in relation to frontline struggles within the body-territory continuum, because oppressions are interconnected, and sociotechnical systems are fundamental to their reproduction. Beginning to repair the damage implies taking joint responsibility for the impacts and not rendering invisible the struggles of land defenders, indigenous peoples, women, gender diversity, and precarious workers, who seek to defend the right to a dignified life and who allow us to imagine other possible, *tequilogical* futures free of violence.

¹⁶²Abya Yala is the term that the Guna people of Panama use to describe the Western Hemisphere's largest landmass as it existed before 1492.

Bibliografía

Bibliografía

Abercrombie, Nicholas; Hill, Stephen; Turner, Bryan S. (1986). *Sovereign Individuals of Capitalism*. Routledge.

Ácido perfluorooctanoico. (24 de enero de 2024). En *Wikipedia*.
https://es.wikipedia.org/w/index.php?title=%C3%81cido_perfluorooctanoico&oldid=157623683

Adversarial Fashion. (s.f.). DEFCON 27 Crypto & Privacy Presentation. *Adversarial fashion*.
<https://adversarialfashion.com/>

Adeleye, Temilola; Berghel, Skye; Desfontaines, Damien; Hay, Michael; Johnson, Isaac; Lemoisson, Cléo; Machanavajjhala, Ashwin; Magerlein, Tom; Modena, Gabriele; Pujol, David; Simmons-Marengo, Daniel y Triedman, Hal. (2023). Publishing Wikipedia usage data with strong privacy guarantees.
<https://doi.org/10.48550/arXiv.2308.16298>

AEPD. (15 de noviembre de 2019). Cifrado y Privacidad: cifrado en el RGPD. *AEPD*.
<https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-y-privacidad-cifrado-en-el-rgpd>

AEPSAL. (27 de junio de 2017). La UE prohíbe el PFOA, un disruptor endocrino presente en el teflón de las sartenes y el hilo dental. *Asociación de Especialistas en Prevención y Salud Labora*.
<https://www.aepsal.com/disruptor-endocrino/>

Agencia Española de Protección de Datos. (28 de octubre de 2021). Anonimización y seudonimización (II): la privacidad diferencial. AEDP. <https://www.aepd.es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion-ii-la-privacidad-diferencial>

Aguilar Gil, Yásnaya Elena. (9 de diciembre de 2020). Una propuesta modesta para salvar al mundo. *Rest of World*. <https://restofworld.org/2020/tecnologia-tequio-cambio-climatico/>

Aguilar Gil, Yásnaya Elena. (1 de noviembre). La lengua como territorio cognitivo y su relación con concepciones tecnológicas. [Ponencia magistral]. *Primer Encuentro Regional del LAC Hub de la red FAIR*.
<https://feministai.pubpub.org/pub/5gmo1xhx/release/2>

Allen, Anita. (1988). *Uneasy Access*. Rowman & Littlefield Publishers.

Allen, Anita. (1999). Coercing Privacy. *William & Mary Law Review*, 40 (3), pp. 723-757.
<https://scholarship.law.wm.edu/wmlr/vol40/iss3/3>

Anderson, Patrick. (2022). Of Cypherpunks and Sousveillance. *Surveillance & Society*, 20(1) pp. 1-17.

<https://doi.org/10.24908/ss.v20i1.14322>

Andrejevic, Mark. (2004). *Reality TV: The Work of Being Watched*. Rowman and Littlefield.

Andrejevic, Mark. (2013). *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. Routledge.

Apple. (s.f.). Differential Privacy. Apple.

https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

Architizer. (s.f.). CHBL Jammer Coat. *Architizer*. <https://architizer.com/projects/chbl-jammer-coat/>

Arrieta-Ibarra, Imanol; Goff, Leonard; Jiménez-Hernández, Diego; Lanier, Jaron y Weyl, E. Glen. (2018). Should We Treat Data as Labor? Moving beyond “Free”. *AEA Papers and Proceedings*, 108, pp. 38-42. <https://doi.org/10.1257/pandp.20181003>

Asamblea General de las Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. Naciones Unidas. <https://www.un.org/es/about-us/universal-declaration-of-human-rights>

Ashley, Paul. (2017). Identity Obfuscation Through Fully Functional Avatars. En Finn Brunton y Helen Nissenbaum (eds.), *Obfuscation Workshop Report*. obfuscationworkshop.io, pp. 22-24.

Augé, Marc. (1993). *Los no-lugares: espacios del anonimato. Una antropología de la sobremodernidad*. (Trad. Margarita Mizraji). Gedisa. (Trabajo original publicado en 1992).

Augé, Marc. (2007). Sobremodernidad. Del mundo de hoy al mundo de mañana. *Contrastes: Revista Cultural*, (47), pp. 101-107.

Austin, Lisa M. (2015). Lawful illegality: what Snowden has taught us about the legal infrastructure of the surveillance state. En Michael Geist (ed.). *Law, Privacy and Surveillance in Canada in a Post-Snowden Era*. University of Ottawa Press, pp. 103-126. <https://doi.org/10.2307/j.ctt15nmj3c.8>

Balsar, Satchit; Buckee, Caroline; Khanna, Tarun. (8 de mayo de 2020). Which Covid-19 Data Can You Trust? *Harvard Business Review*. <https://hbr.org/2020/05/which-covid-19-data-can-you-trust>

Ball, Kirstie (2009). Exposure: exploring the subject of surveillance, *Information, Communication and Society*, 12 (5), pp. 639–657. <https://doi.org/10.1080/13691180802270386>

Barandiaran, Xabier. (28 de abril de 2017). Identidad, censo, privacidad, poder. *Xabier Barandiaran*. <https://xabier.barandiaran.net/2017/04/28/identidad-censo-privacidad-poder/>

- Barandiaran, Xabier. (14 de enero de 2019). Comparativa Decidim vs. Cónsul. *Xabier Barandiaran*. <https://xabier.barandiaran.net/2019/01/14/comparativa-decidim-vs-consul/>
- Barandiaran, Xabier. (2019). Tecnopolítica, municipalismo y radicalización democrática. En Roth, Laura; Monterde, Arnau y Calleja-López, Antonio, *Ciudades democráticas*, Icaria, pp. 173–207.
- Barandiaran, Xabier; Calleja-López, Antonio; Monterde, Arnau y Romero, Carol. (2024) *Decidim, a Technopolitical Network for Participatory Democracy*. Springer. https://doi.org/10.1007/978-3-031-50784-7_1
- Barranquero, Alejandro. (2007). Concepto, instrumentos y desafíos de la edu-comunicación para el cambio social. *Comunicar*, 29, pp. 115-120. <https://doi.org/10.3916/C29-2007-16>
- Bass, Theo; Sutherland, Emma y Symons, Tom. (2018). *Reclaiming the Smart City Personal data, trust and the new commons*. DECODE. https://media.nesta.org.uk/documents/DECODE-2018_report-smart-cities.pdf
- Basset, Marc. (8 de marzo de 2024). Francia es pionera en la protección constitucional del derecho al aborto... ¿O no lo es? *El País*. <https://elpais.com/sociedad/2024-03-08/francia-es-pionera-en-la-proteccion-constitucional-del-derecho-al-aborto-o-no-lo-es.html>
- Baudrillard, Jean. (1991). *La transparencia del mal*. (Trad. Joaquim Jordà). Anagrama. (Trabajo original publicado en 1990).
- Bauman, Zygmunt & Lyon, David. (2013). *Vigilancia Líquida*. (Trad. de Alicia Capel) Paidós. (Trabajo original publicado en 2013).
- Baumeister, Roy F. y Leary, Mark R. (1997). Writing Narrative Literature Reviews. *Review of General Psychology*, 1(3), pp. 311-320. <https://doi.org/10.1037/1089-2680.1.3.311>
- Bax, Maxime; Giebels, Francien y Sepovan, Sasun. (Agosto, 2021). Tracked more than you know. How smartphone SDKs form a major privacy breach. *Information Law and Policy Lab*. <https://ilplab.nl/wp-content/uploads/sites/2/2021/09/ILP-Lab-report-on-tracking-SDKs-1.pdf>
- Bazon, Emili. (1 de abril de 2015). Purvi Patel Could Be Just the Beginning. *The New York Times Magazine*. <https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html>
- Baaz, Mikael; Lilja, Mona; Schulz, Michael y Vinthagen, Stellan (2016). Defining and Analyzing ‘Resistance’. *Possible Entrances to the Study of Subversive Practices. Alternatives*, 41(3), pp. 137–153.

<https://doi.org/10.1177/0304375417700170>

Beauregard, Luis P. (25 de abril de 2024). El Congreso de Arizona abre una vía para derogar la ley del aborto de 1864. *El País*. <https://elpais.com/america/2024-04-25/el-congreso-de-arizona-abre-una-via-para-derogar-la-ley-del-aborto-de-1864.html>

Beetham, David. (1974). *Max Weber and the Theory of Modern Politics*. Polity Press.

Beetham, David. (1987). *Bureaucracy*. Open University Press.

Bell, Daniel. (1973). *The Coming of the Post-Industrial Society: A Ventura in Social Forecasting*. Basic Books.

Benkler, Yochai (2014). Between Spanish Huertas and the Open Road: A Tale of Two Commons? En Brett M. Frischmann *et al.* (eds.). *Governing the knowledge commons*, Oxford University Press, pp. 69-98. <https://doi.org/10.1093/acprof:oso/9780199972036.003.0003>

Benkler, Yochai. (2015). *La riqueza de las redes*. (Trad. Maryam Itatí Portillo *et al.*). Icaria. (Trabajo original publicado en 2006).

Benn, Stanley. (1971). Privacy, Freedom, and Respect for Persons. En J. Roland Pennock y John W. Chapman (eds.), *Nomos XIII: Privacy* (pp. 1-26). Atherton Press.

Bigo, Didier. (2006). Globalized (in)security: the field and the banopticon, en Naoki Sakai y Jon Solomon (eds.), *Traces: A Multilingual Series of Cultural Theory and Transition*. University Press, pp. 109-156.

Black, Edwin (2001). *IBM y el holocausto. La alianza estratégica entre la Alemania nazi y la más poderosa corporación norteamericana*. Atlántida.

Blake, Emili. (10 de diciembre de 2021). The Strength Of K-Pop Fandom, By The Numbers. *Forbes*. <https://www.forbes.com/sites/emilyblake1/2018/04/04/k-pop-numbers>

Blas, Zach. (s.f.). Facial Waponization Suite. *Zach Blas*. <https://zachblas.info/works/facial-weaponization-suite/>

Bonini, Tiziano y Treré, Emiliano. (2024). *Algorithms of Resistance*. The MIT Press.

Bowell, Tracy. (s.f.) Feminist Standpoint Theory. *Internet Encyclopedia of Philosophy*. <https://iep.utm.edu/fem-stan/>

Boling, Patricia. (1996). *Privacy and the Politics of Intimate Life*. Cornell University Press.

Bordiec, Sylvain. (agosto de 2024). Soledades de ricos, soledades de pobres. *Le Monde Diplomatique en español*. <https://mondiplo.com/soledades-de-ricos-soledades-de-pobres>

- Bloustein, Edward J. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*, 38, pp. 962-1007. <https://doi.org/10.4324/9781351319966-1>
- Brascia, Clara A. (26 de enero de 2024). La red se llena de porno ‘deepfake’ de Taylor Swift y muestra el peligro de la IA para las mujeres. *El País*. <https://elpais.com/tecnologia/2024-01-26/la-red-se-llena-de-porno-deepfake-de-taylor-swift-y-muestra-el-peligro-de-la-ia-para-las-mujeres.html>
- Bria, Francesca. (5 de abril de 2018). Our Data is valuable. Here’s how we can take that value back. *The Guardian*. www.theguardian.com/commentisfree/2018/apr/05/data-valuable-citizens-silicon-valley-barcelona
- Bria, Francesca y Morozov, Evgeny. (2018). *Rethinking the Smart City*. Codice Edizioni
- Broca, Sébastien. (Marzo de 2020). La tecnología digital empieza con el carbón. *Le Monde Diplomatique en español*. <https://mondiplo.com/la-tecnologia-digital-funciona-con-carbon>
- Brown, Geoffrey. (1990). *Information Game: Ethical Issues in a Microchip World*. Humanities Press.
- Brunton, Finn y Nissenbaum, Helen. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, 16(5). <https://doi.org/10.5210/fm.v16i5.3493>
- Brunton, Finn y Nissenbaum, Helen. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. The MIT Press.
- Brunton, Finn y Nissenbaum, Helen. (2017). Obfuscation Going Forward: A Research Agenda. En Finn Brunton y Helen Nissenbaum (eds.), *Obfuscation Workshop Report*. obfuscationworkshop.io, pp. 4-6.
- Burrows, Roger and Gane, Nicholas. (2006) Geo-demographics, software and class. *Sociology*, 40 (5), pp. 793-812. <https://doi.org/10.1177/003803850606067>
- Byrne, Ciara. (18 de marzo de 2019). Trading Privacy for Survival Is Another Tax on the Poor. *Fast Company*. <https://www.fastcompany.com/90317495/another-tax-on-the-poor-surrendering-privacy-for-survival>
- Cabello Fernández-Delgado, Florencio (2019). Introducción. En Chris Kelty, *Two Bits. La trascendencia cultural del software libre*. (Trad. Ana M. Alconchel et al.) Icaria, pp. 9-52.
- Cabello Fernández-Delgado, Florencio. (2024). Dan McQuillan, Resisting AI: An Anti-Fascist Approach to Artificial Intelligence. [Reseña del libro *Resisting AI: An Anti-Fascist Approach to Artificial Intelligence* de Dan McQuillan]. *International Journal of Communication*, 18, pp. 967–970.
- Cabello, Florencio, Franco, Marta. G. & Haché, Alex (2013). The social web beyond “walled

gardens”: interoperability, federation and the case of Lorea/N-1. *PsychNology Journal*, 11(1), pp. 43 – 65.

Cabello Fernández-Delgado, Florencio y Solera Navarro, Fátima. (2020). Ofuscación algorítmica. En Jesús Sabariego, Augusto Jobim y Eduardo Baldissera (eds.). *Algoritarismos*. Tirant Lo Blanch. pp. 332-346.

Cabello Fernández-Delgado, Florencio y Rascón Gómez, María Teresa (2020). (En)Cerrar el círculo de la marginación: control actuarial y cárcel en Asperones. *DEDiCA. REVISTA DE EDUCAÇÃO E HUMANIDADES*, 17, pp. 273-293. <http://dx.doi.org/10.30827/dreh.v0i17.12218>

Cabezudo Vidal, Nicolás. (2023). Las sentencias Schrems I (2015) y Schrems II (2020) del Tribunal de Justicia de la Unión Europea y la protección de datos de carácter personal en las relaciones internacionales. *CEFLegal. Revista Práctica de Derecho*, 265, pp. 91-126. <https://doi.org/10.51302/ceflegal.2023.15785>

Cadenas, Julia. (28 de junio 2022). Por qué recomiendan borrar las apps que registran los ciclos menstruales tras la sentencia del Supremo sobre el aborto en Estados Unidos. *Newtral*. <https://www.newtral.es/apps-menstruacion-aborto/20220628/>

Calderón Almendros, Ignacio, Mojtar MENDIENTA, Luz y Cabello Fernández-Delgado, Florencio. (2021). *Cómo hacer inclusiva tu escuela*. Ministerio de Educación y Formación Profesional. <https://bit.ly/3LeGcWg>

Calderón Almendros, Ignacio y Rascón Gómez, María Teresa (Coords.) (2020). *Análisis y propuestas para una nueva Ley Educativa. Conversaciones de la ciudadanía sobre la escuela inclusiva*. Octaedro.

Calderón Almendros, Ignacio y Rascón Gómez, María Teresa. (2022). Hilando luchas por el derecho a la educación: Narrativas colectivas y personales para la inclusión desde el modelo social de la discapacidad. *Pedagogía Social. Revista Interuniversitaria*, (41), pp. 43-54. https://doi.org/10.7179/PSRI_2022.41.03

Calleja-López, Antonio. (2018). *Technopolitical democratization and data commoning: the case of the Digital Democracy and Data Commons (DDDC) pilot*. [Working Paper]. Decodeproject.eu

Calleja-López, Antonio; Arroyo, Liliana y Balestrini, Mara. [Barcelona.cat] (7 de enero de 2020). #DecidimFest 2019: Más allá del capitalismo de datos. [Video]. Youtube. <https://www.youtube.com/watch?v=BsgTXvHX0NI>

Caponi, Sandra. (2013). Quételet, el hombre medio y el saber médico. *História, Ciências Saúde* –

Manguinhos, 20, pp. 831-847.

Carey, James. (1989). *Communication as Culture: Essays on Media and Society*. Unwin-Hyman.

Castells, Manuel. (1997). *La era de la información. Economía, sociedad y cultura. Vol.1: La sociedad red* (trad. Carmen Martínez Gimeno), Alianza. (Trabajo original publicado en 1996).

Castells, Manuel. (2001). *The Internet Galaxy*. Oxford University Press.

Castells, Manuel. (2009). *Communication Power*. Oxford University Press.

Castillo, Carlos del (28 de mayo de 2024). Si la inteligencia artificial bebe tanta agua, ¿cómo brotan sus centros de datos en la España seca? *ElDiario.es*. https://www.eldiario.es/tecnologia/si-inteligencia-artificial-bebe-agua-brotan-centros-datos-espana-seca_1_11399434.html

Certeau, Michel de. (1990). *L'Invention du Quotidien, vol. 1. Arts de faire*. Gallimard.

Certeau, Michel de. (1993). *La culture au pluriel*. Éditions du Seuil. (Trabajo original publicado en 1974).

Certeau, Michel de. (2001). De las prácticas cotidianas de oposición. En Paloma Blanco, Jesús Carrillo, Jordi Claramonte y Marcelo Expósito (eds.), *Modos de Hacer: Arte crítico, esfera pública y acción directa*, (Trad. Jordi Claramonte) Ediciones Universidad de Salamanca, pp. 383-425.

Cheney-Lippold, John. (2017). *We Are Data: Algorithms and the Making of Our Digital Selves*. New York University Press.

Church, Frank. (17 de agosto de 1975). The Intelligence Gathering Debate. #NBC Meet the Press [Video]. Youtube. <https://www.youtube.com/watch?v=YAG1N4a84Dk#t=1m25s>

Clarís Viladrosa, Robert. (26 de octubre de 2015). Ofuscación de código: te reto a que entiendas este programa. *Tecnología++: El blog de los Estudios de Informática, Multimedia y Telecomunicación de la UOC*. <https://blogs.uoc.edu/informatica/es/ofuscacion-de-codigo-te-reto-a-que-entiendas-este-programa/>

Clarke, Roger. (1988). Information technology and dataveillance. *Communications of the ACM*, 31, (5), pp. 498 - 512. <https://doi.org/10.1145/42411.42413>

Clarke, Roger. (1994a). Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People*, 7 (4), pp. 6-37
<http://www.rogerclarke.com/DV/HumanID.html>

Clarke, Roger. (1994b). The digital persona and its application to data surveillance. *The Information*

Society, 10(2), pp. 77–92. <https://doi.org/10.1080/01972243.1994.9960160> (Recuperado de: <http://www.rogerclarke.com/DV/DigPersona.html>).

Clarke, Roger. (1998). Smart Card Technical Issues Starter Kit. *Roger Clarke's Dataveillance and Information Privacy Home-Page*. <http://www.rogerclarke.com/DV/SCTISK3.html>

Cohen, Julie E. (2012). *Configuring the Networked Self: Law, Code and Play in Everyday Practice*. Yale University Press

Cohen, Julie E. (2013). What Privacy Is For. *Harvard Law Review*, 126 (7), pp. 1904-1933. <https://www.jstor.org/stable/23415061>

Cohen, Julie E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Cohen, Stanley. (1991). *Visions of Social Control*. Polity.

Comisión Europea. (s.f.). Ley de Mercados Digitales: garantizar unos mercados digitales justos y abiertos. Comisión Europea. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_es

Comisión Europea. (s.f.). ¿Qué son los datos personales?. *Comisión Europea*. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

Comisión Europea. (6 de septiembre de 2023). Ley de Mercados Digitales: La Comisión designa seis guardianes de acceso. Comisión Europea. https://ec.europa.eu/commission/presscorner/detail/es/ip_23_4328

Consejo de Europa, Tribunal Europeo de Derechos Humanos. (1950). *Convenio Europeo de Derechos Humanos*. Oficina de Publicaciones de la Unión Europea.

Consejo de Europa, Tribunal Europeo de Derechos Humanos, Supervisor Europeo de Protección de Datos y Agencia de los Derechos Fundamentales de la Unión Europea. (2019). *Manual de legislación europea en materia de la protección de datos: edición de 2018*. Oficina de Publicaciones de la Unión Europea. <http://www.doi.org/10.2811/824752>

Constitución de los Estados Unidos [Const]. IV Enmienda. 1791 (Estados Unidos).

Cordero, Clara I. (2019). La transferencia internacional de datos con terceros estados en el nuevo reglamento europeo: especial referencia al caso estadounidense y la Cloud Act. *Revista Española de Derecho Europeo* (70), 49–108.

- Coufreur-Blaauwendraad, Marcel. (29 de marzo de 2017). *A HKU Design - Anonymous (english) - PLEASE READ DESCRIPTION + STATEMENT BELOW* [Archivo de Vídeo]. Youtube. <https://www.youtube.com/watch?v=D1Thmz61sho> (Recuperado el 2 de febrero de 2025).
- Courpasson, David y Vallas, Steven. (2016). *Resistance Studies: A Critical Introduction*. Sage.
- Covarrubias, Sebastián de. (1943). *Tesoro de la lengua castellana o española*, edición de Martín de Riquer. Alta Fulla. (Trabajo original publicado en 1611).
- Craven, J. Braxton Jr. (1976). Personhood: The Right to Be Let Alone. *Duke Law Journal*, 15, pp. 699-720. <https://doi.org/10.2307/1371935>
- Crenshaw, Kimberle. (1991) Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*, 43 (6), pp. 1241–1299. <https://doi.org/10.2307/1229039>
- Cruz, Octavio (2007). El trabajo de campo como descubrimiento y creación. En María Cecilia de Souza (ed.), *Investigación social. Teoría, método y creatividad*. Lugar Editorial, pp. 41-52.
- Cucchietti, Fernando; Moll, Joana; Esteban, Marta; Reyes, Patricio y García Calatrava, Carlos. (2022). *_carbolytics, an analysis of the carbon costs of online tracking. Carbolytics Report*. <https://carbolytics.org/report.html>
- Dandeker, Christopher. (1990). *Surveillance, Power and Modernity*. St. Martin's Press.
- Das, Ranju. (21 de noviembre de 2017). Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection. *AWS Machine Learning Blog*. <https://aws.amazon.com/es/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection/>
- Dawson, Michael. (2004). *The Consumer Trap*. University of Illinois Press.
- Dean, Jodi (2002). *Publicity's secret: How Technoculture Capitalizes on Democracy*. Cornell University Press
- DeCew, Judith Wagner. (1997). *In Pursuit of Privacy*. Cornell University Press.
- Decidim. (s.f.). Contrato social de Decidim. *Decidim Docs*. <https://docs.decidim.org/en/develop/understand/social-contract-es.html>
- DECODE (2019). D5.9 Final report on the Barcelona Pilots, evaluations of Barcelona Now and sustainability plans. *DECODE*. <https://decodeproject.eu/publications/final-report-barcelona-pilots-evaluations-barcelonanow-and-sustainability-plans.html>

Deleuze, Gilles. (1995). *Conversaciones 1972-1990*. (Trad. José Luis Pardo). Pretextos. (Trabajo original publicada en 1990).

Deleuze, Gilles y Guattari, Félix. (1983). *Anti-Oedipus: Capitalism and Schizophrenia*. (Trad. Robert Hurley, Mark Seem y Helen R. Lane). University of Minnesota Press. (Trabajo original publicado en 1972).

Denzin, Norman. (1995). *The Cinematic Society: The Voyeur's Gaze*. Sage.

Dewey, John. (1978). En Jo Ann Boydston (ed.), *The Middle Works of John Dewey*. Southern Illinois University Press. (Trabajo original publicado en 1908)

Dewey, John. (1995). Liberalism and Civil Liberties. En Jo Ann Boydston (ed.), *The Later Works of John Dewey*. Southern Illinois University Press. (Trabajo original publicado en 1936).

Diffie, Whitfield y Hellman, Martin E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), pp. 644-654. <https://doi.org/10.1109/TIT.1976.1055638>

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Diario Oficial de la Unión Europea, 31 de julio de 2002, pp. 37-47. <http://data.europa.eu/eli/dir/2002/58/oj>

Dwork, Cynthia. (2008). Differential Privacy: A Survey of Results. En: Manindra Agrawal, Dingzhu Du, Zhenhua Duan, Angsheng Li (eds.) *Theory and Applications of Models of Computation. TAMC 2008. Lecture Notes in Computer Science*, 4978. Springer. pp. 1-19. https://doi.org/10.1007/978-3-540-79228-4_1

Edwards, Paul N. (1989). The Closed World: Systems Discourse, Military Policy, and Post-World War II. US Historical Consciousness. En Lev Levidow y Kevin Robins (eds.). *The Military Information Society*. Free Association Books, pp. 135-158.

Edwards, Paul N. (1996). *Closed Worlds: Computers and the Politics of Discourse in the Cold War America*. MIT Press.

Eisenhowers, Dwight D. (17 de enero de 1961). President Dwight D. Eisenhower's Farewell Address (1961) [Transcripción de audio de un discurso]. *Milestone Documents*. <https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address>

Electronic Frontier Foundation. (s.f.). NSA Spying. How It Works. *Electronic Frontier Foundation*. <https://www EFF.org/nsa-spying/how-it-works>

Ellul, Jacques. (1967). *The Technological Society*. (Trad. John Wilkinson). Vintage Books. (Trabajo original publicado en 1954).

Eschler, Jordan; Menking, Amanda; Fox, Sarah y Backonja, Uba. (2019). Defining Menstrual Literacy With the Aim of Evaluating Mobile Menstrual Tracking Applications. *CIN* 37 (12), 638-646. <https://doi.org/10.1097/cin.0000000000000559>

España Naveira, Enrique. (2021). *(El derecho a) Inventar la Ciudad*. [Tesis doctoral]. Universidad de Sevilla. <https://hdl.handle.net/11441/116616>

Eticas Foundation. (2016). Plan de Privacidad de Decidim Barcelona. *Eticas Foundation*. Recuperado de: https://web.archive.org/web/20220405135202/https://eticasfoundation.org/wp-content/uploads/2020/04/Plan-de-Privacidad-de-Decidim-Barcelona_FINAL.pdf

Eticas Foundation. (2019). Mi cuerpo mis datos sus normas. *Eticas Foundation*. https://eticasfoundation.org/wp-content/uploads/2022/06/ETICAS_Mi-cuerpo-mis-datos-sus-normas-202206.pdf

Etzioni, Amitai. (1999). *Limits of Privacy*. Basic Books.

EU Artificial Intelligence Act. (27 de febrero de 2024a [actualizado 30 de mayo de 2024]). Resumen de alto nivel de la Ley AI. *EU Artificial Intelligence Act*. <https://artificialintelligenceact.eu/es/high-level-summary/>

EU Artificial Intelligence Act. (2024b). Artículo 59: Tratamiento posterior de datos personales para el desarrollo de determinados sistemas de IA de interés público en el espacio aislado de regulación de la IA. *EU Artificial Intelligence Act*. <https://artificialintelligenceact.eu/es/article/59/>

Ewald, François. (1986). *L'État providence*. Grasset.

Fals Borda, Orlando y Rodrigues Brandão, Carlos. (1987). *Investigación Participativa*. La Banda Oriental.

Fals Borda, Orlando y Anisur Rahman, Mohammad. (1991). *Acción y conocimiento: Como romper el monopolio con investigación acción participativa*. Cinep.

Federal Trade Commission. (22 de junio de 2021). FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others. *Federal Trade Commission*. <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

Federici, Silvia. (2010). *Calibán y la bruja. Mujeres, cuerpo y acumulación originaria*. (Trad. Verónica Hendel y Leopoldo Sebastián Touza). Traficantes de Sueños. (Trabajo original publicado en 2004).

Federici, Silvia. (2020). Reencantar el mundo: El feminismo y la política de los comunes. (Trad. María Aranzazu Catalán Altuna, excepto el capítulo 9 traducido por Carlos Fernández Guervós y Paula Martín Ponz Traficantes de Sueños. (Trabajo original publicado en 2019).

Federici, Silvia. (2022). *Ir más allá de la piel*. (Trad. Aránzazu Catalán Altuna). Traficantes de Sueños. (Trabajo original publicado en 2020).

Feeley, Malcolm y Simon, Jonathan. (1994). Actuarial justice: The emerging new criminal law, en David Nelken (ed.), *The Futures of Criminology*. Sage.

Felton, James. (7 de octubre de 2019). That “Wearable Face Projector” Hong Kong Protesters Are Supposedly Using Is Not Real. *IFLScience*. <https://www.iflscience.com/that-wearable-face-projector-hong-kong-protesters-are-supposedly-using-is-not-real-53877>

Finn, R. Welldon. (1963). *An Introduction to the Domesday Book*. Longmans.

Fisher, Jill; Monahan, Torin. (2011). The 'biosecuritization' of health-care delivery: Examples of post-9/11 technological imperatives. *Social Science Medicine*, 72 (4), pp. 545-52. <https://doi.org/10.1016/j.socscimed.2010.11.017>

Ford, Andrea, Togni; Giulia, y Miller, Livia. (2021). Hormonal Health: Period Tracking Apps, Wellness, and Self-Management in the Era of Surveillance Capitalism. *Engaging Science, Technology, and Society*, (7), 48-66. <https://doi.org/10.17351/ests2021.655>

Forouzan, Kimya; Friedrich-Karnik, Amy y Maddow-Zimet, Isaac. (Diciembre de 2023). The High Toll of US Abortion Bans: Nearly One in Five Patients Now Traveling Out of State for Abortion Care. *Guttmacher*. <https://www.guttmacher.org/2023/12/high-toll-us-abortion-bans-nearly-one-five-patients-now-traveling-out-state-abortion-care>

Foucault, Michel (1998). *Historia de la sexualidad I. La voluntad de saber*. (Trad. Ulises Guinazú). Siglo XXI Editores. (Trabajo original publicado en 1978).

Foucault, Michel. (2002). *Vigilar y castigar: nacimiento de la prisión*. (Trad. Aurelio Garzón del Camino) Siglo veintiuno editores Argentina. (Trabajo original publicado en 1975).

Foucault, Michel. (2005). *El poder psiquiátrico, Curso en el Collège de France (1973-1974)*. (Trad. Horacio Pons). Fondo de Cultura Económica. (Trabajo original publicado en 2003).

- Foucault, Michel. (2006). *Seguridad, Territorio, Población. Curso en el Collège de France (1977-1978)*. (Trad. Horacio Pons). Fondo de Cultura Económica. (Trabajo original publicado en 2004).
- Foucault, Michel. (2009). *Nacimiento de la Biopolítica. Curso del Collège de France (1977-1978)*. (Trad. Horacio Pons). Ediciones Akal. (Trabajo original publicado en 2004).
- Foster, John Bellamy; McChesney, Robert. (2014). Surveillance capitalism: Monopoly the military-industrial complex and finance capital, the digital age. *Monthly Review*, 66 (3). Recuperado de: <https://monthlyreview.org/2014/07/01/surveillance-capitalism/>
- Fraser, Nancy. (2014). Behind Marx's Hidden Abode: For an Expanded Conception of Capitalism. *New Left Review*, 86, pp. 55–72.
- Freire, Paulo. (1982). Creating alternative research methods: learning to do it by doing it. En Budd Hall, Arthur Gillette y Rajesh Tandon (Eds.), *Creating knowledge: A Monopoly? Participatory research in development*. International Council for Adult Education, pp. 29-37.
- Freire, Paulo. (1985). *The politics of education: Culture, power, and liberation*. Bergin & Garvey Publishers.
- Freund, Paul. (1975). Discurso en el 52nd Annual Meeting. *American Law Institute* pp. 42-43.
- Friedman, Lawrence. M. (2007). *Guarding Life's Dark Secrets: Legal and Social Control over Reputation, Propriety, and Privacy*. Stanford University Press.
- Fuchs, Christian. (2017). *Digital Labour and Karl Marx*. Routledge.
- Galbraith, Vivian H. (1974). *Domesday Book: Its Place in Administrative History*. Oxford University Press.
- Gandy, Oscar. (2006) Quixotics unite! Engaging the pragmatists on rational discrimination, en David Lyon (ed). *Theorizing Surveillance: The Panopticon and Beyond*. Willan, pp. 318-336.
- García Barrios, Raúl y Jiménez Martínez, Nancy Merary. (13 de julio de 2020). ¿Antropoceno o Capitaloceno?. *Nexos*. <https://medioambiente.nexos.com.mx/antropoceno-o-capitaloceno/>
- Gavison, Ruth. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89 (3), pp. 421-471. <https://ssrn.com/abstract=2060957>
- Gavison, Ruth. (1992). Feminism and the Private-Public Distinction. *Stanford Law Review*, 45, pp. 1-46. <https://doi.org/10.2307/1228984>
- Gerety, Tom. (1977). Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review*, 12 (2), pp. 233-296.

- Gerstein, Robert. (1978). Intimacy and Privacy. *Ethics*, 89(1), pp. 76–81.
<http://www.jstor.org/stable/2380133>
- Gearan, Anne. (6 de junio de 2013). ‘No Such Agency’ spies on the communications of the world. *The Washington Post*. https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497_story.html
- Giddens, Anthony. (1985). *The Nation-State and Violence*. Polity Press.
- Giddens, Anthony. (1987). *Social Theory and Modern Sociology*. Polity Press.
- Giddens, Anthony. (1990). *The Consequences of Modernity*. Polity Press.
- Girardin, Émile de. (1852). *La Politique universelle. Décrets de l'avenir*. Muquardt.
- Gitelman, Lisa y Jackson, Virginia (2013). Introduction. En Lisa Gitelman (ed.), *“Raw Data” Is an Oxymoron*. MIT Press (pp. 1-14).
- Glaze. (s.f.) What Is Glaze? Samples, Why Does It Work, and Limitations. *Glaze*.
<https://glaze.cs.uchicago.edu/what-is-glaze.html>
- Godkin, Edwin L. (1890). The Right of the Citizen, IV. To His Own Reputation. *Scribner's Magazine*, 8 (1). pp. 58-67.
- Goffman, Erving. (1959). *The Presentation of the Self in Everyday Life*. Anchor Book.
- Gómez Alcalde, Marina (2023). *MIS DATOS, MIS REGLAS*. [Trabajo Fin de Grado]. Universidad de Málaga. <https://hdl.handle.net/10630/31275>
- Graeber, David. (2015). *La utopía de las Normas*. (Trad. Joan Andreano Weylan). Ariel. (Trabajo original publicado en 2015).
- Graeber, David. (2018). *Trabajos de mierda*. (Trad. Iván Barbeitos García). Ariel. (Trabajo original publicado en 2018).
- Graeber, David y Wengrow, David. (2022). *El amanecer de todo*. (Trad. Joan Andreano Weyland) Ariel. (Trabajo original publicado en 2021).
- Graham, Stephen y Wood, David. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy*, 23, pp. 227-248. <https://doi.org/10.1177/02610183030230020>
- Gramsci, Antonio. (1929). Américanisme et fordisme. *Cahiers internationaux*, 89, septembre-octobre

de 1957.

Griffiths, Hugh D. (julio 2020). The History Column: Chaff. *IEEE Aerospace and Electronic Systems Society*. <https://ieeaeess.org/post/blog/history-column-chaff>

Grundy, Quinn; Chiu, Kellia; Held, Fabian; Continella, Andrea; Bero Lisa y Holz, Ralph. (2019). Sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ*, pp. 1-11. <https://doi.org/10.1136/bmj.1920>

Guliani, Neema Singh. (24 de octubre de 2018). Amazon Met With ICE Officials to Market Its Facial Recognition Product. *ACLU*. <https://www.aclu.org/news/privacy-technology/amazon-met-ice-officials-market-its-facial>

Gutiérrez Ruiz, Pablo. (s.f.) Cifrado Homomórfico: una introducción a la computación segura de los datos. *Instituto de Ingeniería y Conocimiento*. <https://www.iic.uam.es/noticias/cifrado-homomorfico-introduccion-a-la-computacion-segura-datos/>

Haggerty, Kevin D., & Ericson, Richard V. (2000). The surveillant assemblage. *The British Journal of Sociology*, 51 (4), pp. 605-622. <https://doi.org/10.1080/00071310020015280>

Hallnäs, Lars y Redström, Johan. (2002). From use to presence: on the expressions and aesthetics of everyday computational things. *ACM Trans. Comput.-Hum. Interact*, 9 (2), pp. 106-124. <https://doi.org/10.1145/513665.513668>

Halpin, Harry; Nielsen, Aileen; Bateyko, Dan y Liu, Yisi. (7 de mayo de 2021). Obfuscation is dead? Long Live Obfuscation! En Amelia Andersdotter (Moderadora), Mesa Redonda. *3rd Workshop on Obfuscation*. Online. [Ver Anexo 3]

Haraway, Donna J. (1995). *Ciencia, cyborgs y mujeres. La reinención de la naturaleza*. (Trad. Manuel Talens). Ediciones Cátedra. Universidad de València. Instituto de la Mujer. (Trabajo original publicado en 1991).

Haraway, Donna J. (2019). *Seguir con el Problema. Generar parentesco en el Chthuluceno*. (Trad. Helen Torres). Consonni. (Trabajo original publicado en 2016).

Harcourt, Bernard. (2015). *Exposed: Desire and Disobedience in the Digital Age*. Harvard University Press.

Harding, Sandra. (1998). *Is science multicultural?: postcolonialisms, feminisms, and epistemologies*. Indiana University Press.

Hartsock, Nancy (1975). Fundamental Feminism: Process and Perspective. *Quest*, II (2), pp. 67-80.

Hartsock, Nancy (1983a). The Feminist Standpoint: Developing the Ground for a Specifically Feminist Historical Materialism. En Sandra Harding y Merrill Hintikka (Eds.), *Discovering Reality: Feminist Perspectives on Epistemology, Metaphysics, Methodology, and Philosophy of Science*. Reidel/Kluwer, pp. 283-310

Hartsock, Nancy (1983b). *Money, Sex and Power. Toward a Feminist Historical Materialism*. Northeastern University Press.

Hartsock, Nancy (2019). *The Feminist Standpoint Theory Revisited and Other Essays*. Routledge.

Heikkilä, Melissa. (23 de octubre de 2023). This new data poisoning tool lets artists fight back against generative AI. *MIT Technology Review*.

<https://www.technologyreview.com/2023/10/23/1082189/data-poisoning-artists-fight-generative-ai/>

Heilmann, Eric y Vitalis, André. (1996). *Nouvelles technologies, Nouvelles régulations?*. CNRS.

Herman, Tamar. (2 de enero de 2018). K-Pop Fans Spend Big On Times Square Ads Promoting Their Favorite Stars. *Forbes*. <https://www.forbes.com/sites/tamarherman/2017/12/21/k-pop-fans-spend-big-on-times-square-ads-promoting-their-favorite-stars/>

Herrmann, Clara. (4 de mayo de 2017). The Future of Living with Surveillance, with Adam Harvey. *Digital Culture, Theory & Art*. <https://schloss-post.com/the-future-of-living-with-surveillance/>

Hill, Kashmir. (4 de julio de 2022). Borrar el registro de tu menstruación no te protege. *The New York Times*. <https://www.nytimes.com/es/2022/07/04/espanol/app-ciclo-menstrual.html>

Hill, Kashmir. (13 de febrero de 2023). This Tool Could Protect Artists From A.I. Image Generators. *The New York Times*. <https://www.nytimes.com/2023/02/13/technology/ai-art-generator-lensa-stable-diffusion.html>

Hixson, Richard F. (1987). *Privacy in a Public Society: Human Rights in Conflict*. Oxford University Press.

Hochschild, Arlie. (2013). *Outsourced Self: What Happens When We Pay Others to Live Our Lives for Us*. Picador Paper.

Hondius, Frits W. (1975). *Emerging Data Protection in Europe*. North-Holland Publishing Company.

Howe, Daniel. (2015). Surveillance Countermeasures: Expressive Privacy via Obfuscation. *APRJA*, 4 (1), pp. 88-100. <https://doi.org/10.7146/aprja.v4i1.116108>

Howe, Daniel, y Nissenbaum, Helen. (2009). TrackMeNot: Resisting Surveillance in Web Search.. En Ian Kerr, Carole Luckock, y Valerie Steeves Lessons (eds.), *From the Identity Trail: Anonymity, Privacy*

and Identity in a Networked Society. Oxford University Press. <https://ssrn.com/abstract=2567412>

Howe, Daniel y Nissenbaum, Helen. (2017). Engineering privacy and protest; A case study of AdNauseam. *CEUR Workshop Proceedings*, 1873, pp. 57-64.

Huizinga, Johan. (2012). *Homo ludens*. (Trad. Eugenio Imaz Echeverría). Alianza Editorial. (Trabajo original publicado en 1938).

Inness, Julie C. (1992). *Privacy, Intimacy, and Isolation*. Oxford University Press.

Innis, Harold. (1950). *Empire and communications*. Dundurn Press.

Innis, Harold. (1951). *The Bias of Communication*. University of Toronto Press.

Jameson, Fredric. (2013). Historia y Conciencia de Clase como un proyecto inacabado. En *Valencias de la dialéctica*. (Trad. Mariano López Seoane). Eterna Cadencia, pp. 232-256. (Trabajo original publicado en 2009).

Jenkins, Henry. (1992). *Textual Poachers: Television Fans and Participatory Culture (Studies in Culture and Communication)*. Routledge.

Jenkins, Henry. (2012). 'Cultural Acupuncture': Fan Activism and the Harry Potter Alliance. *Transformative Works and Cultures*, 10. <https://doi.org/10.3983/twc.2012.0305>

Joyce, Simon, Stuart, Mark y Forde, Chris. (2023). Theorising labour unrest and trade unionism in the platform economy. *New Technology, Work and Employment*, 38(1), pp. 21–40. <https://doi.org/10.1111/ntwe.12252>

Kang, Haeryun. (21 de febrero del 2020). Inside Sajaegi, K-Pop's Open Secret. *NPR*. <https://www.npr.org/2020/02/21/808049441/inside-sajaegi-k-pops-open-secret>

Kelty, Chris. (2019a). *Two Bits. La trascendencia cultural del software libre*. (Trad. Ana M. Alconchel *et al.*) Icaria. (Trabajo original publicado en 2008).

Kelty, Chris. (2019b). *The Participant*. University of Chicago Press.

KFF (22 de enero de 2025). State and Federal Reproductive Rights and Abortion Litigation Tracker. KFF. <https://www.kff.org/report-section/state-and-federal-reproductive-rights-and-abortion-litigation-tracker-federal-litigation/>

Kienscherf, Markus. (2022). Surveillance Capital and Post-Fordist Accumulation: Towards a Critical Political Economy of Surveillance-for-Profit. *Surveillance & Society*, 20(1), pp. 18-29.

<https://doi.org/10.24908/ss.v20i1.14235>

Kitchin, Rob. (2014a). The real-time city? Big data and smart urbanism. *GeoJournal*, 79, pp. 1–14.

<https://doi.org/10.1007/s10708-013-9516-8>

Kitchin, Rob. (2014b). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. Sage.

Kitchin, Rob. (2020). Civil liberties or public health or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, 24 (3), pp. 362–81.

<https://doi.org/10.1080/13562576.2020.1770587>

La Voz de Galicia. (17 de octubre de 2024). Protesta en Vigo para reclamar más profesores de apoyo. *La Voz de Vigo*. https://www.lavozdeg Galicia.es/noticia/vigo/vigo/2024/10/17/vigo-sale-calle-escuela-inclusiva/0003_202410V17C4992.htm

Lafuente, Antonio. (2007). Los cuatro entornos del procomún. *Archipiélago*, 77–78, pp. 15–22.

<http://hdl.handle.net/10261/2746>

Larson, Erik. (1994). *Naked Consumer: How Our Private Lives Become Public Commodities*. Penguin Books.

Laudon, Kenneth C. (1986). *Dossier Society*. Columbia University Press.

Lazzarato, Maurizio. (2008). Postfacio. En Gerald Ragnig, *Mil Máquinas*. (Trad. Marcelo Expósito). Traficantes de Sueños. (Trabajo original publicado en 2008).

Lerner, Sharon. (12 de agosto de 2015). The Teflon Toxin DuPont and the Chemistry of Deception. *The Intercept*. Recuperado de: <https://theintercept.com/2015/08/11/dupont-chemistry-deception/>

Lersundi, Francisco. (11 de octubre de 1987). 'Huelga de embarazos' en Rumanía. *El País*.

https://elpais.com/diario/1987/10/11/internacional/560905215_850215.html

Lessig, Lawrence. (2009). *El Código 2.0*. (Trad. Maryam Itatí Portillo *et al.*). Traficantes de Sueños. (Trabajo original publicado en 2006).

Levy, Johanna y Romo Avilés, Nuria. (2019). “A good little tool to get to know yourself a bit better”: a qualitative study on users’ experiences of app-supported menstrual tracking in Europe. *BMC Public Health* (19), pp. 1–11. <https://doi.org/10.1186/s12889-019-7549-8>

Lewin, Kurt. (1946) Action research and minority problems. *J Soc. Issues*, 2(4), pp. 34–46.

<https://doi.org/10.1037/10269-013>

Lewis, Michael. (2014). *Flash Boys*. Norton.

Ley Orgánica 3/2018. (5 de diciembre de 2018). Protección de Datos Personales y garantía de los derechos digitales. *BOE Núm. 294*

Linebaugh, Peter (2013). *El Manifiesto de la Carta Magna. Comunes y libertades para el pueblo*. (Trad. Yaiza Hernández y Astor Díaz). Traficantes de Sueños. (Trabajo original publicado en 2008).

Liu, Jing-Cail. (s.f.) Wearable Face Projector. *Jing-Cai Liu*. <https://jingcailiu.com/wearable-face-projector/>

Lizcano, Emmánuel. (2006). *Metáforas que nos piensan*. Bajo Cero/Traficantes de Sueños.

Lloredo Alix, Luis (2020). Bienes comunes. *Eunomía. Revista en Cultura de la Legalidad.*, pp. 214-236. <https://doi.org/10.20318/eunomia.2020.5709>

López-Gabrielidis, Alejandra. (2020) *Datificación e Individuación. Estudio sobre la corporalidad digital en prácticas artísticas contemporáneas*. [Tesis doctoral. Universidad de Barcelona]. Barcelona.

López Trujillo, Noemí (3 de julio de 2023). Derivar a una mujer a otra comunidad para abortar vulnera sus derechos fundamentales, según el Constitucional. *Newtral*. <https://www.newtral.es/abortar-otra-comunidad-tribunal-constitucional/20230703/>

Lorenz, Taylor; Browningy, Kellen y Frenkel, Sheera. (21 de junio de 2020). TikTok Teens and K-Pop Stans Say They Sank Trump Rally. *The New York Times*. <https://www.nytimes.com/2020/06/21/style/tiktok-trump-rally-tulsa.html>

Lupton, Deborah. (2015). *Digital Sociology*. Routledge.

Luo, Wanying; Xie, Qi y Hengartner, Urs. (2009). FaceCloak: An Architecture for User Privacy on Social Networking Sites. *Proc. of 2009 IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT-09)*, pp. 26-33.

Lyon, David. (1994). *The Electronic Eye. The Rise of Surveillance Society*. University of Minnesota Press.

Lyon, David. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.

Lyon, David. (2003a). *Surveillance after September 11*. Polity.

Lyon, David. (2003b). *Surveillance as Social Sorting Privacy, risk, and digital discrimination*. Routledge.

Lyon, David. (2006). *Theorizing Surveillance: The Panopticon and Beyond*. Willan.

Lyon, David. (2007). *Surveillance Studies. An Overview*. Polity.

- Lyon, David (2015). *Surveillance After Snowden*. Polity
- Lyon, David. (2018). *The Culture of Surveillance*. Polity
- Lyon, David. (2022). *The Pandemic Surveillance*. Polity.
- Machlup, Fritz. (1962). *The Production and Distribution of Knowledge in the United States*. Princeton University Press.
- MacKinnon, Catharine. (1989). *Toward a Feminist Theory of the State*. Harvard University Press.
- Marmor, Andrei. (2015). What is the Right to Privacy? *Philosophy and Public Affairs*, 43 (1), pp. 3-26. <https://ssrn.com/abstract=2422380>
- Marras, Mirko y Laniado, David. (14 de junio de 2018). BarcelonaNow at “The Web Conference 2018”. DECODE. <https://decodeproject.eu/blog/barcelonanow-%E2%80%9Cweb-conference-2018%E2%80%9D>
- Marshall, Alfred. (1919). *Industry and Trade: A Study of Industrial Technique and Business Organization and of Their Influences on the Condition of Various Classes and Nations*. MacMillan and Co. Limited.
- Marshall, Thomas. H. (1950) *Citizenship and Social Class*. Cambridge University Press.
- Marwick, Arthur. (1988). *Total War and Social Change*. Macmillan.
- Marx, Gary. T. (1988). *Undercover: Police Surveillance in America*. University of California Press.
- Marx, Gary T. (2002). Identity and Anonymity: Some Conceptual Distinctions and Issues for Research. En Jane Caplan y John Torpey (eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton University Press. pp. 311-327.
- Marx, Gary T. (2007). Soft surveillance: the growth of mandatory volunteerism in collecting personal information - “Hey buddy can you spare a DNA”, en Torin Monahan, (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*. Routledge. (pp. 37-56).
- Marx, Karl. (1975). *El Capital. Tomos I y III*. (Trad. Pedro Scaron) Siglo XXI Editores. (Trabajo original publicado en 1867).
- Mathiesen, Thomas. (1997). The viewer society: Michel Foucault's “Panopticon” revisited. *Theoretical Criminology*, 1 (2), pp. 215-34. <https://doi.org/10.1177/13624806970010020>
- Mattelart, Armand. (2007). *Historia de la Sociedad de la Información*. (Trad. Guilles Multigner). Paidós. (Trabajo original publicado en 2001)

- Mattelart, Armand. (2009). *Un Mundo Vigilado*. (Trad. Guilles Multigner). Paidós. (Trabajo original publicado en 2007).
- Mattelart, Armand y Mattelart, Michèle. (2005). *Historia de las teorías de la comunicación*. (Trad. Antonio López Ruiz y Fedra Egea). Paidós Comunicación. (Trabajo original publicado en 1995).
- Mattelart, Armand y Vitalis, André. (2015). *De Orwell al Cibercontrol*. (Trad. Juan Carlos Miguel de Bustos). Gedisa. (Trabajo original publicado en 2014).
- Mayer-Schoenberger, Viktor; Cukier, Kenneth. (2013). *Big Data. A Revolution that will transform how we live, work, and think*. John Murray Publishers.
- McChesney, Robert. (2004). *The Problem of the Media*. Monthly Review Press.
- McChesney, Robert. (2014). *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*. The New Press.
- McGrath, John. (2004). *Loving Big Brother: Performance, Privacy and Surveillance Space*. Routledge.
- McLuhan, Marshall. (1996). *Comprender los medios de comunicación*. (Trad. Patrick Ducher). Paidós. (Trabajo original publicado en 1964)
- McNeill, William. (1984). *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*. University of Chicago Press.
- McQuillan, D. (2022). *Resisting AI. An Anti-fascist Approach to Artificial Intelligence*. Bristol University Press.
- Mejías, Ulises A. y Couldry, Nick. (2019). Colonialismo de datos: repensando la relación de los datos masivos con el sujeto contemporáneo. *Virtualis*, 10 (18), pp. 78-97.
- Messina, Chris (25 de agosto de 2007a). Groups for Twitter; or A Proposal for Twitter Tag Channels. *Factory Joe*. <https://factoryjoe.com/2007/08/25/groups-for-twitter-or-a-proposal-for-twitter-tag-channels/>
- Messina, Chris (22 de octubre de 2007b). Twitter hashtags for emergency coordination and disaster relief. *Factory Joe*. <https://factoryjoe.com/2007/10/22/twitter-hashtags-for-emergency-coordination-and-disaster-relief/>
- Meyerowitz, Joseph T. y Choudhury, Romit Roy. (2010). CacheCloak: enabling realtime location privacy for mobile users. *ACM SIGMOBILE Mobile Computing and Communications Review*, 13, (3), pp. 38-41. <https://doi.org/10.1145/1710130.1710138>

Miller, Arthur. (1971). *The Assault on Privacy*. The University of Michigan Press.

Mills, Mark P. (2013). *The Cloud begins with Coal*. Digital Power Group. Disponible en:
https://www.tech-pundit.com/wp-content/uploads/2013/07/Cloud_Begins_With_Coal.pdf

Mokrosinska, Dorota. (2018). Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy. *Laws and Philosophy*, 37, pp. 117-143. <https://doi.org/10.1007/s10982-017-9307-3>

Monckton, Paul. (22 de mayo de 2024). Radical Google Photos Update Allows AI To Manage Your Memories, But Should You Trust It?. *Forbes*.
<https://www.forbes.com/sites/paulmonckton/2024/05/22/google-photos-will-change-forever-after-this-game-changing-ai-update/>

Monge, Fernando; Barns, Sarah; Kattel, Rainer y Bria, Francesca. (2022). *A new data deal: the case of Barcelona*. UCL Institute for Innovation and Public Purpose, Working Paper Series (No. WP 2022/02).
<https://www.ucl.ac.uk/bartlett/public-purpose/wp2022-02>

Moore, Barrington. (1984). *Privacy: Studies in Social and Cultural History*. M. E. Sharpe.

Morozov, Evgeny. (4 de febrero de 2019). Capitalism's New Clothes. *The Baffler*.
<https://thebaffler.com/latest/capitalisms-new-clothes-morozov>

Morozov, Evgeny. (2022). Crítica de la razón Tecnofeudal. (Trad. Jose María Amoroto, Álvaro García-Ormaechea, Juan Mari Madariaga, Cristina Piña y Ana Useros). En Carlos Prieto del Campo (ed.). *New Left Review 133/134*, (pp. 99-140). Traficantes de Sueños.

Morozov, Evgeny. (3 de abril de 2023). Ni es inteligente ni es artificial: esa etiqueta es una herencia de la Guerra Fría. *El País*. <https://elpais.com/ideas/2023-04-03/ni-es-inteligente-ni-es-artificial-esa-etiqueta-es-una-herencia-de-la-guerra-fria.html>

Morozov, Evgeny. (agosto de 2024). Otra inteligencia artificial es posible. *Le Monde Diplomatique en Español*. <https://mondiplo.com/otra-inteligencia-artificial-es-posible>

Moulier Boutang, Yann. (2012). *La abeja y el economista*. (Trad. Samuel Simón Pulido y Marisa Pérez Colina). Traficantes de Sueños. (Trabajo original publicado en 2010).

Mojtar-Mendieta, Luz; Rascón-Gómez, María Teresa y Calderón-Almendros, Ignacio. (2025). Students as subjects. Resistance, youth agency, and inclusive education through participatory action research. *International Journal of Qualitative Studies in Education*. pp. 1-19.

<https://doi.org/10.1080/09518398.2025.2454281>

Mumford, Lewis. (1998). *Técnica y civilización*. (Trad. Constantino Aznar de Acevedo). Alianza. (Trabajo original publicado en 1934).

Myers West, Sarah. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 58, pp. 20-41. <https://doi.org/10.1177/0007650317718185>

Neff, Gina. [@ginasue]. (2022, 24 de junio). *Right now, and I mean this instant, delete every digital trace of any menstrual tracking. Please.* [Tuit]. Recuperado de: <https://web.archive.org/web/20230528093552/https://twitter.com/ginasue/status/1540354137304760321>

Newman, Lily Hay. (5 de mayo de 2022). How to Protect Your Digital Privacy if *Roe v. Wade* Fall. *The Wired*. <https://www.wired.com/story/roe-v-wade-privacy-practices>

Niquille, Simone C. (2013). REALFACE Glamouflage: Tricking Facebook's Facial Recognition with Weird Patterns. *Design for sustainability*. <https://www.designforsustainability.studio/signals/realface-glamouflage>

Nissenbaum, Helen. (2004). Privacy as contextual integrity. *Washington Law Review*, 79 (1), pp. 119-158.

Nissenbaum, Helen. (2009). Privacy in Context. Technology, Policy and the Integrity of Social Life. *Stanford University Press*.

Noiriel, Gérard. (1998). Surveiller les déplacements ou identifier les personnes ? Contribution à l'histoire du passeport en France de la Ie à la IIIe République. *Genèses. Sciences sociales et histoire*, 30, pp. 77-100.

NOYB. (10 de diciembre de 2018). “Pay or Okay” bei derStandard.at?. NOYB. <https://noyb.eu/en/pay-or-okay-bei-derstandardat>

NOYB. (10 de diciembre de 2019). Say “NO” to cookies – yet see your privacy crumble?. NOYB. <https://noyb.eu/en/say-no-cookies-yet-see-your-privacy-crumble>

NOYB. (2020). Informe anual NOYB 2018/2019. NOYB. <https://noyb.eu/en/annual-report-2018-2019>

NOYB. (2021). Informe anual NOYB 2020. NOYB. <https://noyb.eu/en/annual-report-2020-out-now>

- NOYB. (2022a). Informe anual NOYB 2021. NOYB. <https://noyb.eu/en/annual-report-2021-out-now>
- NOYB. (23 de mayo de 2022b). Open Letter on the Future of EU-US Data Transfers. NOYB. <https://noyb.eu/en/open-letter-future-eu-us-data-transfers>
- NOYB. (9 de agosto de 2022c). 226 complaints lodged against deceptive cookie banners. NOYB. <https://noyb.eu/en/226-complaints-logged-against-deceptive-cookie-banners>
- NOYB. (2023a). Informe anual NOYB 2022. NOYB. <https://noyb.eu/en/annual-report-2022-out-now>
- NOYB. (24 de enero de 2023b). Data Protection Authorities support noyb's call for fair yes/no cookie banners. NOYB. <https://noyb.eu/en/data-protection-authorities-support-noybs-call-fair-yesno-cookie-banners>
- NOYB. (3 de julio de 2023c). noyb win: First major fine (€ 1 million) for using Google Analytics. NOYB. <https://noyb.eu/en/noyb-win-first-major-fine-eu-1-million-using-google-analytics>
- NOYB. (29 de septiembre de 2023d). € 5,8 million fine for Grindr confirmed. NOYB. <https://noyb.eu/es/eu-58-million-fine-grindr-confirmed>
- NOYB. (28 de noviembre de 2023e). noyb files GDPR complaint against Meta over “Pay or Okay”. NOYB. <https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay>
- NOYB. (2024a). Informe anual NOYB 2023. NOYB. <https://noyb.eu/en/annual-report-2023-out-now>
- NOYB. (14 de junio 2024b). (Preliminary) noyb WIN: Meta stops AI plans in the EU. NOYB. <https://noyb.eu/en/preliminary-noyb-win-meta-stops-ai-plans-eu>
- NOYB. (12 de noviembre 2024c). Ads: Meta wants to be 'less illegal' - but much more annoying... NOYB. <https://noyb.eu/en/ads-meta-wants-be-less-illegal-much-more-annoying>
- NOYB. (19 de diciembre de 2024d). Want to book a Ryanair flight? Prepare for a face scan!. NOYB. <https://noyb.eu/es/want-book-ryanair-flight-prepare-face-scan>
- O'Neill, Cathy. (2017). *Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia*. (Trad. Violeta Arranz de la Torre). Capitán Swing. (Trabajo original publicado en 2016).
- Olsen, Frances. (1993). Feminist Critiques of the Public/Private Distinction. *Constitutional Commentary*, 10, pp. 319-327.

Oviedo Sotelo, Daniel (2015). *Solo sé que no sé nada*. Book Sellers.

Pascual, Manuel. (17 de abril de 2024). Lavender, la inteligencia artificial de Israel que decide a quién se bombardea en Gaza. *El País*. <https://elpais.com/tecnologia/2024-04-17/lavender-la-inteligencia-artificial-de-israel-que-decide-a-quien-se-bombardea-en-gaza.html>

Pateman, Carole. (1989). *The Disorder of Women: Democracy, Feminism, and Political Theory*. Stanford University Press.

Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea. (2000). *Carta de Derechos Fundamentales de la Unión Europea*. Diario Oficial de las Comunidades Europeas.

Pascual, Manuel G. (14 de noviembre de 2023). La inteligencia artificial se bebe miles de millones de litros de agua. *El País*. <https://elpais.com/tecnologia/2023-11-14/la-inteligencia-artificial-se-bebe-miles-de-millones-de-litros-de-agua.html>

Peertube (s.f.). Qué es Peertube. Peertube. <https://joinpeertube.org/es>

Pecora, Vicent P. (2002). The culture of surveillance. *Qualitative Sociology*, 25 (3), pp. 345-58. <https://doi.org/10.1023/A:1016081929646>

Peirano, Marta. (2019). *El enemigo conoce el sistema*. Debate.

Peirano, Marta. (2022). *Hacia una nueva ilustración digital europea*. Fundación Carolina, Oxfam Intermón. <https://doi.org/10.33960/issn-e.1885-9119.DTFO03>

Peirano, Marta. (30 de enero de 2024). La lección de las ‘swifties’: salir a pelear. *El País*. <https://elpais.com/opinion/2024-01-30/la-leccion-de-las-swifties-salir-a-pelear.html>

Peirano, Marta. (8 de agosto de 2024). Google es un monopolio ilegal. Ahora qué pasa. *El País*. <https://elpais.com/opinion/2024-08-08/google-es-un-monopolio-ilegal-ahora-que-pasa.html>

Peñamarín, Cristina (14 de abril de 2020). La imaginación post-pandemia y el peligro de las metáforas. *CTXT*. <https://ctxt.es/es/20200401/Firmas/31917/covid-19-imaginacion-meta>

Pérez Alonso, Jorge. (2023). Crónica de la batalla judicial en torno al aborto: de Roe v. Wade a Dobbs v. Jackson. *Teoría y Realidad Constitucional*, 51, pp. 529-564. <https://doi.org/10.5944/trc.51.2023.37519>

Pérez Colomé, Jordi. (28 de julio de 2020). El día en que las grandes tecnológicas dejaron de ser intocables. *El País*. <https://elpais.com/tecnologia/2020-07-28/el-dia-en-que-las-grandes-tecnologicas-dejaron-de-ser-intocables.html>

Pérez Colomé, Jordi. (9 de septiembre de 2020). El Gobierno publica un código incompleto y confuso de la 'app' Radar Covid. *El País*. <https://elpais.com/tecnologia/2020-09-09/el-gobierno-publica-hoy-el-codigo-de-radar-covid-casi-medio-ano-despues-de-lanzar-el-proyecto.html>

Pérez Yélamo, Claudia. (2024). *LA BATALLA POR LA PRIVACIDAD EN LA UE. Análisis del modelo pay or okay de Meta en la lucha europea por la salvaguarda del consentimiento libre*. [Trabajo Fin de Grado no publicado]. Universidad de Málaga.

Perragin, Charles y Renouard, Guillaume. (Julio de 2021). Los cables submarinos, un asunto de Estados. *Le Monde Diplomatique en español*. <https://mondiplo.com/los-cables-submarinos-un-asunto-de-estados>

Pitron, Guillaume. (Octubre de 2021). Cuando la tecnología digital destruye el planeta. *Le Monde Diplomatique en español*. <https://mondiplo.com/cuando-la-tecnologia-digital-destruye-el-planeta>

Piza, Eric L.; Welsh, Brandon C.; Farrington, David P.; Thomas, Amanda L. (2019). CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis. *Criminology & Public Policy*, 18(1), pp. 135-159. <http://dx.doi.org/10.1111/1745-9133.12419>

Porat, Mark Uri. (1977). *The Information Economy: Definition and Measurement*. Government Printing Office.

Poster, Mark. (1990). *The Mode of Information: Poststructuralism and Social Context*. University Chicago Press.

Priest, Dana. (14 de agosto de 2013). Government surveillance spurs Americans to fight back. *The Washington Post*. https://www.washingtonpost.com/lifestyle/style/government-surveillance-spurs-americans-to-fight-back/2013/08/14/edea430a-0522-11e3-a07f-49ddc7417125_story.html

Profesional Review. (11 de diciembre de 2022). Side-channel attacks: ¿qué son? *Profesional Review*. <https://www.profesionalreview.com/2022/12/11/side-channel-attacks/#%C2%BFQue son Side-channel attacks>

Rachels, James. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, 4 (4), pp. 323-333. <http://www.jstor.org/stable/2265077>

Raunig, Gerald (2023). *Dividuum*. (Trad. Raúl Sánchez Cedillo). Subtextos. (Trabajo original publicado en 2015).

Raz, Joseph. (1988). *The Morality of Freedom*. Oxford University Press.

Raz, Joseph. (1995). Rights and Politics. *Indiana Law Journal*, 71 (1), pp. 27-44.

Razac, Olivier. (22 de marzo de 2007). Bracelet électronique mobile: les barreaux à la cheville. *Libération*. Recuperado de: <https://www.liberation.fr/societe/2007/03/22/bracelet-electronique-mobile-les-barreaux-a-la-cheville> 88194/

Real Academia Española (RAE). (s.f.). Ofuscar. En *Diccionario de la lengua española*. Consultado el 29 de enero de 2025, de <https://dle.rae.es/ofuscar>

Redondo, Iván (10 de octubre de 2024). Días de futuro terror. *La Vanguardia*. <https://www.lavanguardia.com/politica/20241014/10018261/dias-futuro-terror.html>

Reiman, Jeffrey H. (1976). Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 6, (1), pp. 26-44. <https://www.jstor.org/stable/2265060>

Reisz, Matthew. (15 de febrero 2019). Philosopher Explores How to Combat Toxicity of Social Media. *Times Higher Education*. <https://www.timeshighereducation.com/news/philosopher-explores-how-combat-toxicity-social-media>

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, 4 de mayo de 2016, pp. 1-88. <http://data.europa.eu/eli/reg/2016/679/oj>

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea, 13 de junio de 2024, pp. 1-144. <http://data.europa.eu/eli/reg/2024/1689/oj>

Ricaurte Quijano, Paola. (2023). *Descolonizar y despatriarcalizar las tecnologías*. Centro Cultural Digital.

Rich, Natalie. (6 de enero de 2016). The Lawyer Who Became DuPont's Worst Nightmare. *The New York Times Magazine*. <https://www.nytimes.com/2016/01/10/magazine/the-lawyer-who-became-duponts-worst-nightmare.html>

Richards, Neil M. (2006). The Information Privacy Law Project. *Georgetown Law Journal*, 94, pp. 1087-

1140. <https://ssrn.com/abstract=941181>

Richards, Neil. (2022). *Privacy Matters*. Oxford University Press.

Rieback, Melanie. (23 de diciembre de 2021). Putting Post Growth Theory Into Practice. *Resilience*. <https://medium.com/postgrowth/putting-post-growth-theory-into-practice-70033f334088>

Roché, Sebastian. (1996). *La Société incivile*. Seuil.

Roio, Denis; Bria, Francesca; Barritt, James; Hoepman, Japp-Henk; Villiers, Mark de; Samuel, Prima; Danezis, George; Demeyer, Tom; Bano, Shehar y Sagarra, Oleguer. (2018). DECODE Whitepaper v1.0. *DECODE Project*. <https://decodeproject.github.io/whitepaper/>

Rosen, Jeffrey. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. Random House.

Rosenfeld, Michael J., Thomas, Reuben J., y Falcon, Maja. (2018). How Couples Meet and Stay Together (HCMST), Wave 1 2009, Wave 2 2010, Wave 3 2011, Wave 4 2013, Wave 5 2015. *Inter-university Consortium for Political and Social Research*. <https://doi.org/10.3886/ICPSR30103.v8>

Rouvroy, Antoinette y Stiegler, Bernard. (2016). The Digital Regime of Truth: From the Algorithmic Governmentality to a New Rule of Law. (Trad. Anaïs Nony y Benoît Dillet). *La Deleuziana*, 3, pp. 6-29. http://www.ladeleuziana.org/wp-content/uploads/2016/12/Rouvroy-Stiegler_eng.pdf

Rubí Puig, Antoni; Herrerías Castro, Laura. (2022). “Radar COVID” y protección de datos personales. *InDret*, 4, pp. 249-280. <https://raco.cat/index.php/InDret/article/view/406128>.

Sánchez, Ana. (11 de octubre de 2022). El fracaso de Radar Covid: echa el cierre tras notificar el 1,17% de contagios e invertir 4,2 millones. *Eleconomista.es*. <https://www.eleconomista.es/salud/noticias/11985548/10/22/El-fracaso-de-Radar-Covid-echa-el-cierre-tras-notificar-el-117-de-contagios-e-invertir-42-millones.html>

Sánchez Cedillo, Raúl. (2021). *Lo absoluto de la democracia: Contrapoderes, cuerpos-máquina, sistema red transdividual*. Subtextos.

Schiller, Dan. (1999). *Digital Capitalism: Networking the Global Market System*. MIT Press.

Scanlon, Thomas. (1975). Thomson on Privacy. *Philosophy & Public Affairs*, 4(4), pp. 315–322. <http://www.jstor.org/stable/2265076>

Schwartz, John. (4 de septiembre de 2001). Giving Web a Memory Cost Its Users Privacy. *The New York Times*. <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy>

- Schwartz, Paul M. (1989). The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, *The American Journal of Comparative Law*, 37 (4), pp. 675-701. <https://doi.org/10.2307/840221>
- Schwartz, Paul M. (1999). Privacy and Democracy in Cyberspace, *Vanderbilt Law Review*, 52 (6), pp. 1609-1702. <https://doi.org/10.2139/ssrn.205449>
- Scholz, Trebor. (2013). *Digital Labor: The Internet as Playground and Factory*. Routledge.
- Scott, James. (1985). *Weapons of the Weak: Everyday Forms of Peasant Resistance*. Yale University Press.
- Seltzer, William y Anderson, Margo. (2001). The Dark Side of Numbers. The Role of Population Data Systems in Human Rights Abuses. *Social Research*, 68, pp. 481-451. <http://www.jstor.org/stable/40971467>
- Shan, Shaw; Ding, Wenxin; Passananti, Josephine; Wu, Stanley; Zheng, Haitao y Zhao, Ben Y. (2024). Nightshade: Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models. *IEEE Symposium on Security and Privacy (SP)*, pp. 807-825. <https://doi.org/10.1109/sp54263.2024.00207>
- Shannon, Claude y Weaver, Warren. (1949). *The Mathematical Theory of Communication*. University of Illinois Press.
- Shils, Edward. (1966). Privacy: Its Constitution and Vicissitudes. *Law and Contemporary Problems*, 31 (2), pp. 281-306. <https://doi.org/10.2307/1190672>
- Sikka, Tina. (2019). *Climate Technology, Gender, and Justice. The Standpoint of the Vulnerable*. Springer. <https://doi.org/10.1007/978-3-030-01147-5>
- Smink, Verónica (6 de marzo de 2023). Los cientos de miles de trabajadores en países pobres que hacen posible la existencia de inteligencia artificial como ChatGPT (y por qué generan controversia). *BBC News Mundo*. <https://www.bbc.com/mundo/noticias-64827257>
- Snowden, Edward. (2019). *Vigilancia permanente*. (Trad. Esther Cruz Santaella). Planeta. (Trabajo original publicado en 2019).
- Solera Navarro, Fátima. (2023). Ofuscación. Tácticas de resistencia frente al capitalismo de vigilancia. *Teknokultura*, 20 (1), pp. 125-131. <https://doi.org/10.5209/tekn.80980>
- Solera Navarro, Fátima. (2025). Decidir Decidim: prácticas recursivas para una democracia participativa. En Jesús Sabariego *et al.* (eds.), *Algoritmos II*. Tirant lo Blanch. [pendiente de publicación].

Solera Navarro, Fátima y Cabello Fernández-Delgado, Florencio. (15 de mayo de 2024). Cómo rodar un movimiento: el proceso de creación del documental “Educación inclusiva: Quererla es crearla”. [Ponencia]. *V Congreso Internacional sobre Movimientos Sociales y TIC Move.net*.
<https://hdl.handle.net/10630/38009>

Solera Navarro, Fátima y Gómez Alcalde, Marina (2025). Desimplantar Matrix de la matriz. En Jesús Sabariego *et al.* (eds.), *Algoritarismos II*. Tirant lo Blanch. [pendiente de publicación]

Solnit, Rebecca. (2009). *A paradise built in hell*. Viking

Solove, Daniel. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, 53, pp. 1393-1462. <https://doi.org/10.2139/ssrn.248300>

Solove, Daniel. (2003). The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure. *Duke Law Journal*, 53, pp. 967-1065. <https://doi.org/10.2139/ssrn.440200>

Solove, Daniel. (2006). *The Digital Person*. New York University Press.

Solove, Daniel. (2009). *Understanding Privacy*. Harvard University Press.

Solove, Daniel. (2011). *Nothing to Hide*. Yale University Press.

Sotelino, Begoña R. (14 de septiembre de 2024). Héctor no podrá seguir en el IES Valadares sin apoyos para niños especiales. *La Voz de Galicia*.
https://www.lavozdeg Galicia.es/noticia/vigo/2024/09/14/hector-podra-seguir-ies-valadares-apoyos-ninos-especiales/0003_202409V14C3992.htm

Srnicek, Nick. (2017). *Platform Capitalism*. Polity.

Stake, Robert E. (1995). *The Art of Case Study Research*. Sage.

Stallman, Richard. (2004). *Software libre para una sociedad libre*. (Trad. Jaron Rowan, Diego Sanz Paratcha y Laura Trinidad). Traficantes de Sueños. (Trabajo original publicado en 2002).

Staples, William. (2000). *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Rowman and Littlefield.

Sumrall, Robert F. (febrero de 1973). Ship Camouflage (WWII): Deceptive Art. *United States Naval Institute Proceedings*, pp. 67–81.

Taylor, Linnet; Sharma, Gargi ; Martin, Aaron y Jameson, Shazade (eds.).(2020). *Data Justice and COVID-19: Global Perspectives*. Meatspace Press.

The Guardian. (9 de junio de 2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>

Thompson, Edward P. (1967). Time, work-discipline and industrial capitalism. *Past and Present*, 38, pp. 56-59. <https://www.jstor.org/stable/649749?origin=JSTOR-pdf>

Toro, Paula del. (28 de septiembre de 2024). Más del 81% de los abortos de 2023 se realizaron en la sanidad privada a pesar de ser un derecho financiado. *Newtral*. <https://www.newtral.es/abortos-2023-sanidad-privada/20240928/>

Toubiana, Vicent [vtoubiana]. (s.f.). TrackMeNot. [Repositorio]. GitHub. <https://github.com/vtoubiana/TrackMeNot> (Recuperado el 3 de febrero de 2025).

Townley, Dafydd. (2021). *The Year of Intelligence in the United States*. Palgrave Macmillan Cham. <https://doi.org/10.1007/978-3-030-67646-9>

Tratado de la Unión Europea y Tratado de Funcionamiento de la Unión Europea. Versiones consolidadas. DOUE. núm. 83, de 30 de marzo de 2010, pp. 1-388.

Tribunal de Justicia de la Unión Europea. Sentencia de 8 de abril de 2014. Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014. Comunicaciones electrónicas — Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea (Asuntos C-293/12 y C-594/12).

Tribunal de Justicia de la Unión Europea. Sentencia de 13 de mayo de 2014. Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 (petición de decisión prejudicial planteada por la Audiencia Nacional — España) — Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Asunto C-131/12).

Tudela, Ana y Delgado, Antonio. (14 de enero de 2025). Alerta PFAS: 70 años de engaños de la industria química que ya han llegado al grifo y a tu sangre. *Datadista*. <https://especiales.datadista.com/medioambiente/alerta-pfas-papeles-secretos-contaminacion-quimica/>

Turkington, Richard C.; Allen, Anita L. (1999). *Privacy Law: Cases and Materials*. West Group.

Ullah, Areeb. (17 de noviembre de 2020). Muslim Pro prayer app cuts ties with tech firm after US

military buys user data. *Middle East Eye*. <https://www.middleeasteye.net/news/us-military-data-muslim-pro-apps-ties-severed>

United States Census Bureau.(22 de julio de 2021). La privacidad diferencial y el Censo del 2020. United States Census Bureau. <https://www.census.gov/library/fact-sheets/2021/differential-privacy-and-the-2020-census/differential-privacy-and-the-2020-census-spanish.html>

Valdivia, Ana. (2024). The supply chain capitalism of AI: a call to (re)think algorithmic harms and resistance through environmental lens. *Information, Communication & Society*, pp. 1-17. <https://doi.org/10.1080/1369118X.2024.2420021>

van Dijck, José. (2013). *The Culture of Connectivity. A Critical History of Social Media*. Oxford University Press.

van Dijck, José. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, (12), pp. 197-208. <https://doi.org/10.24908/ss.v12i2.4776>

van Dijck, José; Poell, Thomas. (2013). Understanding Social Media Logic. *Media and Communication*, (1), pp. 2-14. <https://doi.org/10.12924/mac2013.01010002>

Vargas Jiménez, Ileana. (2012). La entrevista en la investigación cualitativa: nuevas tendencias y retos. *Revista CAES*, 3I (1), pp. 120-139. <https://doi.org/10.22458/caes.v3i1.436>

Véliz, Carissa. (2021) *Privacidad es Poder. Datos, Vigilancia y Libertad en la era Digital*. (Trad. Albino Santos Mosquera y Carissa Véliz). Debate. (Trabajo original publicado en 2020).

Véliz, Carissa. (2022a). Digitalization, Surveillance, Colonialism. *Liberties*, 3 (1), pp. 20-40.

Véliz, Carissa. (2022b). Self-Presentation and Privacy Online. *Journal of Practical Ethics*, 10 (1). <https://doi.org/10.3998/jpe.2379>

Véliz, Carissa. (2023). The Surveillance Delusion. In *The Oxford Handbook of Digital Ethics*, edited by Carissa Véliz. Oxford University Press.

Véliz, Carissa. (2024). *The Ethics of Privacy and Surveillance*. Oxford University Press.

Veyne, Paul. (1992). The Roman Empire. En Phillippe Ariès y Georges Duby (eds.), *A History of Private Life: From Pagan Rome to Byzantium* (pp. 5-207). (Trad. Arthur Goldhammer). Harvard University Press. (Trabajo original publicado en 1985).

Virilio, Paul. (1994) *The Vision Machine*. British Film Institute.

- Virilio, Paul. (1996). *Cybermonde. La politique du pire*. Textuel.
- Virilio, Paul. (1999). *La inercia polar*. (Trad. Miguel Rubio). Trama. (Trabajo original publicado en 1990).
- Wajcman, Judy. (2006). *El Tecnofeminismo*. (Trad. Magalí Martínez Solimán) Catedra. (Trabajo original publicado en 2004).
- Warren, Samuel D.; Brandeis, Louis. D. (1890). The Right to Privacy. *Harvard Law Review*, 4 (5), pp. 193-220. <https://doi.org/10.2307/1321160>
- Watson, Gary. (2013). Moral Agency. In *The International Encyclopedia of Ethics*.
- Weber, Max. (1930). *The Protestant ethic and the spirit of capitalism* (Trad. Talcott Parson). Scribner. (Trabajo original publicado en 1904).
- Weber, Max. (1946). En Hans Gerth y C. Wright Mills (eds.). *From Max Weber: essays in sociology*. Oxford University Press.
- Weiss, Linda. (2014). *Beyond a Military-Industrial Divide: Innovating for Both Security and Commerce*. Cornell University Press
- Weiser, Marx. (1993). Some Computer Science Issues in Ubiquitous Computing. *Communications of the ACM*, 36, pp. 75-84. <https://doi.org/10.1145/159544.159617>
- Welsh, Brandon C., Farrington, David. (2004). Surveillance for Crime Prevention in Public Space: Result and Policy Changes. *Criminology and Public Policy*, 3 (3). pp. 497-526. <https://doi.org/10.1111/j.1745-9133.2004.tb00058.x>
- Wengrow, David. (16 septiembre de 2019). Repensando las ciudades, desde sus bases. *Arquine*. <https://arquine.com/repensando-las-ciudades-desde-sus-bases/>
- Wiener, Norbert. (1948). *Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine*. MIT Press.

- Winner, Langdon. (1985) Do Artifacts Have Politics? en: Donald MacKenzie y Judy Wajcman (eds.), *The Social Shaping of Technology*. Open University Press, pp. 28-40.
- Wolff, Jonathan. (1998). Fairness, Respect, and The Egalitarian Ethos. *Philosophy and Public Affairs*, 27 (2), pp. 97-122. <https://doi.org/10.1111/j.1088-4963.1998.tb00063.x>
- World Economic Forum. (Enero 2011). Personal Data: The Emergence of a New Asset Class. *We Forum*. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
- WWF. (s.f.) *PERFLUORINATED CHEMICALS (PFCs) (INCL. PFOS & PFOA)*. *Factsheet*. WWF. https://wwfeu.awsassets.panda.org/downloads/fact_sheet_pfcs_food.pdf
- Zakrzewski, Cat; Verma, Pranshu y Parker, Claire. (3 de Julio de 2022). Texts, web searches about abortion have been used to prosecute women. *The Washington Post*. <https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/>
- Zhang, Qian y Negus, Keith. (2020). East Asian pop music idol production and the emergence of data fandom in China. *International Journal of Cultural Studies*, 23(4), pp. 493–511. <https://doi.org/10.1177/1367877920904064>
- Ziegler, Philip. (1969). *The Black Death*. Harper and Row Publishers.
- Zinn, Howard. (1991). Machiavellian Realism and U.S. Foreign Policy: Means and Ends. *Third World Traveller*. https://thirdworldtraveler.com/Zinn/Machiavelli_ForPol.html
- Zuboff, Shoshana; Maxmin, James. (2002). *The Support Economy*. Penguin Publishing Group.
- Zuboff, Shoshana. (15 de septiembre 2014). A Digital Declaration: Big Data as Surveillance Capitalism. *FAZ.NET*. <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html>
- Zuboff, Shoshana. (2020). *La era del capitalismo de la vigilancia*. (Trad. Albino Santos Mosquera). Paidós. (Trabajo original publicado en 2019).
- Zureik, Elia. (2003). Theorizing surveillance: The case of the workplace, en David Lyon (ed.). *Surveillance as Social Sorting*. Routledge.

Anexos

Anexo I: Transcripción de la entrevista a Martín Nadal

14 de noviembre de 2023.

Duración total 47 minutos 52 segundos.

[00:00:27]

M: Pues mi nombre es Martín Nadal, mmmm. Mi nombre es Martín Nadal, soy de Madrid, estudié... ingeniería informática hace mucho tiempo. Luego hice bastante, siempre me ha interesado mucho... me ha interesado mucho el arte, yo la programación la veo como un material, como un material creativo. Igual que a mí, de las cosas que más me interesan, es, dibujar y programar, lo veo cosas súper parecidas, o sea, entiendo que en mi cerebro va como en el mismo rollo. O sea, y yo entiendo la programación como un material, un material creativo. Además, como todo está, como es tecnología, todo es código, te permite decir cosas y te permite lanzar nuevos mensajes, o sea, me parece muy potente, artísticamente.

[00:01:19]

M: Con ese motivo, viajé a Linz, donde hice el [Máster de Interface Culture](#), en la Universidad de Diseño, de Arte y Diseño Industrial de Linz. Donde, bueno, para mí fue, muy, o sea, fue, vamos, muy importante.

[00:01:36]

M: El primer cambio es el primer golpe de suerte, lo que hace una persona, así que le gustaba la tecnología, le gustaba el arte... Madrid... 2000 y que no sabe muy bien qué hacer con su existencia. Que es el golpe de suerte, lo tuve con Madrid Medialab. Madrid Medialab que es una institución que está fundada por Karin [Karin Ohlenschläger], que luego estuvo en La Laboral, y entonces de repente ahí llega una exposición de las electrónicas del año 2006, hay una serie de talleres que se organizan con gente como David Cuartielles de Arduino, gente como Zach Lieberman de Open Frameworks... Donde de repente ves que hay otra cosa, ¿no?, o sea, yo estaba en una universidad que era como, tío, una base de datos que yo no... yo no sé, si yo con esto voy a hacer algo en mi vida o le veo alguna utilidad ¿no?.

[00:02:22]

M: O sea, era un momento muy concreto, porque tampoco... o sea, porque no había nada así de gráficos o de algo que te pudiera interesar, lo que te decía un poco, ¿no? Yo ya intuía que, que el código era algo muy potente y que me iba a servir mucho para, pues a lo mejor me iba a servir mucho que, que se podían hacer cosas diferentes que hacer una hoja de cálculo, ¿no? Entonces, para mí ese fue mi primer golpe de suerte. Entonces, pues yo estudiaba ahí, tuve la suerte de colaborar con algunos artistas y de trabajar... Al principio es un camino que hace bastante la gente, que es, bueno, colaboras y das asistencia técnica, a otros artistas que está bien, porque te permite vivir, de alguna manera, relacionado con eso, aunque no completamente... Ahí hay un, o sea, ahí hay un dilema grande, ¿no? Y es... el... el tema que, o sea, vamos, o sea hay como una disyuntiva entre el artista y el ingeniero, el artista piensa que el ingeniero no vale nada y el ingeniero piensa que lo que hace el artista es una estupidez. Entonces, está siempre muy bien tener las dos partes, o sea, porque puedes así ser un poco más... más

independiente. Pero bueno, es super importante tratar con respeto a los artistas y es súper importante tratar con respeto a los ingenieros.

[00:03:42]

M: Bueno, entonces, estuve en eso. Esto, tuve la suerte, ya te digo, que Madrid Medialab fue súper importante, fui a las primeras electrónicas, con lo cual siempre las electrónicas, este que está en Linz... Para mí siempre ha sido súper importante, referente. Bueno, por cosas de la vida, me dediqué a hacer eso... me dediqué, o sea, dejé de centrarme tanto en el arte. Bueno porque la institución, de alguna manera decayó... ¿sabes? Cuando Medialab se volvió más, más colaborativa. Y yo ya... estaba más lejos de mi casa, lo que fuera, ¿no?

[00:04:10]

M: Entonces yo ya tuve una vida más normal, pues trabajando, estuve muchos años haciendo como juegucitos para teléfonos móviles y cosas así, nada así muy interesante, pero bueno, supongo te sirve de algo. Y luego en el... llega un momento en el que sale la oportunidad del máster, de ir al máster, de Interface Culture en Linz y yo en esa época ya tenía mis años, entonces dije, pues lo haces ahora o no lo haces nunca ¿no? Entonces cogí y lo hice, era justamente al final de 2013, todavía quedaban restos de la crisis, mi pareja era arquitecto y tampoco tenía un futuro, era una cosa un poco como de, tenemos que salir de aquí, esto es una excusa que... no sé. También fue muy bonito y creo que he tenido mucha suerte, yo creo que Linz, y Austria en general, es un sitio al que le agradezco mucho.

[00:05:01]

M: Y, no sé, luego pues desde ahí pues he seguido trabajando, principalmente he colaborado mucho con mi colega de esa universidad sobre... bueno a mí siempre me ha interesado el tema, los temas financieros, los flujos de dinero y cómo afectan a la sociedad, tengo una serie de proyectos que se llaman [*Money Never Sleeps*](#).

Y otro que se llama [*BitterCoin*](#) que es el más conocido, hecho con César Escudero Andaluz, que habla, que es una pieza que es de 2016, que es de las primeras piezas que hablan sobre la problemática de la criptomoneda, bueno y esa pieza, por ejemplo, surge de la fascinación que es cómo se construye el valor, o sea, cómo un ordenador puede empezar a construir valor, vamos a mí eso me flipa.

[00:05:47]

M: Y entonces estudié mucho el proceso, *BitterCoin* es un minero que tiene en una, que está en una calculadora antigua y, bueno es un proyecto, realmente no tiene nada que ver, estuve trabajando mucho tiempo con blockchain, trabajando siempre en una, en un tema muy, o sea, como con mucha, no sé, o sea, primero con mucha fascinación, pero luego con mucho, con mucha duda, ¿no?, o sea, con mucha duda no, como que no me, o sea, pues eso, el rollito *cryptobro*, el rollito ese nunca me ha interesado.

Y por ejemplo, una cosa muy buena que hicimos César y yo, los dos es que nunca tuvimos criptomonedas, con lo cual, nuestro discurso fue como bastante neutral. O sea, si acaso, y tuvimos, vamos yo, por ejemplo, compré un poco de bitcoin, cuando estaba a 500€ y lo regalé como para ver la experiencia, ¿sabes?. Pero vamos, yo creo eso, que mola, lo de que poder estar un poco alejado y eso y vamos, por lo menos tener una opinión más honesta, no te digo que todo sea ahora una maravilla, pero que bueno, que por lo menos es más honesto.

[00:06:51]

M: Y ya de ahí estuve trabajando mucho, entonces en 2019 empiezo a trabajar en *Fangø* y me empezó a interesar mucho lo del capitalismo de vigilancia ¿no?, cuando Shoshana Zuboff, escribió el libro este de *La era del Capitalismo de Vigilancia*, a mí ya me interesaba bastante, por el tema este de Juan Martín Prada y un paper que se llama [El Capitalismo Afectivo](#) y que habla pues de, principalmente, o vamos como yo lo recuerdo, hace un tiempo que no lo leo, pero vamos por lo menos la idea que despierta en mí, es la confrontación de nosotros humanos con estos mamotretos tecnológicos, que nos controlan, o sea, o nos controlan o que por lo menos somos registrados en esos sistemas ¿no?

A mí por ejemplo hay una idea que me flipa un montón y es que, por ejemplo, el algoritmo de Tinder no es que tú encuentres la relación de tu vida, sino que tú pases el mayor tiempo posible en el sistema, o sea, me parece que es una, me parece súper interesante ¿no?

[00:08:01]

M: O como por ejemplo, bueno tienes luego el tema que también lo menciona Shoshana Zuboff, que dice como lo, bueno para la gente que no lo sepa, aunque ya supongo que ya lo saben, pero introduzco así mi pequeña introducción es como tú... Lo que el capitalismo de vigilancia es, todo estos sistemas que nos están vigilando constantemente en nuestras interacción. A dónde vamos, con la idea de hacer predicciones ¿no?. En el tema cuando tú te haces predicciones, hay un libro de, como se apellida, ¿Neith? Se apellida Nate que se llama [Signal and Noise](#). Y es tú cuando vas a hacer una predicción, tú tienes la señal, que es lo que te va a permitir hacer predicciones y luego tiene ruido, que es lo que tú tienes que evitar ¿no?.

Eso también va a aparecer, luego tiene está muy relacionado con el tema de la ofuscación. Y bueno, entonces es Shoshana Zuboff, habla de cómo, cómo el que nos estén constantemente vigilando, permiten que haga unas mejores predicciones de nosotros, con lo cual la publicidad va a ser cada vez más fina. A mí eso siempre me ha interesado. Porque creo que una publicidad que sea infalible quita libertad al individuo que a mí eso me flipa también. O sea, siempre es cómo, cómo la tecnología quita libertad como persona cuando no hay una comunicación directa. Pero luego lo que todavía es, a mí me parece que es todavía peor, es que. Cuando realmente estas compañías ganan dinero es cuando consiguen manipularte que cuando consiguen que tus miedos, que te vuelvas más radical que estés todo el rato en el scroll, scrolleando como un loco, viendo ¿sabes como? Tus miedos porque te pasas más horas en el sistema, con más anuncios y en teorías es como un bucle bastante chungo. ¿no?

[00:09:34]

M: Entonces es ahí cuando, también viendo trabajos de César, César también estaba muy interesado en, en ese en ese tema, eso al final siempre, siempre nos hemos influido mucho. Pero bueno, lo que me parece un proyecto que me influyó mucho y que bueno, que es el punto de partida en referente, que es en el que se tiene de cimentar que es [AdNauseam](#) de, Mushon... un nombre israelí, no me acuerdo, no tengo muy buena memoria, un tío muy majete, y también la tía de obfuscation también está en ese proyecto ¿no?. Que es un proyecto que en la web va dando clic a todo y va haciendo todo un lío, ¿no? Y a mí me parece muy bien. Pero claro, nosotros ya no usamos tanto en el esto [refiriéndose al ordenador] como los usábamos antes. Entonces Fangø, bebe perfectamente de ese, bebe de eso, bebe de una cosa que tú lo puedes instalar fácilmente. Y luego, pero tiene como dos, dos cosas nuevas, ¿no?, yo creo que son: te habla al móvil directamente, o sea, tiene una cosa que a mí me parece que es

interesante, que es, la frase con la que tú puedes definir Fangø es Fangø es un arma en defensa del capitalismo de vigilancia, y eso es lo que define el proyecto.

[00:10:42]

M: A mí por ejemplo, la peña se mosquea y me lo cambia como, es una herramienta, pero yo realmente tengo la intención de que sea un arma ¿por qué?, porque es algo que nos están atacando y que no podemos hacer nada, efectivamente tú te puedes conectar con SSA en Beirut, y a lo mejor puedes conseguir que no te trackeen, o a lo mejor puedes nunca nunca hablar por WhatsApp y que nunca te trackeen o nunca ver Instagram, pero a mí me interesa más el lanzar ideas para el público normal, para mi madre, para mi prima, para mí, o sea, para mi primo, para mi tío, para mi abuelo, o sea, vamos para mi colega.

Entonces para eso se utilizan dos cosas, una es una técnica, sabes, como esta idea, Fangø como novedad es que es un aparato que se conecta en el cargador y luego toma el control del teléfono móvil y entonces cuando el teléfono se está cargando, va lanzando aplicaciones random y va haciendo, esto, likes random e interacciones random, con la idea de que estos sistemas que nos están vigilando no sepan si es el humano el que está usando el teléfono o es la máquina quién la está utilizando. Ahí conectamos con la idea de *Signal and Noise*, o sea, nosotros somos la señal, nosotros somos lo que nosotros, todas nuestras interacciones, y luego metemos una capa de ruido, de, interacciones falsas, que vamos es lo que es la ofuscación y todo esto y los proyectos que hemos mencionado antes.

[00:12:08]

M: Y luego también, una cosa que se cuidó mucho es que tenga un aspecto muy reconocible, que sea, el proyecto sin ningún tipo de pudor, utilizar los logos de las grandes marcas, tiene como un chiste en castellano es como que es fango, que es barro, porque estás ensuciando toda tu interacción, pero sobre todo, y luego cuando se presenta en una exposición, se presenta como si fuera una tienda, como si fuera un producto que realmente te lo podrías comprar y que te podría salvar. Que por lo menos tendría que tener alguna utilidad. Eso yo lo que intento es, que igual que hay objetos preciosos que son un poco chungos, pues por ejemplo, el iPhone, el iPhone o el Pixel 8, que son como una preciosidad y que luego de repente el negocio que tiene ese teléfono no es que tú hables bien, el negocio es extraerte el mayor número de datos y el que haya unas campañas de publicidad que estén perfectamente orientadas hacia ti. ¿no?

Entonces intenta como ponerse en ese nivel, hoy en día, y utiliza para eso todo el tema render, todo el tema de fabricación. Y luego, en el punto de a quién está dirigido ese proyecto, tiene como dos visiones, tiene una visión individual, de proteger la privacidad de una persona pero luego también tiene una visión más utópicas, que es una visión global, y es por eso que es si todo el mundo usara un dispositivo de estos, el capitalismo de vigilancia no tendría razón de ser y colapsaría. Eso me mola bastante.

[00:13:32]

Para ello, ¿qué es lo que hace? Bueno pues todo el código está en el repositorio, y también el modelo 3D está todo en el repositorio y, y eso, ¿no sé si estoy hablando mucho?

Debuti, porque también voy a contar otra cosa, que es esto el artista cuando hace un proyecto de Open Source, eso es una movida.

Porque tú de repente, tú con toda tu buena intención, haces tu proyecto Open Source, diciendo mira, he venido, o sea. Soy un muerto de hambre [RÍE] , ¡tronco!, estoy aquí, y se me ha ocurrido esta idea, y estoy apasionado por esta idea, donde creo que está bien desde un punto de vista artístico, porque mezcla conceptos, que a mí me parecen interesantes y que son, no es puramente como una cosa técnica, maravillosa, sino que es, más que nada, es un experimento, es un punto de partida, Fangø no es una cosa que, o sea, tiene el aspecto pero, yo soy una artista, soy una persona.

Entonces de repente empiezas a recibir mensajes como “eh tío, o esto no me funciona” y es como de tío, te he dado el código fuente, te he dejado, ¿sabes?, hazlo, arreglarlo tú y es como un poco chungo. Entonces, claro, durante un momento, allí, como... o sea, para la gente que trabaja con un código y que lanza un proyecto de estos. Hay primero, como una especie de, pasar por el purgatorio, y dices, ostras, no consigo dar soporte a todo el mundo. Entonces tardas tiempo en entender que tú no eres una empresa, que tú te levantas por la mañana, te tomas un café con leche y no está rodeado de 20000 accionistas, sino que estás más solo que la una.

[00:14:46]

F: Es que lo has hecho solo tú.

M: ¡Claro!

F: Estás solo tú detrás del proyecto

M: ¡Claro!

F: Es que yo vi, o sea, como investigando y tal, que mucha gente te decía ¡ay! ¿dónde lo venden?

M: ¡Claro! Eso es, sí, sí, sí.

F: Decían, ¡ay! Yo quiero uno, ¿dónde lo venden? ¿no?

M: Sí, sí

F: Es como, que la gente también necesita, como el producto cerrado, porque, claro está acostumbrada al producto cerrado.

M: Claro.

F: Y ahora es como...

[00:15:07]

M: Y ahora es como, estuve, claro, ahí hay como dos cosas muy, muy, también, muy utópicas. Una es... Esto yo, el capitalismo nunca te va a solucionar los problemas del capitalismo. Entonces yo no creo que vendiendo un producto, metiéndole más, otra capita más, otro electrodoméstico más, otro dispositivo, te vaya a solucionar el problema. O sea, es mucho más un objeto como a mí, esa persona que te pregunta ¿dónde se vende esto? Por lo menos se está dando cuenta que hay una problemática. Le ha visto el uso. O sea, es ahí donde está la obra. O sea, que alguien me dé el coñazo [RÍE] que a ver, a ver que dice, esto es como claro, tío, todo el mundo dice me gustaría tener uno ¿no? Y es muy difícil salir de ese bucle, o sea, yo no he conseguido cómo.. cómo conectar, ¿sabes? cómo... a veces te paras, Que tú estás en un proceso y te ves entre media y dices no, esto es lo que yo quería hacer.

Yo he hecho esto, he lanzado esta idea y de repente viene como, ¡tío! Pero si por ejemplo, estoy en el *Xataka*, que es un blog de tecnología, me hicieron un reportaje, que no me han preguntado en la vida ni, ni nombre, ni “Hola, ¿qué tal estás?”, sabes, ya en su, en en la vida, solo una vez en la revista *Vice*? Me escribió el pibe y tuvimos, nos entrevistamos, que la primera vez que se mostró esto fue en Nueva York. Y ahí me escribió uno, y dijo: “Ah, qué interesante, no sé qué y no sé cuántos” lo escribió y tiene ahí como...

[00:16:20]

M: Pero vamos, esto es como... o sea, es lo más cutre, o sea, los primeras imágenes, es como yo en *blender* no tengo ni puta idea de cómo hacerlo como... O sea, pero ni idea ni idea y luego esto como, o sea, como cogiendo los logotipos, cargando... ¿sabes?

F: Bueno, es el encanto que tiene.

M: Sí, claro, sí, sí, pero que es muy... y luego sí que los otros no sean como... Que sean imágenes con mucha estética. O sea, sí que trabajé bastante como... Pues hay un video de 3 minutos. Y bueno... ¿Y sí? No sé, es un poco, o sea, para mí es un proyecto difícil y vamos, esto lo pongo así. Un proyecto difícil porque es un proyecto que es en el 2020, o sea el 2020 lo saco y tengo la residencia de MAB, además estoy súper contento y está la pandemia. Y afortunadamente... pero de repente me veo como en Berlín, que no conozco a nadie con un proyecto para hacerlo y es... como de jostias! ¿sabes? Que es un momento como, como en marzo y todo, ese momento que todos estamos un poco locos.

Claro, tú imagínate estar en una ciudad que no entiendes ni papa, que no sabes muy bien qué vas a hacer, ¿no? yo, porque yo ejemplo, todo este tema del arte a mí lo que me interesa es viajar y hacer cosas interesantes. No sé, cómo es, es para mí es un proyecto que durante una época... ahora, ahora lo estoy disfrutando más, pero que durante una época era como un proyecto como de... O sea, tampoco estaba yo muy. [RÍE] como que tú estás ahí y todo el mundo como “¡ay! Esto no funciona” o “esto funciona”, “esto no se qué”, y estás como... tío estoy intentando sobrevivir, hay una pandemia, vamos a morir todos, ¿cómo nadie pensaba eso, tío? Que era como de, ¿yo qué cojones hago con esto? ¡Si vamos a morir todos como chinches!

[CONTENIDO ELIMINADO]

[00:19:33]

M: Te iba a decir, porque yo también, vamos, no, es porque yo hice unas cosas como, unos cassettes pequeñitos, con todo el ADN del virus, hice una serie, que las tengo que vender, o sea, y las vendí en unos mercadillos, también, pero vamos como muy poco... a mí me flipaba también el código, en eso, ¿sabes? Porque yo, el coronavirus son cuatro Ks, son cuatro Ks tío y te follan, es impresionante, es como los... un poco así viéndolo y es un poco así. Pero sí es como una época muy difícil, y la gente ha salido como ¡uy! Súper normal. A mí no. Yo me quedé como de, ¿qué cojones hago aquí? bueno, me pagaban algo, porque era justamente una residencia de Onassis Stegi, que me iba ir, que mi plan era irme ahí a tomar el sol, y lo pasé en Berlín con un frío del carajo... pero... yo decía, ¿qué importancia tiene esto? ¿qué sentido tiene? pero... y que no pasa nada, puede ser un muy buen momento para vivir la vida... tío, y olvidarte de cosas de estas, fue una época muy chungu, muy chungu. Muy difícil.

[CONTENIDO ELIMINADO]

[00:21:02]

M: ¿No sé si tienes alguna pregunta o algo?

F: Sí, sí, quería preguntarte, ¿cómo está el proyecto ahora? ¿cómo lo has retomado? ¿en qué punto estás? En plan, qué dificultades te has encontrado, cómo ha cambiado, si ha cambiado tu visión sobre el problema o, o ¿ha ido por otro lado? El año pasado, ya con el ChatGPT todo el mundo hizo como un...

M: ¡Claro! Y ahí ya pasaron directamente a...

F: En plan, buah ¿para qué quiero tanto dato? Si luego se lo inventa...¿no?

M: ¡Claro!, esto... esto como bueno como proyecto, lo que te he contado, pues las dificultades de...

F: O sea, está vinculado a la residencia.

M: Está, vinculado... había empezado antes pero ahí fue en la residencia fue un momento que me permitió desarrollar, no sé si desarrollar, es bastante mala suerte tenerlo en el 2020, pero bueno, me permite hacer esta versión en USB, la primera versión son de enchufes y esta versión... [TOSE] Pues bueno, hice la fundita, y luego pues lo escaneé, estas cosas, es súper sencillo. O sea solo son dos cables que tienes que soldar y cuatro tornillos. Me ayudó mi hermano en modelarlo. Porque él es arquitecto, y esto es básicamente como una Raspberry Pi. Esto es una cosa que vale €1 y pones dos cables y ya está, pero también, como que también, pero luego lo metes con una fundita como si fuera algo... es como de una marca, así, cuqui ¿no?. Entonces lo fijas, ¿no? Y es un poco de lo que va.

[00:22:34]

M: El... A ver de... así que te pueda contar. Pues no, vamos, fue un año raro en el ver que se mostró así después de la residencia fue... bueno a ver se mostró en una exposición en realidad virtual que eso era como para crear tu tiro. Pero luego... luego tiene... luego... hice... la primera exposición fue en Alemania en el 21, en junio del 21. Fue la primera vez que se mostró, que se mostró en 3D. Con una estética que se cuida mucho, porque yo en el fondo, lo que hablábamos. Me interesa mucho que la gente normal, me pueda preguntar. O sea, yo, en plan, a mí es lo que más me interesa, que alguien si... porque aunque luego no exista, un poco, pero que por lo menos ahí lo que pretendo es como, vamos que por lo menos le surja la pregunta a la persona normal. Es más a la gente a la que hablo.

[00:23:30]

F: Yo hablé de ti, sin conocerte, perdón. Pero hablé de ti en un congreso en Sevilla, y lo presenté y luego la gente, lo que me decía era... como que “Fangø toma el control del teléfono” ¿no? Pues a mí me vino gente como, preocupada por eso, como “no, yo es que, yo no me fio de que este aparato esté tomando el control de mi teléfono”

M: ¡Claro, claro!

F: A lo que yo los miraba y les decía, corrígeme si lo dije mal, y te pido disculpas de antemano, pero yo lo que les decía era, a ver que está hecho con software libre y que has programado tú, o sea, no va a haber nada que tú no hayas controlado antes. Que está todo bajo...tu control, no se te va a meter un virus o algo...

M: No claro, no se te va a meter... o sea, la verdad es que a ver, o sea, es el proyecto de un artista, o sea, no, no es un producto claro, o sea, no está, no pasa las certificaciones de un producto, es mucho

más una idea ¿no?. O sea, pero por ejemplo, si... esto... por ejemplo, es completamente aleatorio. Y luego también si quieres podemos hablar sobre el tema de la de lo de la obra digital de largo recorrido. Esto, las obras digitales que hablan, por ejemplo, con Instagram, el software, se tiene que actualizar cada vez que Instagram actualiza su interfaz. Básicamente como funciona, pues tú tienes que volver a, como volver a calibrarlo, ¿no?, o sea, este aparato es medio inteligente porque ve el interfaz que tiene, y sabe donde está el like, sabe donde no está, pero claro, si cambia lo tiene que actualizar. Yo lo actualizo siempre que voy a una exposición, o sea ese es el ciclo de actualizaciones que tiene el sistema. ¿Sabes?, por ejemplo, ahora bien, vengo de estar en Utrecht. En esta exposición de aquí [señala un documento]. Y bueno, pues lo he actualizado, lo he dejado funcionando y ahora va a estar ahí. La versión, o sea, tengo una versión impresa en alta definición, que vamos está mostrándose allí, y ya pues en enero creo que vuelve, pues ya está.

[00:25:39]

M: Pues otra cosa es como mi equilibrio, que es muy importante como artista, que tú te quedas como ¡ay, Dios mío!, que tengo que dar soporte a las 32 personas que no pagado nada. Y ¡ay Dios mío!, que si no me va a decir que que vaya, qué horror, es como de ¡tío!. El mundo no es, no sé, es un poco, es un poco así. O sea, para mí es muy difícil el... O sea, me queda como mucho, mucha tensión. Decir, vamos a hacer como un producto como comercial realmente, por ejemplo, que alguna vez siguen he dicho pues ya está, podrías hacer una edición corta. A lo mejor harías, una edición de la funda ¿sabes? Solo lo que es la cosa impresa. Pero no me interesa cómo hacerme responsable.

No sé, yo también tengo como un problema con el tema del trabajo, yo siempre trabajo con el digital, donde todo te da igual lo que sea uno que sea 50 mil. Que a mí que el pasar las cosas a físico es como súper movida. Si una vez que tenía un para un catálogo. Y había que imprimir una URL, ahí es cuando me di cuenta que estaba yo un poco ¡ay! y eso para mí era una movida porque digo ¿y si cambia la URL? ¿Y si de repente decido cambiarla? Pero bueno necesitas saber cuál es tu página web. ¿Sabes? No era exactamente una página web, era todo un poco más complicado, ¿no? cómo pasarlo... ¿Sabes? Para personas que estamos acostumbrados a trabajar solo con lo digital, pasarlo a lo físico siempre es un poco contradictorio, o sea, siempre es un poco... como que no.. no estás tan... acostumbrado. Y eso, entonces, bueno, pues ese es el proyecto, son, como que se lanzan ideas que mueven.

[00:27:03]

M: Tengo, el último proyecto que tengo, que si quieres, ¿te parece bien que te lo enseñe?

F: ¡Claro!

M: Es como, es una residencia que hice en Austria pero es que yo no sé si ahora funciona, que es un, es un, pues es una página web donde tú, sí, a ver si lo puedo enseñar... sí, a ver, no, no, esto es... es una página web que, vamos, que tengo que acabar, vamos que tengo que entregarla ¿lo típico, idea de las residencias? Que se llama *Fango Cam*. *Fango Cam*. Entonces *Fango Cam*, es lo mismo que *Fango* pero juega con la imagen. O sea, la imagen es la siguiente cosa, ya nos tienen pillados por el texto, pero una cosa que mucha gente no sabe, por ejemplo, es que a nosotros nos están dando *Google Fotos*, o *Amazon Fotos*, y está demostrado, los de Google yo no sé muy bien, pero lo que es seguro es que los de Amazon entrenan sus modelos con las fotos de todo el mundo, que eso se relaciona también.

Entonces, este programa que se llama *Fango Cam*, es un programa vamos, es un programa es también, o sea, es un es como una página web donde tú te puedes loguear, yo tengo a ver [hace sonido de teclear] o

sea, son fotos, esto no sé yo debo de estar logueado con, sí bueno con Martín, ¿no? Pero bueno, tú tienes una cámara de fotos, que tú puedes hacer fotos a cosas, en la página web ¿no? ¡uy! Mira me la hago yo a mí mismo, y lo que hace es cortarla.

F: ¡Ah, mira!

M: Y es así como la sube a la nube ¿no? Entonces, tú tienes tus fotos, aquí tú ves o sea en el álbum ves como tus fotos, a ver [hace sonido de teclear], ¡ay Dios mío! por supuesto no funciona, como puede como tenía que ser.

F: Bueno, cosas del directo.

M: Pero... claro lo que tú lo que hace es que te corta todas las fotos no son reconocibles... [hace sonido de teclear]

F: Entonces, tú las ves enteras...

M: Tú las ves enteras y luego en el, en el, mira por ejemplo, esta es la foto que nosotros hemos visto pero está rota, o sea, así es como está en la nube y eso es como, como la ves tú. Entonces, esto lo que hace es partirla en cachitos, para que los sistemas de inteligencia artificial no la puedan reconocer y luego la reconstruyes y tú las y la puedes utilizar, es también otra estrategia que se utiliza mucho en la obra, tanto en *Fangø* como en *Fangø Cam* que es la parasitación de estos mecanismos ¿no? que es como, o sea, como no voy a dejar de usar fotografías, no voy a dejar de usar Google o cualquiera de estas herramientas, lo que hago es parasitarlo, ¿sabes? como, o sea, es un poco, es un poco la, la, la cosa. Entonces sí bueno esto es un poco todo.

F: ¿Y para cuándo tienes la entrega?

M: ¿Para publicarla?

F: Sí

M: Esto... para publicarla, pues yo supongo, esto, no, esto es *Fangø Cam*, *Fangø Cam*, esta aquí, mira aquí por ejemplo tengo dos perfiles, yo creo ¡ah! No mira esta es la foto que he hecho ahora. Pues mira así se ve cómo... [hace sonido de teclear], a lo mejor se monta, a lo mejor no se monta, pero vamos, en teoría funcionaba, ¡ay! Aquí parece que se monta, bueno no sé, pues es para final de año, para final de año.

F: ¿De este año?

M: De este año, sí, sí, pero vamos que está ya está todo el test, vamos, como son solo fotos para mí, porque tampoco lo he puesto... lo he puesto.

F: Son pruebas.

M: Pero, sí, sí, sí... no sé si tengo más pruebas...

[00:30:47]

F: Y... ¿conoces? porque digo, a lo mejor te conviene o ya lo conoces... *Nightshade* es de Ben Zhao, de la Universidad de Chicago.

M: No sé, ¿cómo se llama?

F: Night, night shade.

M: Pero ¿cómo se escribe? night de... cómo está *Nightshade*, no lo conozco.

F: Es que yo lo conocí la semana pasada ¿eh?

M O sea, tú estás... ahí...

F: ¿Haciendo una tesis? Sí [RÍEN]

M: *Nightshade*, con H.

F: Ah, bueno. Pon Ben Zhao, Z-H-A-O

M: ¿B?

F: B-E-N Z-H-A-O. Pero, Ben el nombre. Igual ya te aparece, que Google es muy “listo”.

M: ¡Ah! esto es lo de los venenos estos.. esto es la hostia es un proyectazo, proyectazo, proyectazo, proyectazo, proyectazo, tío es un proyectazo...

F: Bueno, es de la Universidad de Chicago, ahí hay...

M: Sí bueno pero que hay, hombre, supongo que de ahí podrá salir... pero también es esto o sea se podrá saltar muy probablemente porque los ataques a, o sea, [One Pixel Attack](#), lo llevan haciendo desde hace tiempo, que eso es que era como de los primeros, o sea yo creo que, vamos no lo sé, pero muy probablemente, pasándole un filtro te lo consigas a saltar. Pero es un proyectazo, sí, sí lo conozco este proyecto sí, sí, sí, sí superbonito, me encanta, su, me encanta, o sea, típico ojalá se me hubiera ocurrido a mí, o sea, que esos son los proyectos que más te, pero vamos, tampoco, tampoco es que todo se pueda hacer, pero que vamos.

Porque es como, de que ha juntado dos ideas y se ha hecho un proyectazo. No sé si está dentro, del este del arte, pero sí, sí claro que lo conocía, qué bonito.

[00:32:37]

M: ¡Claro! Porque ahora nos vamos a un mundo chungo, chungo lerundo y no sé si tienes algo más...

F: Sí, el... ¿cómo lo ves tú? ¿cómo seguir con el problema?

M: [RESOPLA] ¿cómo seguir con el problema? pues yo que sé, la verdad, o sea yo, es que a mí, yo qué sé, yo, yo pienso que yo soy mucho más productivo con Google Search. O sea, yo lo pienso y yo he aprendido un mogollón de cosas y yo no sé cómo lo haría... o sea, a mí lo que me tocan la moral, hombre, ellos también, o esa, un poco sabes, a ver claro, es que Google Search es el servicio, y luego el espionaje constante, es como... viene, viene después, después de la explosión del, de las puntocom, ¿no? es cuando.

F: Es como, de la capa de financiación ¿no? De cómo nos financiamos.

M: Es claro, claro, cómo unos sucumbieron, por las señales del puntocom de dónde se saca la pasta todo eso. ¿Y el futuro como lo veo? ¿el futuro cómo lo veo en general? el futuro lo veo que vamos a acabar todos con nuestro Chat GPT, que nos va decir lo guapos que somos y espero, tronco, que no se... esto ¿sabes? Nos hartemos y hablemos más entre personas, o sea, no sé, o sea, porque yo creo que

ahora, porque ahora todo el mundo piensa que es ilustrador, que todo el mundo es, no sé qué, que todo el mundo... y es como... o sea, no lo sé, pero luego tiene como cosas bonitas, porque yo por ejemplo, he hecho, el Chat GPT, y que ahora que tengo mucho trabajo y hay cosas que no tengo ni idea, entonces como que te lo explique, pues puedes tener una conversación de no sé qué y hay cosas como, pues sí, hay cosas que no tienen ni puta idea y se equivoca y otras pues supongo que se equivocará, pero como mi ignorancia también es muy grande... pero también la gente cuando habla se equivoca, o sea la peña te cuenta unas cosas que luego descubres que no es verdad, y tener a alguien, o sea, alguien, algo, que está ahí, capaz de explicarte cosas a mí lo que más me flipas y más que me escribe una carta, a mí lo que me mola es: “dime cómo yo que sé”.

Da data, de algo que no tengas ni idea, pero yo el futuro no sé cómo lo veo, pues el futuro lo veo mal lo veo en el sentido, es que es, que el futuro ¿cómo? Es que tecnológicamente, pues lo veo, que a lo mejor la gente todo el tema del buscador ya pasa de tener buscadores y que todos como, todo este churro de letras, y a lo mejor esto acaba como el rosario de la aurora, porque de repente nadie es capaz de hacer nada nuevo. No sé, esto... lo veo como un cambio que a lo mejor, los modelos ya pueden correr en dispositivos y los tengo, no sé, no sé, cómo lo veo, lo veo.. no lo sé ¿tú cómo lo ves? [RÍE]

[00:35:38]

M: A ver, que es lo más interesante es lo que hay que hablar como artista.

F: Sí, sí, sí. Pero yo creo que también, o a lo mejor, definiendo también, que, esa capa de legalidad, de que digamos la tecnología es capaz de hacer esto, pero nosotros desde el punto legal / ético no lo vamos a usar.

M: Claro, eso es por ejemplo lo que quiere hacer Europa, tío y si Europa lo hace no va tener a 20,000, o sea, por ejemplo, o sea, es que esto de una competición, es que es una putada, pero es que tú, por ejemplo, tú imagínate, pues eso, que o sea estamos aquí tú y yo, y tú dices pues yo no voy a usar Chat GPT. Y yo de repente venga a hacer papers y vengas, y subir las cartas de recomendación ¡tío! te vas a quedar atrás. O sea, es chungo eso, o sea, así porque, por ejemplo, ahora terminó otro que todavía no me lo he leído, pero el título también, tampoco es un tema que me interese mucho, que te ahora, ¡claro!, que ahora ya todas las cartas de aplicaciones a la universidad, ¡tío! Que el Chat GPT te puede hacer buena mierda, ¡claro! que antes era como, no sé qué... No sé si te ha pasado a ti, a mí, por ejemplo, otro día, me llegó, la primera carta que yo, escribí, o sea, tuve una pregunta hace un poco mosqueado, por un tema de la universidad donde doy clases y de repente recibí una carta que está, que es la primera carta, que digo esto lo ha escrito Chat GPT, me juego el cuello, tío.

O sea, porque era un tío que hablaba inglés como: “hello, how are you, very well Manuel” no sé qué, y de repente te suelta una parrafada de... y dices... y aparte sin tener ningún sentido y digo eso se va a ser la comunidad del futuro.

[00:37:16]

M: Yo creo que vamos a estar muy solos, así que espero que haya un movimiento, me gustaría mucho que hubiera un movimiento, tío, de hablar, que se valore un montón hablar con personas, que a lo mejor se insertan listas y tal maravillosas y que te digan “ten siempre la razón” por lo menos puedas confrontar ideas, a lo mejor creo que eso es una manera guay, que se aprecie eso otra vez, no sé, o sea, creo que, eso creo que el aprender y el escuchar es lo que está guay. Y eso es lo que a mí me molaría, no lo sé. Y sí, sino el mundo muy solo en su eco, en su cámara de eco, dándole la razón siempre.

Porque tú imagínate, si tu ahora en Google, buscas lo que buscas, tío, de decir “Trump es alienígena” vas a encontrar una página seguro que Trump es alienígena. Pues tú imagínate con un modelo de estos, o sea dale un poco la brasa, y todo el mundo va a estar convencido de unas cosas muy raras.

[00:38:10]

M: Y no sé, y, pero luego también hay alguna cosa que es bonita, que dicen que... es complicado, yo por ejemplo, el arte no se si hemos hablado antes lo del arte de inteligencia artificial antes, a mí no me interesa nada el Stendhal.ai y eso, o sea nada es nada, porque no me interesa nada un arte que dependa de una plataforma, ¡tío! de un tío en Idaho con su ordenador, o sea, es que no me interesa nada. No me ha interesado nunca el Chat GPT4, o sea todo ese arte, toda esa obra que era como “¡oh! voy a escribir una obra sobre los ventiladores y los ratones bien que se llevan con Chat GPT 3.” Es que si tienes que poner eso, tío, es una mierda. O sea, pero eso también pasa por la, por, por, porque tú, cuando tú, yo creo que tú, cuando ves una obra de arte tienes, de alguna manera pensar que es única o sea que esa experiencia es única. Tú estás con esa hora de arte y dices qué interesante es esto, esto es preciosos, ¿sabes? ¡ay qué bonito es!, me hace pensar, no se qué, no sé cuantos.

Pero en el momento en que te das cuenta que eso es como, la he hecho una máquina, o sea, no sé como que tú, de repente, cuando ves que eso es como, como que es una una obra automática tú ya no tienes ese *engagement*, ¿no? ese, con eso hay una vez que me pasó fue, yo fui a una vez, a una conferencia de [Mario Klingemann](#), ¿sabes quienes? Es [Cuasimondo](#), y es un tío que es de los primeros que hace esto, él lo llamaba foto, fotoneuralasis o algo así. Son los primeros, es de las primeras personas que hacen obras dentro del espacio latente, ¿sabes lo que es el espacio latente? que es como, bueno como obra generadas, fotos súper realistas de... Klingemann, de AI es como de los precursores del de lo que se llama AI art y que luego ha estado ahí con el... pues hacía estas cosas ¿no? El tío muy fino, o sea, claro, ahora esto hacerlo parece una basura pero esto hace 3 años era el copete. O sea, fíjate, desde el punto de vista de antes, como de tío, hemos llegado hasta aquí y esto es oro puro.

Pues el tío, yo fui una conferencia, y diciendo estas imágenes que son caras, las hay más bonitas o menos bonitas, pero como que parecen, la primera vez que ves una imagen, como un cuadro que dices pero esto es una preciosidad, son dos personas ¿sabes? como que lo ves y tú tienes como ¡uff! bueno, lo que te puede decir una imagen ¿no? Pues de repente cuando estaba preparando el tío sus diapositivas, pues estaba, el típico que estaba como conectado con, o sea me flipaba estas imágenes, y esta imagen me flipa, pero de repente estaba, con preparando, las, las diapositivas y estaba enchufado al beamer, ¿no? entonces, de repente se veía una carpeta de 7.000 fotos, todo lleno de imágenes, sino está, muy parecidas y estaban muy bien todas, técnicamente muy interesantes, pero a mí de repente mi cerebro dijo como “boooooom” [sonido como de desinflarse] ¿sabes? como que ya a mí, estas cosas me flipaban o sea me flipaba, o sea, me hacían qué pensar, era como de ¡hostia! esa, no sé cómo decirte, pero de repente es como se perdió la magia ¿no?

Y yo no sé si pasará algo parecido, o sea, yo, o sea yo por ejemplo estaba el otro día viendo una serie, y ya pasa, estaba viendo ahí una serie, pues que se llama *La Mesías* que es de... y hay ahí como una escena que la tía se mete, se va de pastillas y pues se mete al típico rollito de inteligencia artificial, pero ya es súper conocido, o sea mi ya no me dice nada eso, o sea, eso es como si lo desenfocas, es como el típico, la típica obra de paseo latente, tío, o sea, ¿tú sabes las obras de paseo latente? pues es tú, cuando tú, mira te las enseño ahora, es como, por ejemplo, ésta. Esta era la escena, y esto son, o sea, los... por ejemplo, *Interpolation Videos* a mí esto me flipaba, son imágenes que se van interpolando, son canales artificiales, cuadros artificiales, tú puedes poner lo que tú quieras ¿no? Por ejemplo, este es de la cara

como lo han hecho, es, meten millones de fotos en el ordenador, entonces en el ordenador te genera lo que se llama un embedding, que es cada foto, le consigues asociar unas coordenadas. Pues por ejemplo, la foto de un niño pequeño está aquí, y la foto de una monja está aquí. Entonces, si tú, entonces está en lo que se llama el espacio latente, un espacio de varias dimensiones, normalmente, bueno, cientos de dimensiones... y entonces te va haciendo, este efecto que hace es como el viaje generando la imagen, entre esos dos puntos, entonces puedes hacer como una especie de interpolación o un paso de una imagen a otra. Eso por ejemplo ahora es como obvio, pero hace unos años, claro, yo esto lo veía y decía “esto, ¡esto es impresionante!”. Nos vamos a morir ¿no?, como ¡esto es impresionante! ¿no? Pero claro, ya normalmente esto va, pierdes el interés, toda esa obra tiene ya muy poco que decir, o a mí me dice muy poco, vamos. Porque es como, como bueno, fue una época.

[00:43:12]

M: A mí por ejemplo, no sé si has visto de mi página web, yo, cuando uno se pone a hablar de su obra... pero bueno, yo por ejemplo, yo con esta cosa, la única, la única que he hecho es [esta](#), y a mí esta todavía, me mola, ¿por qué?

F: Pero es que ésta, yo pensaba tanto en ella, la semana pasada, tanto... [RIEN] es que la pensaba tanto, vamos, que no te escribía por... pero como vuelve, ¿no? la veía.

M: ¡Claro! pues esta tiene pues, esa justamente tiene como un proceso, ¿no? y es como para mí es una cosa que, que bueno que mola. Y el otro día estaba mirando, y claro, con el *Stable Diffusion* te lo hará automáticamente pero, o con cualquiera de estos ¿no? Pero claro como las banderas es una cosa censurada, que es por eso por lo que tampoco me interesa el arte en la inteligencia artificial en plataformas cerradas, ésta por ejemplo es una obra que está que está, vamos que está hecha en ese ordenador en una hora, porque a mí pasarme 20 horas no me interesa nada, ¿sabes? prefiero que quede todo hecho una mierda, pero que bueno que es lo que quieres decir, pero eso de “¡oh! no me voy a pasar aquí hasta que la bandera de España sea súper realista” y es como que eso ya lo tendrías, eso ya está superado, es mucho más lanzar ideas ¿no? vamos ¿sabes?

Anexo II: Acta charla Obfuscation is dead? Long Live Obfuscation!

Obfuscation is dead? Long Live Obfuscation! Chair: Amelia Andersdotter Speakers: Harry Halpin, Aileen Nielsen, Dan Bateyko, Yisi Liu Note taker: Mary Anne Smart (I had trouble keeping up, but I did my best! Hopefully these notes cover the main points!)

AA: Good evening everyone, we are at the top of the hour, about to begin. We can give everyone still a couple of minutes to join.

...

AA: Good evening, ladies and gentlemen. This is the last session of the day. For some of us, closing in on late hours. ... I hope you've had rewarding sessions throughout the day ... we hope to get back to more usual schedules. This is your reminder that the session will be recorded. Recordings cover presentations + conversations. If you do not wish to appear in the recording, you can send me a private message in the BB platform, and I can pause the recording while you ask your question. ... I will start the recording now.

AA: This paper session is titled: Obfuscation is dead? Long live obfuscation! ... We will hear about investments made in obfuscation technologies ... We will cover a large span of expertise from law, commerce, political governance ... I am very grateful that I am able to be here moderating. This is a big privilege for me to be able to take part. Thanks to Seda ... Mary Anne Smart is taking notes. This is how we remember notes and insights for the times ahead. As for our presenters, you should all be on video. We have:

- Yisi Liu, CTO & cofounder of Mask Network ... tool that encrypts social media messages. - Harry Halpin, cofounder of Nym technologies. Network level anonymity even in the face of powerful systems. - Dan Bateyko, master's student in law & technology at Georgetown. - Aileen Nielsen, fellow for law & tech. Author of Practical Fairness.

Comprehensive bios linked on platform. We're all very grateful that you could be here.

If you have any questions for the presentors during their initial presentations, record them and we will collect them for after.

Our first presenter is Aileen. Next is Dan. Yisi and Harry will present last. Ready to go ahead.

AN: Thank you, Amelia! ... so impressed with the organization & content of event. I'm a fellow in law and tech, background primarily in law. That probably means that I'm someone who believes in centralization probably a bit more than others at this workshop.

"Centralized obfuscation" need not be a contradiction in terms.

I'm not someone who builds technical tools. I think about how do we form regulatory proposals: digital services, AI, data protection, fairness, competition law. Compile relevant empirical and experimental data for obfuscation technologists. I'm working to compile this and make it actionable.

Thought experiment: Imagine that I started proposing decentralized solutions to air pollution. Let's stop worrying about Paris climate treaty, let's solve it ourselves. Potential solutions: face mask, personalized air purifiers, don't go outside, move to a better neighborhood with more trees / etc. All sorts of problems with this if we're thinking about long term good of the planet. No political/economic pressure on polluters. Poor people will always be worse off than the rich. Leads to bigger runaway problems.

We can apply this thinking to obfuscation. Is obfuscation a personal choice or a political act? (Doesn't have to be a binary dichotomy.) In either case, some problems to think about. If a personal choice, is it one of resignation? If a political act, is it effective?

3 concerns w/ decentralized obfuscation: - highly consolidated market structure, low rates of competition, big tech doesn't

seem to compete on privacy, obfuscation might not put the right kind of pressure (productive efficiency)

- decentralized technological self-help traditionally favors highly sophisticated actors who can exercise self-help. Solves your personal problem. (allocative efficiency)

- obfuscation for bad (negative externalities)

Wrt first problem: I don't think it's that controversial to say that decentralized obfuscation has limited utility as a form of market or political feedback. Acts of civil disobedience / economic protest -> we don't necessarily see the response we want. Likewise, people have a limited amount of endurance even for things that they care about. Turow et al. (2015) people are resigned, tired. Another problem with decentralized action -- people get tired! Tired of wearing glasses to block facial recognition, getting the right browser extensions, etc.

- Decentralized tech self-help tend to have distributive impacts ad odds w/ egalitarian and democratic underpinnings of obfuscation movement GDPR -> people who opt out of tracking tracked less, but if you don't opt out, your data becomes more valuable. Possibly concerning if people who didn't opt out were in some ways more vulnerable. Has their failure to opt out told companies even more about them. P2P example from 1990s. Cryptocurrencies: skew male, specific industries. Decentralized communities don't always lead to democratic outcomes. - Decentralized obfuscation can be used for bad as well as for good. Nothing that bad has happened yet so we sort of live with this.

Centralized obfuscation in practice. e.g. Laws that create obfuscation, environments that expand obfuscation bubble. Ex: EU rules on AI, proposed ban on use of remote biometric identification systems. Ex: bans on data sharing btwn certain US agencies. These can be seen as forms of centralized obfuscation.

Also worth mentioning... centralization / decentralization not mutually exclusive. e.g. blockchain permissioning. decentralized digital contact tracing with decentralized architecture but centralized authority. GDPR is arguably hybrid.

Concluding thoughts: when building obfuscating tools, consider these three potential downsides and how to mitigate especially distributional concerns. More empirical feedback could help. Developing more hybrid obfuscation infrastructure. Centralized obfuscation as infrastructure. e.g. good regulation.

AA: Thank you very much.

DB: Thanks. I want to echo Aileen in thanking all the organizers ... Hi, my name is Dan. Masters students. I come to obfuscation from previous position at BKC. A lot of the ideas I'm presenting today originate from conversations with developers, measurement community. Work in progress on political tradeoffs that developers must make.

Pluggable Transports and Internet Freedom: Dilemmas in 2 obfuscation protocols

big \$2 mil grant from state dept for censorship-defeating obfuscation protocols. A bit unusual. Envisioned as a resource for at risk populations for circumventing censorship. US agency for global media and others have poured \$ millions into obfuscation tech. These tools broadly help individuals help subvert gov control, undermine internet sovereignty. Obfuscation is a "trouble making" strategy.

US gov and agencies are in the business of making trouble abroad. Again, very unlike other funding. Targeting pluggable transports specifically. High level view. Kind of network infrastructure. Technical standard. Lets developers plug in diff strategies for obfuscation into browsers, social media, etc. to obfuscate web traffic. Diff types but each standardized to make it easy for developers to swap in and out. Metastrategy for escaping watchful eye. Tunnelbear, signal have pluggable transports built-in. What I aim to do in this paper is surface some of the ethical tradeoffs, drama in the design of these pluggable transports.

My first contention is that the internet freedom ideology is ... the realization of a broader strategy. Depends on American companies to work. That dependency on American companies is reflected in how the strategies are used. One example: meek obfuscates web traffic to appear to come from, say Amazon, Microsoft. I think that when we look again to this grant at the state dept, we can see how that ideology affects what's seen as worthy of funding and what's not. In 2018 notice of funding each recipient encouraged to reach out to VPNs. VPN companies don't always have good practices! Some of them are lemons. Missed opportunity to limit who gets access to these pluggable transports. Could have formed partnership with specific responsible companies. Maybe there's some necessity of centralization. Pluggable transport devs have started to require centralization. For

example, Tor project uses pluggable transport strategy that requires secret list of confidants. As a result, organization keeps close guard of list on centralized server. In order to connect people living in restricted countries, there's this choice to centralize. ... IT also relies on US companies' continued success. On occasion creates pressure for Tor project to maintain relationship with these companies. Need to surface these tradeoffs between centralization and access. Again we're seeing a way in which these protocols pose ethical challenges. Think of this kind of like a thief hiding in a crowd of people. Thief's strategy depends on police unwillingness to "burn the haystack to find the needle." But that's not always the case. e.g. russia. Devs that use mimicry PTs are taking a risk. Do they understand this ethical tradeoff? I'll end by talking about takeaways

- looking to software side of media infrastructure - academic study of these tools has been limited to CS and we can bring that out into other disciplines - contrary to its own mythology does

AA: ... Now, Harry and Yisi.

HH: I'll give a little introduction. Basically I'm Harry Halpin, CEO of Nym technologies.

AA: In the meantime, question: is refusing cookies an example of obfuscation?

AN: Sure, I take a broad view of obfuscation. As a lawyer I would say yes. That's a place where a centralized authority can support that decision, enable that obfuscation.

AA: Can network obfuscation survive without funders w/ deep pockets?

YL: In short, we provide a tool that everyone can install in their browser as an extension to encrypt their data and all the encryption/decryption done offline without interaction w/ centralized servers. As long as we're still open sourcing all the tools and users will be able to survive ...

HH: Maskbook, mask network extension that helps all users encrypt their data, encrypt their posts in ciphertext, gibberish. ... No one but maskbook users can see the content.

This is how the encryptions/decryptions work. If you say something like hello world it will be encrypted with AES key. We will post encrypted post on twitter / fb. How do we share the key to decrypt? we use decentralized db. In mask network, each person has public key. (i.e. public identity) We can use this to encrypt AES key ... in decentralized way. I guess I will finish my talking in one shot. Basically mask is using encryptions to help users to protect their data so that basically all the data that

are posted on these giant social medias are owned by these platforms they can use your data directly without even notifying you. we want to protect data from the very beginning. Encryption tools like ours also a kind of obfuscation. Just like ad blockers. Could make negative impact bc your data can no longer be processed

or learned by those big data, AI algorithms so that you will not receive the recommendations, other "benefits" in web 2.0 platforms. I guess that's the very beginning of our combat, fight against giant companies .We want to ensure that people own their data. Then we can explore more options to further use these data. I will leave the time to Harry.

HH: Sorry about hiccup. Now we know what maskbook does. Why is this important, interesting? What is obfuscation? Let's look at it technically. If you look at it technically, you have this ability to detect packets. If I'm watching the wire, I can see oh look they were accessing this etc. I can steal stuff, all kinds of terrible things. Obfuscation makes it look less intelligible. The vision is that this would prevent censorship help freedom of speech. The reality of the situation is different. People don't know how to use pub/priv keys. Focus on Tor. Focus on hiding traffic. But it's actually an arms race with ML. I can look at timing, metadata, volume. I can figure out what you're doing. I can spy on you. The problem is that when you build systems based on hard encryption, you're trying to fight really powerful adversaries. Obfuscation works better with weak adversaries. You're kind of doomed. Is it even ethical to teach people how to use these technologies, given their limitations? IT's easy to use these technologies to block Tor. Tor doesn't work in China at all. PT doesn't work in china very well. Crazy situation. What people actually do, they have sets of small servers that just use encryption. That's how they get through. Lots of people access the internet that way. Tor can't mimic that. Tor has a structural problem. Funded by centralized entity. IT's hard. We're going to take the opposite view: cryptocurrency great solution. Not censored in China. Not viewed as hostile. Used for financial speculation, etc. What happens is that cryptocurrencies provide incentive to run nodes. You can make other kinds of cryptocurrencies. This actually works. We got our software to 3000 nodes with incentives. Mask has community of thousands of users raised nearly 7 miooin. Built on top of cryptocurrency. Radically decentralizes power. People who were dependent to geopolitical goals of nation states now don't have to do tht. They can raise \$ themselves, build the tools that work in their local contexts. Not dependent on state actors. People in China know this. (Shadowsocks). End on a slightly stronger threat model. We defend your metadata. But what I really want to end on is philosophical point. Classical obfuscation (doesn't depend on hard encryption) is fine to push to other countries bc Europe doesn't have ability to fight back against NSA. Tor is fine against weaker gov, IRan for example. Doesn't work well within United States. Same with Pluggable Transport. Cryptocurrency rather as being seen as something for speculation, it can empower people. The only reason people believe in the US \$ is bc of giant US army. Maybe somehow it's for the greater good but a lot of people are no longer buying it. Cryptocurrency empowers local communities, programmers to do what they want to do for/against who knows. But it's that element of freedom which does bode well in the long term for the future of technologies and human freedom in general.

AA: Thank you for this contrarian view on feasibility of obfuscation technologies. ... Somehow optimistic... This is now the time we have left for open questions. You can ask questions or put them in the chat. If you don't want your question

recorded you can write private message. Click on my name in participant to send me a private message.

We've also prepared some questions in advance to get the conversation going. Let's return to the question: can network obfuscation survive w/out funders w/ deep pockets.

Dan you've been looking at funder w/ very deep pockets. Is there another way?

DB: Yeah I guess looking at Harry and Yisi's presentation there's clearly some ability to use other means of crowdfunding, cryptofunding. The question is wht about all the other needs that users have when subverting censorship. Localization, dev of community. Some of this is about building volunteer community. There's other ways in which funding becomes really vital. One aspect about all this .. so when we look to say these flaws in obfuscation protocols that ML can pick up and discriminate and continue to block individuals -- yeah Tor not working in China -- this is kind of the end shot Aileen was asking. IS this an achievable goal? At some point I think we will see the arms race is over and the government will have run. And I guess my question is, I'll come back to it.

HH: For 10 years, "internet freedom" essentially ran by US gov soft power. Not freedom for anyone inside the US that gov didn't agree with. They control the funding so they control the people. These people now working on content moderation which I Call censorship. Regardless what's happened with cryptocurrency, weirdly enough you can crowdsource much larger international funding than previously imaginable. That is new. Maskbook raised millions. That's kind of interesting to be honest, may be a game changer.

AA: Also a question by David in the chat. Unobservability as a design goal. Do you object to FTE approach of Tor project or something else?

HH: Tor project did great job given constraints as non profit. Same w/ efforts to fund localization. Ability to financial incentivize didn't exist when Tor kicked off. They made a reasonable compromise at the time. The times have changed in a good way. Don't have to use a nonprofit. Let local communities find out their own translation needs. They can have the financial capabilities to do that. This ay actually differ vastly across cultures an dI think that's ok. IT's a big world no longer US gov fishbowl. Anyone who talks about rule of law and wants to take it seriously, look at Trump regime. Can't take US seriously as stable rule of law.

AN: register disagreement. I think it's much more nuanced.

AA: Broader discussion should be left for after. Question for Aileen. In the creation of these centralized institutions ... you talked a lot about EU, GDPR, etc ... but isn't it also the case that European institutional makeup somehow shows that laws are not as effective as we would hope in creating the sort of empowerment that obfuscation is meant to ensure? ... EU through its regulatory strategy has consistently drawn short straw. Do we really want to continue down that path? Should EU look for inspiration in other projects rather than in regulation?

AN: I guess I have a few brief thoughts. I don't view the EU as having drawn short straw. They don't have the biggest players in their jurisdiction. But they're still making change. Not always the change they intend--it's complicated. Main message is don't give up on regulation as a route to what we want out of obfuscation. We need both. I worry when people say the government is corrupt, just give up on it. To think regulation never works is also a mistake.

AA: Any thoughts on this Dan?

DB: Users who continue to opt-in, some how their data becomes more vaulable. Struck me as an interesting dilemma. Those not obfuscating are surveilled more, value of their data increases. Obfuscating puts you in the long tail of users. The web traffic looks the same and any deviation is suspect. There's some limits here to the tactic of obfuscation becuae if you are in long tail, no matter what you're doing, the fact that you are very different from typical users is enough to be suspect. Whenit comes to web obfuscation, yes we're seeing more and more development that's breaking obfuscation tactics. But it's not distributed equally. We can see that some of the most basic ways of obfuscation are still working in many places. Arms race isn't quite the right term. IN some cases the arms race is at full force in other cases there's ways to get through w/ obfuscation tactics. Depends on

geopolitical politics, etc. Glad to see focus on EU and privacy provisions there, ways that these might be insufficient.

AA: Yisi, from perspective of running business in China, what take up do you see from civilians, consumers in Chinese market? What is the appetite in China with end consumers for preserving some kind of market privacy?

YL: Thanks for the question. I guess it's a large question. Some things I've observed from the past years. I've been back for 3-4 years (in China). I'm seeing a really progressive dev of tech in China (Alibaba, tiktok). These apps are demanding, growing rapidly, all over the world. Technology itself growing, people still not seeing privacy as a major thing to take care of in development. Privacy/security are still really really small thing to talk about in China. Talking about the environment where the community working on these tools is still a small size of people. People are being spied on by the giant platforms that have applied some discrimination. Now a lot of users are realizing their data is being abused. We need to find a way to protect our own data. Get back to ownership of our data. But still people are not really caring about this because they're receiving more benefits than the harm. Talking about the technologies, there are already some people working on the specific direction to protection people's privacy such as shadowsocks and others, but still this is a really small thing. Lot of people still controlled by GFW just like we talk about. Obfuscation has been disabled in China. Endpoint being accessed by too many people. So you cannot just have a really large endpoint that can be accessed by a lot of people. Only thing that still works is you set up small private server for you and your friends. That will still work with Tor. Large bridge accessible publicly won't work. That will be recognized easily by GFW. We're still in early stage developing these tools for people. We are actually based in Shanghai China but we are under really large risk doing these encryptions, decryptions

because China has done such things in their platforms. We're operating on twitter, fb, but we're not touching any Chinese platforms because China has restricted the usage of encryption, cryptography everywhere. Because every single packet needs to be monitored or accessed by the

government or some central authority. We can't just abide to that so we're not planning to operate in China at all. That's the circumstance we are facing right now. That's something we cannot just change maybe in the next few years. That'll be all for me.

AA: Somber note. We are formally in a break time before final plenary. One sentence you want to share w/ audience before we close?

AN: Centralization and decentralization both have appropriate usage in legal and technical systems

Dan: We need to come up w/ even better obfuscation solns that benefit vulnerable people in countries that face censorship.

Yisi: Technology itself is powerful and useful as long as we are open sourcing everything and sharing the knowledge.

AA: I would like to thank everyone including the participants. I think we have had interesting discussions. Thank you to the presentors, audience, ...