TRABAJO DE FIN DE GRADO

MIS DATOS, MIS REGLAS

Análisis comparativo de las políticas de privacidad de las aplicaciones de control de ciclo en Estados Unidos y Europa en la era post "Dobbs contra Jackson"

MARINA GÓMEZ ALCALDE

TUTOR: **Florencio Cabello Fernández-Delgado**

GRADO PUBLICIDAD Y RELACIONES PÚBLICAS

Facultad de Ciencias de la Comunicación

UNIVERSIDAD DE MÁLAGA 06/2023

Resumen

La presente investigación lleva a acabo una comparación de las políticas de privacidad de 6 de las aplicaciones de seguimiento de periodo más descargadas tanto en Estados Unidos como en la Unión Europea. A través de dicha indagación se pretende averiguar hasta dónde pueden llegar los datos que las empresas dueñas de estas aplicaciones recogen y cómo esto puedo influir en las mujeres según la legislación del país en el que viva.

Abstract

The present research carries out a comparison of the privacy policies of 6 of the most downloaded period-tracking applications both in the United States and in the European Union. The aim of this research is to find out how far the data collected by the companies that own these apps can reach and how this can influence women according to the legislation of the country in which they live.

Palabras clave

Privacidad, vigilancia digital, feminismo, libertad sexual, derechos sexuales y reproductivos, salud sexual y reproductiva, aborto, embarazo, fertilidad, menstruación, aplicaciones informáticas, control de ciclo menstrual

Índice

Introducción…….5

Justificación ……8

Marco teórico……..9

Objeto de estudio……20

Objetivos y técnicas empleadas……..23

Pregunta de investigación y metodología ……..24

Estado de la cuestión……..28

Aplicaciones de control de ciclo……..29

Leyes en materia de privacidad en EEUU y la UE……..33

Cambios legislativos en el derecho al aborto en EEUU……..50

Colisión entre legislación representativa de los derechos de las mujeres y aplicaciones invasivas de su privacidad……62

Resultados……72

Conclusiones……93

Limitaciones…….98

Prospectiva o enfoque de investigaciones futuras……99

Bibliografía…….102

Anexos…….115

Lista de siglas empleadas

RGPD: Reglamento General de Protección de Datos.

CCPA: California Consumer Privacy Act (Ley de Privacidad del Consumidor de California).

EEUU: Estados Unidos.

UE: Union Europea.

ACLU: American Civil Liberties Union (Unión Americana de Libertades Civiles).

TJUE: Tribunal de Justicia de la Unión Europea.

IDAC: Consejo Internacional de Responsabilidad Digital.

HIPPA: Health Insurance Portability and Accountability Act (Ley de Transferencia y Responsabilidad de Seguro Médico).

PII: Personally Identifiable Information (Información Personal Identificable).

OCDE: Organización para la Cooperación y el Desarrollo Económicos.

ONU: Organización de las Naciones Unidas.

NAACP:National Association for the Advancement of Colored People (Asociación Nacional para el Progreso de las Personas de Color).

VPN: Virtual Private Network (Red privada virtual).

SDK: Software Development Kit (Kit de desarrollo de software).

NOYB: None of your business (No es asunto tuyo).

EEE: Espacio Económico Europeo

Introducción

La red ha cambiado abismalmente la forma en la que nos comunicamos, la cultura, los negocios y en definitiva cada uno de los aspectos de nuestras vidas. Además hoy día es común y forma parte de la cotidianidad que muchas empresas hagan un mal uso de nuestra privacidad. Para poder descubrir esta realidad se ha decidido estudiar en profundidad qué datos y con qué fines recogen algunas aplicaciones de control de ciclo disponibles en la actualidad.

Antes de comenzar me gustaría marcar la siguiente premisa: para Peirano (2019), "la vigilancia es un problema colectivo, como el cambio climático", y lo mismo vale decir para "la privacidad" .

Como ya expuso Zuboff (2020) profesora emérita de Harvard Business School, cada uno de nuestros gestos cotidianos dentro de la red, por insignificantes que nos parezcan, generan un rastro de datos: "nuestro trayecto diario al trabajo en Google Maps, la cafetería donde paramos a desayunar, un estado de Facebook con palabras que denotan tristeza y el tono de voz con el que le pedimos a Alexa que ponga una canción, los hoteles que estamos mirando para las vacaciones de verano y la última serie a la que te has enganchado en Netflix (…) Este sinfín de información, íntima e inconexa, revela más de lo que creemos sobre nosotros y por lo tanto tiene un valor que desconocemos" .

El presente Trabajo de Fin de Grado aborda una revisión de la literatura existente y un análisis exploratorio de las diferentes políticas de privacidad de las aplicaciones de seguimiento menstrual escogidas.

Lo que se busca es ver cómo interactúan entre sí cuatro conceptos que según Lessig (2009) son reguladores de la web: ley, arquitectura, normas y mercado. De cada uno de ellos me ocuparé más detenidamente a lo largo de la investigación ya que están estrechamente relacionados con el tema que tratar.

Asimismo las principales coordenadas de la investigación se encuentran relacionadas por un lado con el feminismo, que trata de luchar contra ese afán por controlar el cuerpo de la mujer, y por otro, con la vigilancia indiscriminada o el "capitalismo de vigilancia".

A lo largo de su libro la escritora feminista Silvia Federici (2022) hace alusión al cuerpo y a su relación con lo económico. Para la gran pensadora "el capitalismo ha transformado nuestros cuerpos en fuerza de trabajo" .

Según la activista el control del cuerpo de la mujer nunca ha sido un problema puramente cuantitativo, pues el Estado y el capital siempre han intentado determinar quién tiene permitido reproducirse y quién no (*idem*).

Shoshana Zuboff (1951), en su libro *"La era del capitalismo de vigilancia"* explica que este actúa "por medio de unas asimetrías de conocimiento sin precedentes, y del poder que se acumula con ese conocimiento". Y es que según la autora de Harvard los capitalistas de la vigilancia son capaces de saber todo sobre nosotros, pero sus actividades están diseñadas con el fin de que nos resulten lo más ajenas posibles. "Acumulan montañas ingentes de nuevos conocimientos extraídos de nosotros, pero no para nosotros. Predicen nuestros futuros para el beneficio de otros, no para el nuestro".

Ella cree que donde muchos solo ven una intrusión relativamente inofensiva, existe "una amenaza antidemocrática a valores esenciales como la soberanía personal y la autonomía"(*idem*).

Para Zuboff nos encontramos en un momento en el que "estamos volviendo a una especie de patrón feudal de asimetrías extremas de conocimiento y poder que crean un nuevo eje de desigualdad social". La autora llama a esta desigualdad social: desigualdad epistémica, (desigualdad del derecho a saber). "Se ejemplifica en este abismo creciente entre lo que sabemos y lo que se puede saber de nosotros" (*idem*).

La autora piensa que si nos pidieran todos los datos, no querríamos darlos, así que la única forma de mantener sus cadenas de suministro por parte de ciertas empresas es a través de lo que es esencialmente una operación de vigilancia. "Sin vigilancia, la creación de valor que acompaña a esta lógica económica no sería posible" (*idem*).

Por otro lado también se encuentra 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" (Ibid (2020) citado en Cabello y Solera, 2020).

Esta forma de actuación en la que podríamos decir que “los jugadores no conocen las reglas del juego” es llamado por algunos autores, 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” (Ibid (2020) citado en Cabello y Solera, 2020).

Por otro lado en el panorama europeo la preocupación por dichos asuntos ha sido confrontada con la gran promesa de privacidad: el RGPD (Reglamento General de Protección de Datos). Esta es la nueva normativa que regula la protección de los datos de los ciudadanos que viven en dicho territorio. Entró en vigor el 24 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018. Su relevancia recae en que se trata de la primera norma sobre esta materia que afecta a todos los países de la Unión Europea y unifica, por tanto, tanto los derechos como las obligaciones.

Además éste se convierte en uno de los reglamentos más duros a día de hoy relacionados con dicha materia. Asimismo las sanciones previstas por RGPD han sido uno de los temas más polémicos y controvertidos (Diario Oficial de la Unión Europea, 2016).

El principal motivo por el que surge el ánimo de esta investigación podría relacionarse con la siguiente situación: en EEUU, las redes sociales y las asociaciones se han movilizado para animar a las mujeres estadounidenses a desinstalar sus aplicaciones de seguimiento menstrual. Los medios de comunicación han difundido informes alarmantes que demuestran la facilidad con la que los datos personales gestionados por Apple y Google pueden utilizar para localizar a personas que buscan información sobre el aborto. Con la derogación del derecho constitucional al aborto, más de la mitad de los estados de EEUU están prohibiéndolo, lo que obliga a las mujeres a recorrer largas distancias para acceder a un centro abortista que sea seguro y legal (Vidal y Merchant, 2022).

El 24 de junio de 2022 la situación en cuanto al aborto en los Estados Unidos cambió totalmente. Fue tras el caso Dobbs contra Jackson Women's Health Organization cuando la Corte Suprema sostuvo que la Constitución de los Estados Unidos no contempla ningún derecho al aborto, anulando así casos anteriores como el de Roe contra Wade (1973) y Planned Parenthood contra Casey (1992), de los que se hablará a lo largo de la investigación.

El problema que trata el estudio es el siguiente: hoy en día nos encontramos con un conflicto en cuanto a la gestión de los datos. En la medida en la que se hace uso de ciertas aplicaciones generamos de alguna forma información que parece ser de gran valor. Además existe una tendencia desencadena y compulsiva por convertir el cuerpo en dato, o lo que es igual, por dar un valor monetario, a lo que segregamos diariamente, lo que está provocando un problema ético y moral en nuestra sociedad.

Esto se encuentra estrechamente relacionado con la legislación de cada país pues según este apruebe unas leyes u otras la protección de los ciudadanos y ciudadanas puede verse agravada o sostenida. Además, que el estado posea la potestad para hacer uso de determinados datos puede crear diversas brechas para las que aún apenas existe fondo legal.

Este Trabajo de Fin de Grado pretende poner sobre la mesa diferentes casos que quizás sitúen a la ciudadanía frente al problema de la vigilancia indiscriminada, como una grave violación de los derechos fundamentales. Además se quiere sacar poner en el punto de mira ese peligro, muchas veces implícito, que conlleva la generación de ciertos datos ya que algo, en principio digital, puede dar con tus huesos en la cárcel.

Antes de entrar de lleno en la investigación, comentar que el trabajo constará de varias partes entre ellas una breve exposición de los antecedentes que constituyen la sentencia "Dobs contra Jackson" en EEUU y un recopilatorio de la evolución de las leyes en materia de privacidad en UE y en EEUU. Asimismo se incluirán algunos casos reales que han pasado a manos de la justicia, muchos de ellos objeto de discordia por causar discrepancias territoriales. Tras contextualizar se pasará a exponer los resultados y conclusiones obtenidas gracias al profundo análisis llevado a cabo.

Justificación

Considero que el tema seleccionado es muy actual y que quizás pueda servir como ejemplo paradigmático de una política general y afianzada. Además ejemplifica una de las muchas formas de coacción hacia las mujeres, en este caso, mediante la violencia de género institucional.

Dicho término hace alusión a la responsabilidad que tiene el Estado y sus agentes en la prevención, sanción y erradicación de dichas violencias contras las mujeres (Bodelón, 2014).

En el ámbito europeo esta dimensión institucional de la violencia contra las mujeres y la obligación de los Estados de indemnizar a las mujeres que la han sufrido ha sido recogida a través del Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica. Especialmente en sus artículos 5 y 30. [1]

Este TFG apela a la gravedad de la vigilancia digital masiva e indiscriminada y advierte ante el peligro de su insercción en la lucha feminista por los derechos sexuales y reproductivos, además en un contexto internacional, que parte de EEUU pero podría tener repercusiones mundiales.

Me gustaría que la investigación sirviera para sensibilizar sobre cómo los datos son extraídos de nuestro cuerpo sin apenas percibirlo e intentar que las mujeres perciban este asunto latente, obteniendo sus propias reflexiones y actuando al respecto.

Ver cómo el uso de la tecnología puede desembocar en delatar a mujeres embarazadas o gestantes es algo que nos hace replantearnos hacia donde nos lleva este mal uso de nuestra privacidad. La amenaza de cárcel y los cargos penales enfocados en la mujer por no ejercer "su misión natural" pueden hacernos ver la magnitud del conflicto.

Es por esto que considero importante la función de investigaciones como esta, cuyo objetivo es ordenar la información y fundamentarse en las más recientes noticias y estudios para así poder ayudar, en cierto modo, a transformar la realidad en la que vivimos.

Marco teórico

Quizás sea un clásico, pero recurrir a Orwell y a su obra -*"1984"*- me parece de los más oportuno para introducir este amplio apartado. Como explica Lessig (2009) en *"El Código 2.0"* explica, resulta interesante apuntar a la ineficacia de las tecnologías orwellianas, con respecto a la gama actual de tecnologías. Y es que en ese mundo el

1. Council of Europe Treaty series. https://rm.coe.int/1680462543

dispositivo de vigilancia fundamental era una simple pantalla de televisión que emitía contenidos a la vez que controlaba la conducta de quienes se hallaban al otro lado. La gran ventaja de la pantalla de televisión era que todos conocían, en principio, lo que ésta podía ver. Así, el protagonista sabía dónde esconderse ya que todos podían conocer la posición de la pantalla. Por lo tanto era sencillo saber dónde hacer aquello que uno no quería que ésta viese. "Por desgracia ese no es el mundo en que vivimos hoy" (*idem*).

Es complicado saber cuánto de lo que hacemos en Internet está siendo controlado; tampoco si una cámara está intentando identificar quiénes somos. "Las tecnologías de hoy no tienen nada de la integridad de las de *"1984"*. Ninguna tecnología actual es lo bastante decente como para avisarnos cuando nuestra vida está siendo grabada" (*idem*).

Existe, según Lessig (2009) una segunda diferencia entre el mundo de "*1984"* y el actual. Así según el catedrático de Harvard el gran "fallo" del diseño de *"1984"* radicaba en el control de la conducta, pues al no existir ordenadores en ese mundo ,el control era ejercido por una cuadrilla de guardias que observaba varios monitores de televisión. Un guardia era capaz de observar que alguien estaba hablando con quien no debía, o que había entrado en una parte de la ciudad prohibida pero ningún guardia disponía individualmente de una panorámica completa de la vida de ninguno de los personajes. Hoy en día esa "imperfección" puede quedar eliminada. "Ni el propio Orwell pudo imaginar algo así(...)" (*idem*).

"Así, nuestra vida se convierte en un registro perpetuo, donde nuestras acciones quedan almacenadas para siempre, disponibles para ser reveladas en cualquier momento y, por consiguiente, susceptibles de ser puestas en tela de juicio" (*idem*).

Matterlart y Vitalis (2015) en su libro *"De Orwell al cibercontrol"* mencionan que la historia, y especialmente la europea, es testigo de los peligros de los ficheros de personas. Los autores ponen como ejemplo las fichas realizadas a los judíos durante la Segunda Guerra Mundial y mencionan que estas demuestran como "una ficha" puede conducir directamente a la muerte.

Más adelante los autores se posicionan en el momento de la historia en el que gracias al ordenador aparecen proyectos de ficheros automatizados y de bases de datos sobre las personas. "En todos los países que se informatizan, se toma conciencia de que una máquina capaz de registrar todo, sin ignorar nada, puede atentar contra la privacidad del

individuo y hacer de éste un ser transparente, fácilmente manipulable por los poderes vigentes" (*idem*).

Ambos autores coinciden en que no se trata tanto de dar valor a los pequeños secretos de la persona, sino en proteger una esfera de autonomía ciudadana.

Pongamos como ejemplo la época de la COVID-19, los ciudadanos y ciudadanas comenzamos a llevar mascarilla, no solo para protegernos a nosotros mismos sino para proteger a los demás y así poder crear una atmósfera limpia y libre de virus.

Desde 1973, el Consejo de Europa ha adoptado resoluciones sobre los ficheros informatizados de los sectores público y privado sobre las que se han basado la mayoría de las legislaciones europeas y que, posteriormente, han sido consideradas y precisadas por la OCDE (Organización para la Cooperación y el Desarrollo Económicos) y la ONU (Organización de Naciones Unidas). El texto de estas resoluciones enuncia un cierto número de principios básicos: el principio de la lealtad de la recogida de informaciones, el principio de finalidad, el principio de acceso individual a sus propios datos, y el principio de seguridad (*idem*).

Snowden (2019) en su libro *"Vigilancia permanente"* habla también de la problemática del censo y menciona que tanto en la Alemania nazi como en la Rusia soviética, los primeros indicios públicos de esa vigilancia tomaron la forma superficialmente inofensiva de un censo, lo que se consideraba la enumeración oficial y el registro estadístico de una población.

El primer censo íntegro de la Unión Soviética, en 1926, tenía unas segundas intenciones más allá del simple recuento ya que preguntaba abiertamente a los ciudadanos soviéticos por su nacionalidad. Los resultados parecieron convencer a los rusos étnicos que conformaban la élite soviética de que estaban en minoría en comparación con el resto de ciudadanos que afirmaban tener ascendencia de Asia central (uzbecos, kazajos, tayikos, turcomanos, georgianos y armenios). 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" (*idem*).

Asimismo el autor comenta en su libro que la vigilancia masiva es en nuestros días un censo infinito. Snowden (2019) comparte su preocupación al mencionar que hoy en día

todos nuestros dispositivos, desde nuestros teléfonos a los ordenadores, son básicamente "censadores" en miniatura los cuales nos acompañan en todo momento, "censadores que recuerdan todo y que no olvidan nada" afirma el experto. "Una vez que la ubicuidad de la recopilación se combinó con la permanencia del almacenamiento, lo único que tenía que hacer un gobierno era seleccionar a una persona o un grupo de personas como cabezas de turco y buscar —igual que yo había buscado entre los archivos de la agencia — pruebas de un delito adecuado" (*idem*).

Por otro lado, la conocida activista feminista, Silvia Federeci (2022) en su libro *"Ir más allá de la piel"* cuenta que a lo largo de la historia de Estados Unidos no se ha obligado directamente a ningún colectivo de mujeres a tener hijos (a excepción de las esclavas). Sin embargo la procreación involuntaria y el control estatal del cuerpo femenino parecen haberse institucionalizado a través de la criminalización del aborto. La pensadora feminista cree que la procreación tiene un valor económico que no se ha reducido lo más mínimo aunque el capital haya aumentado su poder tecnológico.

La activista sostiene que es un pensamiento erróneo suponer que el interés de la clase capitalista por controlar la capacidad reproductiva de las mujeres está disminuyendo gracias a su capacidad de sustituir a los trabajadores por máquinas. Pues, a pesar de la tendencia de hacer innecesarios a los trabajadores y de crear lo que ella llama "poblaciones excedentes", la acumulación de capital sigue necesitando trabajo humano. "Solo la mano de obra crea valor, no las máquinas" (*idem*).

Por su parte la escritora y periodista Marta Peirano (2022), menciona que Europa mantiene una posición delicada en la configuración del nuevo paradigma digital global. Por un lado, según la autora, esta lidera la creación de marcos regulatorios capaces de imponer valores democráticos que garanticen un entorno digital más seguro y más justo. Por el otro, sin embargo, carece de una industria propia capaz de competir con los grandes bloques antagónicos de China y EEUU, y delega el desarrollo de las grandes infraestructuras digitales a las plataformas tecnológicas que amenazan su soberanía.

La posición europea es cada vez más frágil con respecto a las dos grandes potencias que se disputan el siglo XXI, EEUU y China. Estas imponen dos modelos de gobernanza aparentemente antagonistas desde la perspectiva política, pero no muy diferentes en lo que se refiere a ambición extraterritorial. Según la periodista ambos países poseen una gran ambición por obtener un mayor control de las grandes infraestructuras de

telecomunicaciones a nivel planetario, incluyendo el acceso, gestión y explotación de los datos que derivan de su funcionamiento. En ese marco geoestratégico, es imprescindible que Europa afiance sus alianzas sin dejar de reforzar su autonomía. También es importante que proteja sus estándares para poder garantizar la protección de los derechos e intereses de los ciudadanos europeos, incluyendo el acceso, comprensión y optimización de las infraestructuras críticas de nuestro tiempo (*idem*).

Para Peirano (2022), Internet, técnicamente, sigue siendo una red de máquinas interconectadas y regidas por los protocolos TCP/IP que garantizan el tráfico libre, atomizado y distribuido, de paquetes de información. Para la autora en la práctica, la mayor parte del tráfico es gestionado de forma opaca, monopolista y extractiva por un pequeño puñado de empresas. Hablamos de las multinacionales estadounidenses que han hecho fortuna con el modelo de negocio que ahora llamamos "capitalismo de datos" y "han facilitado el aparato de vigilancia masiva de las agencias de espionaje del gobierno de EEUU y de sus partners internacionales en la Alianza de los Cinco Ojos (FVEY), como revelaron las declaraciones y documentación aportadas por Edward Snowden en 2013" añade la periodista.

Cynthia Conti-Cook (2020) , abogada especializada en derechos civiles e investigadora del campo de tecnología en la Fundación Ford, realizó un trabajo de investigación sobre los procedimientos legales interpuestos en contra de personas embarazadas acusadas de feticidio o de poner en riesgo la vida del feto, y presentó una clasificación de las pruebas digitales utilizadas en contra de los acusados en un artículo académico titulado *"Surveilling the Digital Abortion Diary".* Aquí la autora cuenta una serie de sucesos que ilustran como ya se han usado los datos para criminalizar a las personas .

Uno de los casos que resaltó fue el de Latice Fisher, una mujer de Misisipi, la cual, fue acusada de asesinato en segundo grado tras dar a luz a una criatura muerta en su casa en 2017. Según noticias locales, los investigadores encargados del caso descargaron el contenido de su teléfono (incluido el historial de búsquedas en Internet) , y la acusada admitió "haber realizado búsquedas en internet sobre cómo inducir un aborto espontáneo" (*idem*) e información sobre "cómo comprar en línea medicamentos para interrumpir el embarazo, como mifepristona y misoprostol". En vista de que el caso en contra de Fisher generó gran atención pública, los fiscales finalmente desistieron. (*idem*).

Otra caso fue el de, Purvi Patel, condenada a veinte años de prisión por "abandono de una persona dependiente y feticidio" tras tomar píldoras abortivas que compró por Internet. Las pruebas presentadas contra ella en el juicio fueron las siguientes: la investigación en línea que realizó, el correo electrónico de confirmación que recibió de *internationaldrugmart.com*, y mensajes de texto no cifrados a una amiga sobre las píldoras que compró. La condena de Patel por feticidio fue anulada aunque si fue condenada por "abandono de una persona dependiente" y pasó más de tres años detenida. Como se puede observar con este caso las pruebas digitales llenan un vacío para los fiscales que desean procesar a las mujeres por los resultados de su embarazo (*idem*).

> "Esos mensajes de texto, esos sitios web visitados, esas búsquedas en Google son el tipo exacto de prueba de intencionalidad que los fiscales quieren para reunir evidencia". (*idem*).

Esos entre muchos otros son los casos que expone en su artículo la autora Cynthia Conti-Cook.

Cuando en 2018 *The New York Times i*nvestigó los datos supuestamente anonimizados que hay a la venta, logró identificar a una mujer que había pasado una hora en una clínica de salud reproductiva Planned Parenthood en Newark. En mayo, un periodista de *Vice* logró comprar por solo 160 dólares información de un vendedor de datos sobre los teléfonos que habían estado a lo largo de una semana en Planned Parenthoods (tras el informe de *Vice*, el vendedor de datos dijo que planeaba dejar de vender datos sobre las visitas a proveedores de salud) (Hill, 2022).

Por su parte, Lessig cuenta cómo a comienzos de 2006, el Chicago Sun-Times informó de que existían sitios web que vendían los registros telefónicos de llamadas realizadas desde teléfonos móviles. Un blog llamado AmericaBlog quiso constatar los hechos adquiriendo el registro telefónico del mismísimo General Wesley Clark. Por unos 120 dólares, el blog logró demostrar lo que la mayoría de la gente consideraba imposible: que cualquiera que pudiera pagarlo podría encontrar algo tan personal como la lista de personas a las que alguien llama desde un móvil (así como la frecuencia y la duración de dichas llamadas) (Lessig, 2009).

Otro dato interesante que menciona el artículo *"Surveilling the Digital Abortion Diary"* es que, en el pasado, los activistas antiaborto crearon *geocercas* o barreras digitales alrededor de las clínicas Planned Parenthood y enviaban a los teléfonos que ingresaban a esa zona avisos que dirigían a sus dueñas a una página web que buscaba disuadir a las mujeres que pretendían terminar con sus embarazos. En el ámbito penal, los fiscales han intentado utilizar esta tecnología para identificar a un sospechoso de atraco a un banco mediante una orden de registro a Google para así poder obtener información sobre todas las personas que, según los servicios de localización, estaban en el banco en el momento del atraco (Conti-Cook , 2020).

Debido a que hay muchas formas de monitorizar digitalmente el movimiento, la comunicación y las búsquedas de Internet de las personas, la gran duda es con cuánto ahinco actuarán las agencias de la ley en los estados que prohíben el aborto. Quienes aconsejan no emplear rastreadores de periodo parecen temerse lo peor: "búsquedas amplias que incluyan a cualquiera que haya estado gestando y luego ya no" (*idem*).

Otro caso relacionado con Planned Parenthood fue el denunciado por la revista Vice ya que tras una investigación concluyó que el broker de datos SafeGraph estaba vendiendo datos en tiempo real de ubicación de personas (Peirano, 2022).

Según la periodista, actualmente Affinity Answers, el data partner del gigante Oracle, ofrece listas de personas asociadas a Planned Parenthood y también a la Asociación Nacional para el Progreso de las Personas de Color (NAACP), la Unión Americana de Libertades Civiles (ACLU) o el Grupo Nacional de Trabajo para la defensa de Gays y Lesbianas (Peirano, 2022).

La autora se pone en situación y se replantea que pasaría si en vez de "Roe contra Wade" hubiera sido el caso Lawrence contra Texas, por el que la Corte Suprema de los Estados Unidos declaró inconstitucionales las leyes que criminalizan la homosexualidad, en junio de 2003 (*idem*).

En caso de que esto ocurriera las aplicaciones como Grindr o Tinder convertirían inmediatamente a sus usuarios en el objetivo de la vigilancia de vecinos, familiares, profesores y colegas (*idem*).

"Es difícil decir qué pasará dónde y cómo y cuándo, pero las posibilidades son bastante peligrosas", afirmó Conti-Cook (2020). "Es muy fácil abrumarse por todas las

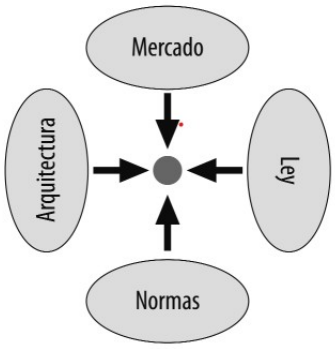
posibilidades, por lo que intento insistir en concentrarnos en lo que ya hemos visto que se usa en contra de las personas" (*idem*).

Lessig (2009) identifica dos amenazas distintas que Internet crea a los principios de privacidad: la primera es la amenaza de la "vigilancia digital". Desde el acceso a Internet hasta un simple paseo por la calle, pasando por el correo electrónico y las llamadas de teléfono, la tecnología digital está brindando la oportunidad de llevar a cabo registros cada vez más perfectos. La segunda amenaza proviene del creciente acopio de datos por parte de entidades privadas (entre otras), en la opinión del autor, no tanto para "espiar" sino para facilitar el comercio (*idem*).

Ante estos dos riesgos diferentes, Lessig (2009) propone cuatro tipos de respuesta:

> 1. Ley: La regulación legal podría diseñarse para responder a estas amenazas. La ley podría, por ejemplo, ordenar al Presidente de EEUU que no vigilase a los ciudadanos sin contar con sospechas razonables o podría prohibir la venta de datos recopilados de clientes sin su consentimiento expreso.
>
> 2. Normas: podrían usarse para responder a estas amenazas. Así, por ejemplo, las normas entre entidades comerciales podrían contribuir a construir confianza en torno a ciertas prácticas protectoras de la privacidad.
>
> 3. Mercados: el mercado podría usarse para proteger la privacidad de los individuos.
>
> 4. Arquitectura/Código: tecnología podría usarse igualmente para proteger la privacidad. A menudo nos referimos a estas herramientas como «tecnologías de aumento de la privacidad» (PET, acrónimo de Privacy Enhancing Technologies), tecnologías diseñadas para proporcionar al usuario un mayor control técnico sobre los datos asociados a él o ella.

Para el célebre académico toda solución requiere una combinación de al menos dos modalidades. Una propuesta del autor es que la arquitectura debería permitir las negociaciones sobre privacidad entre máquinas, de modo que los individuos puedan dar instrucciones a sus máquinas acerca del grado de privacidad que desean proteger.



Fuente: Lessig, 2009

Asimismo es interesante descubrir desde qué perspectivas se ha abordado el tema de estudio. Por ejemplo la investigación en 2019, la ONG con sede en Reino Unido Privacy International, hizo público un estudio en el que indicaba cómo varias de las *apps* más populares encargadas de registrar el periodo menstrual compartían los datos de sus usuarias a Facebook y a otras empresas. Según concluyó la investigación , las aplicaciones dirigidas a los usuarios de la UE deben cumplir, entre otras cosas, las estrictas obligaciones de consentimiento y transparencia en relación con el tratamiento de los datos personales, "pero a menudo no lo hacen".

La investigación de esta ONG reveló que Maya, Mia, Calendario Menstrual, Calculadora de ovulación, Mi calendario y Mi Period Tracker informan a Facebook de las acciones que va tomando la usuaria desde el mismo momento que abre la aplicación. Este paso ya revela información muy preciada para sus perfiles como consumidoras: "Que probablemente eres una mujer, probablemente menstruando, posiblemente tratando de tener (o tratando de evitar tener) un bebé", detalla la ONG.

En *"Periods as powerful data: User understandings of menstrual app data and information"* de Hohmann-Marriott (2021) se cuestiona el nivel de auto vigilancia que sería adecuada para un usuario o usuaria y cita a varios autores para intentar llegar a una conclusión.

En las democracias capitalistas neoliberales, como Nueva Zelanda, Estados Unidos y Europa, se espera que cada individuo ejerza su ciudadanía asumiendo la responsabilidad individual de su vida, incluida la responsabilidad de gestionar sus cuerpos (Turner, 2001, citado en Hohmann-Marriott, 2021). El filósofo francés Michel Foucault, revela que "la gestión individual de los cuerpos incluye vigilar el cuerpo y, a continuación,

disciplinar y controlar esos cuerpos vigilados" (Foucault, 1977, citado en Hohmann-Marriott, 2021).

Siguiendo la línea de los estudio comentados anteriormente Siamka y Biasin (2021) en su estudio *"Bleeding data: the case of fertility and menstruation tracking apps"* se centran en el valor económico de la actividad de muchas usuarias. La mayoría de veces estos datos generados se convierten en recursos que benefician a las empresas, las cuales los procesan junto con sus socios comerciales.

A medida que las usuarias de estas *apps* se convierten en participantes activas en el proceso de producción, la delimitación entre quién produce, consume y se beneficia de sus datos se desvanece y estos se convierten en "prosumidores" (*idem*).

Asimismo este conflicto se ha tratado desde otras perspectivas muy diferentes y que no tienen que ver tanto con la ética de los datos sino con la fiabilidad de las *apps* para predecir los ciclos de ovulación de una mujer. Este es el caso del estudio *"Use of menstruation and fertility app trackers: a scoping review of the evidence"* el cual ofrece una visión general de la bibliografía sobre aplicaciones sanitarias móviles que hacen un seguimiento de la fertilidad. Aquí se cuestiona la precisión de estas *apps* a la hora de predecir la ovulación y pone en duda la fiabilidad médica que estas pueden tener. Además pone sobre la mesa el problema de que muchas mujeres sustituyan métodos anticonceptivos por el uso de aplicaciones de este tipo (Earle *et al.,* 2020).

En este sentido también se encuentra el artículo de Hohmann-Marriott y Starling (2022) que revela que muchas usuarias confirman aplicar la información individualizada dada por la *app* para comprender mejor su propia menstruación. Aunque estas afirmaron no estar en situación de querer concebir, valoran y tienen en cuenta la información proporcionada por la *app*. Sin embargo se quiere tener en cuenta que malinterpretar información del sistema y aplicar erróneamente las predicciones sin conocimientos reproductivos quizás pueda suponer un problema. Además se plantea el problema que surge de que la única fuente de conocimiento sobre ciclos reproductivos y prevención de embarazos sean estas *apps*, privándose las mismas usuarias de buscar fuera otro tipo de información.

Por otro lado *"Menstrual Tracking Mobile App Review by Consumers and Health Care Providers: Quality Evaluations Study"* estudia 34 aplicaciones con el fin de evaluar su

calidad y fiabilidad desde el punto de vista médico. Sus autores creen que las evaluaciones de calidad de los profesionales sanitarios pueden contribuir al desarrollo de aplicaciones. En el estudio opiniones de consumidoras y de profesionales se obtienen mediante escalas de medida válidas y es cierto que estas llegan a confrontar en algunos casos (Ko *et al*., 2023).

El Consejo Internacional de Responsabilidad Digital (IDAC), por su parte, descubrió en 2021 que varias *apps* de menstruación compartían datos sin encriptar y enviaban información a terceros sin comunicarlo a sus usuarios en sus políticas de privacidad, es cierto que tras la revisión de algunas de las políticas se puede observar como esta información ya sí se da en muchos de los casos.

Asimismo el problema no solo reside en las *apps* como se ha podido observar, pues toda nuestra huella digital puede quedar registrada sea del tipo que sea. Por ejemplo en enero de 2009, el Departamento de Justicia inició un estudio sobre pornografía en la Red y quería información sobre la frecuencia y la forma en que la gente la buscaba en Internet, por lo tanto le pidió a Google que le proporcionase un millón de búsquedas aleatorias de su base de datos a lo largo de un periodo concreto.

En esta ocasión el gobierno estadounidense lo pidió. No se discute que el gobierno pida a quienes poseen pruebas relevantes que las proporcionen para una investigación abierta de índole civil o criminal. El problema que ilustra el ejemplo es el siguiente: antes de que surgieran los motores de búsqueda, nadie poseía registros de la curiosidad; no había ninguna lista de las preguntas que pasaban por la mente de la gente.

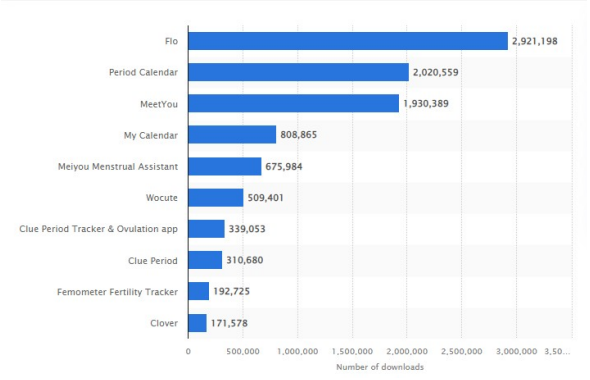
A diferencia de hoy, pues la gente inunda obsesivamente los motores de búsqueda con preguntas sobre cualquier cosa. La mayoría suelen ser inofensivas pero algunas pueden ser inquietantes como "fotografías eróticas y niños". Lessig (2009) por su parte cree que el interés del gobierno en "esta lista" aumentará con el tiempo. "Finalmente cuando las demandas no sean tan inocuas, ni los crímenes a las que se vinculen tan perniciosos, simplemente se insistirá en que se trata de un modo eficaz de hacer cumplir la ley" (Lessig, 2009).

Objeto de Estudio

Dentro de este trabajo se han estudiado un total de 6 *apps*: Mi calendario menstrual, desarrollada por Simple Design Ltd, Flo; por Flo Health Inc, Clue; por BioWink, Meet You; por Meet you-Period tracker, Calendario Menstrual; por Simpleinnovation y Alerta Periodo; por GP Internacional LLC.

La elección de dichas *apps* se ha realizado mediante el siguiente criterio: estas son 6 de las aplicaciones más descargadas y mejor puntuadas en plataformas como Google Play y App Store tanto en Europa como en Estados Unidos. Además estas aparecen en *rankings* o simplemente mencionadas en medios españoles como: Psicología y mente, Dexeus, Con Salud, La Vanguardia, La Lista o El salto. En cuanto a medios estadounidenses algunas de ellas aparecen en periódicos como el *The New York Times* o *Buffalo News* o revistas como *Wired*.

Asimismo Statista, el 27 de enero de 2023, publicó una gráfica que muestra las *apps* de salud femenina más descargadas en todo el mundo durante el año 2022. Entre ellas se encuentran cinco de las escogidas para esta investigación (Alerta periodo, es la excepción). Esto puede observarse en la siguiente grafica que representa a cada aplicación con el número de descargas actual en ese momento:



Fuente: Ceci, 2023.

Según este estudio en abril de 2022 Flo fue la *app* más descargada de todo el mundo de este sector y obtuvo 2.921.198 millones de descargas. Seguida de Calendario Menstrual con 2.020.559 y Meet You con 1.930.389 millones.

Es destacable mencionar que las aplicaciones escogidas también fueron muestra en otras investigaciones como en el estudio realizado por Eticas Foundation en 2022. Por

último, comentar que en You Tube se puede encontrar una amplia gama de videos donde se explican las ventajas e inconvenientes de algunas de las *apps* escogidas, contando algunos de estos con más de 50.000 reproducciones.

Respecto al número de descargas, dos de estas *apps* (Mi calendario menstrual y Flo) cuentan con más de 100M en Google Play y App Store, y el resto con más de 10M.

En cuanto a estrellas (puntuación de personas usuarias) encontramos: en App store a Flo; con 4,7 estrellas, Mi calendario Menstrual; con 4,9 estrellas, Meet You; con 4,6, Alerta periodo; con 4,8, Clue; con 4.7, y a Calendario menstrual; con 4,7.

Dentro de la plataforma de descarga Play Store se puede observar a Flo; con 4,7 estrellas, Mi calendario Menstrual; con 4,9 estrellas, Meet You; con 4,8, Alerta periodo; con 4,6, Clue; con 4.7 y Calendario Menstrual; con 4,9. Como se puede observar existe una leve diferencia entre App Store y Play Store.

En cuanto a la ubicación del desarrollador, el de Mi Calendario Menstrual y Flo se encuentran en territorio de Reino Unido, Clue; en Alemania, Meet You; en Singapur y Calendario Menstrual y Alerta Periodo; en territorio estadounidense.

Relativo a los fundadores de estas iniciativas solo se han podido encontrar los de Flo y de Clue siendo los de la primera Dmitry y Yuri Gurski y los de la segunda Ida Tin, Hans Raffauf, Moritz von Buttlar y Mike LaVigne.

Lo mismo ocurre con los patrocinadores ya que los únicos datos que se han podido encontrar abiertamente son que: Flint Capital, Haxus Venture Fund, Mangrove Capital Partners y Founders Fund patrocinaron Flo y Union Square Ventures y Mosaic Ventures, Clue.

Worsfold *et al.,* (2021) explica que las *apps* de control de ciclo se lanzaron por primera vez en 2013. El autor asegura que se estima que 50 millones de mujeres en todo el mundo utilizan aplicaciones de seguimiento del periodo.

Un estudio realizado por Levy y Romo-Aviles (2019) menciona que las mujeres usan estas aplicaciones por 8 motivos: seguir los datos de su ciclo menstrual y sus regularidades, prepararse para retrasos, saber más sobre sus cuerpos y su ciclo menstrual, anotar sus experiencias menstruales y emociones, informarse por

profesionales de la salud, hacer un seguimiento de su salud, buscar el embarazo y detectar cambios en su periodo.

Otras de las funciones de este tipo de aplicaciones son observar e identificar patrones en los ciclos menstruales, prepararse para el próximo periodo, aprender sobre el cuerpo, controlar afecciones crónicas y lograr o evitar el embarazo (Epstein *et al.,* 2017; Gambier-Ross *et al*., 2018; Levy y Romo-Avilés, 2019).

Ahora bien, el motivo por el que me he centrado durante el estudio en el marco regulatorio de protección de datos Europeo y el de EEUU es el siguiente: en primer lugar mi localización geográfica está dentro de territorio europeo por lo que esta zona es de mi interés, por ser el espacio político en el que habito. Además a partir del 25 de mayo de 2018, se empieza a aplicar el RGPD por sus siglas en español (Reglamento General de Protección de Datos) dentro de la Unión Europea, mencionado anteriormente y del que se hablará en profundidad más adelante.

En cuanto a EEUU se ha escogido principalmente por su nueva ley llamada Cloud Act aprobada y promulgada por los Estados Unidos el 23 de marzo de 2018 cuyo objetivo es facilitar la recopilación de datos del gobierno de Washington (personales y de otro tipo) alojados por proveedores de servicios en la nube de los EEUU.

El principal problema reside en el conflicto que esto genera en contraposición al RGPD y es por esto que se ha tomado esta conflagración como uno de los núcleos de la investigación.

Lucie Audibert (2022), abogada de Privacy International, plantea el conflicto y señala que el hecho de que los datos sean procesados por una empresa europea, no significa que es completamente inmune a los procesos de Estados Unidos. “Cuando se trata de una solicitud legal legítima procedente de las autoridades estadounidenses, las empresas europeas suelen acatarla. Asimismo, es posible que una empresa europea albergue datos fuera de la Unión Europea, circunstancia que la somete a diferentes marcos jurídicos y acuerdos transfronterizos” (*idem*).

En cuanto al periodo temporal que abarca la investigación, comentar, que la mayoría de documentos encontrados datan a partir del 2018. Mucho antes ya se hablaba de la problemática de la venta o mal uso de datos y las violaciones de privacidad, sin embargo, es más reciente el hecho de que esto se relacione con *apps* de menstruación y

aborto. Se podría decir que el detonante que hizo que estos temas confluyeran fue una denuncia a Flo en 2018 por compartir datos sensibles de sus usuarios con más de 150 grandes empresas.

No obstante, es a partir del 24 de junio de 2022, tras revocar la sentencia "Roe contra Wade" por la Corte Suprema de Estados Unidos, cuando el tema empieza a ser una preocupación generalizada y muchas mujeres empiezan a alertar sobre el tema.

La excepción a este "asalto a la privacidad" en los EEUU quizás se encuentre en el estado de California, donde en 2018 se implantó la Ley de Privacidad del Consumidor de California (CCPA), la cual cuenta con un nivel de protección alto al igual que el RGPD europeo. Sin embargo esta norma se aplica únicamente a ciudadanos californianos lo que deja al resto en desventaja. Es cierto que en Europa las ciudadanas pueden llegar a replantearse algo menos la cuestión ya que pueden sentirse protegidas por la legislación, aunque para algunos esto es una simple ilusión.

Este trabajo ha hecho especial hincapié en desglosar cuales de nuestros datos son los más demandados por estas empresas y hasta donde podrían llegar sin nosotros saberlo. Además se ha querido investigar cuales de los datos segregados por el cuerpo de la mujer son los más demandados . Esto se ha logrado mediante la comparación de la muestra escogida que ha permitido crear una visión general sobre el potencial de estas *apps.*

Objetivos y Técnicas empleadas

En cuanto a los objetivos separamos entre generales y específicos:

Un objetivo general es el enunciado en que se expresa la acción general o total que se llevará a cabo para lograr una meta. Se plantea porque existe una meta que se desea lograr, y para lograrla es necesario disponer de cierta información básica. Consiste en enunciar lo que se desea conocer, buscar y lo que se pretende realizar en la investigación (A Cardozo *et al.,* 2016).

Según la Revista multidisciplinar de ciencia latina los objetivos específicos "son enunciados proporcionales desentrañados en etapas de un objetivo general", deben ser: cualitativos, conductuales y específicos (Caballero 2014 citado en Arias *et al.,* 2020).

La cantidad de los objetivos específicos que se formulen depende de lo que se necesita para lograr el objetivo de investigación o están orientados a lograr cada etapa del desarrollo de la investigación (Behar, 2008, citado en Arias *et al.,* 2020). Los objetivos específicos son las etapas o pasos que se deben realizar para lograr el objetivo general (Bernal 2006, citado en Arias *et al.,* 2020) ; por otro lado, se debe evitar disgregar los objetivos específicos del objetivo general y estos deben relacionarse con el objetivo general por medio de sus dimensiones (Barragán *et al*., 2011, citados en Arias *et al.,* 2020).

En el caso de este estudio los objetivos generales marcados son los siguientes:

1. Conocer las diferencias existentes entre las políticas de privacidad de cada una de las *app* de seguimiento menstrual escogidas.

2. Comprobar si hay alguna diferencia entre las políticas de privacidad que encontramos en EU y las que se encuentran en EEUU.

3. Estudiar la relación que pueden tener las políticas de privacidad de las *apps* de control de ciclo con la situación del cambio de legislación con respecto al aborto en EEUU.

Y por lo tanto los específicos que los acompañan son:

1. Analizar la oferta de *apps* junto a sus políticas de privacidad para saber qué datos recopilan y con qué fines.

2. Acceder a VPN estadounidense para obtener las políticas disponibles en ese territorio.

3. Profundizar en la información sobre la era post “Dobbs contra Jackson” y conocer casos reales de vigilancia digital.

Pregunta de investigación y Metodología

En palabras de Hamui (2015) la pregunta de investigación en los estudios cualitativos “condensa aspectos teóricos, temáticos, metodológicos y empíricos, y constituye el eje transversal del proceso de indagación (…) Una buena pregunta de investigación hace la diferencia en la profundidad de los hallazgos y las aportaciones al campo de estudio” .

A partir de los objetivos marcados con anterioridad y del marco teórico expuesto ya es posible definir la pregunta por la cual surge esta investigación: ¿Qué pasaría si una usuaria estadounidense se descarga una *app* de seguimiento menstrual con sede en Europa? ¿Y al contrario?

En caso de que alguna de ellas se viera envuelta en algún problema legal ¿de qué forma se haría uso de sus datos? ¿Estarían ambos sujetos en una situación igualitaria?

Las preguntas vienen a intentar completar los cuadros en blanco de la siguiente tabla ya que lo que sí tenemos claro es que si una *app* cumple a raja tabla el reglamento europeo actual, trata con una usuaria también europea, y posee absolutamente todos sus servidores en territorio también europeo el riesgo de que se usaran los datos de la misma en su contra sería mínimo, por no decir inexistente.

		APLICACIÓN	
USUARIA		EEUU	EU
	EU		✓
	EEUU	✗	

Fuente: Elaboración propia.

Otra cosa también clara es que como se ha podido comprobar en EEUU la legislación en cuanto a datos y privacidad es muy ambigua en la mayoría de los estados (con excepciones como la CCPA). Es por esto que cómo ya varios casos han demostrado una ciudadanas estadounidense se encuentra menos protegida por su legislación de protección de datos y por lo tanto más expuesta a problemas relacionados con su privacidad.

Ahora bien, muchas veces como se ha podido observar el problema reside en que aunque una *app* tenga sede en Europa es posible que sus servidores se encuentren dispersos por diferentes territorios entre ellos EEUU y que esto pueda generar un conflicto territorial.

Como se observa en la tabla el dilema se encuentra cuándo ambos mundos se encuentran en un vacío. Estos problemas de transferencias de datos internacionales se han intentado solucionar a lo largo de la historia con varios acuerdos que finalmente han acabado siendo diluidos por su poca efectividad, de ellos se hablará algo más adelante.

La técnica metodológica que se llevará a cabo para la consecución de los objetivos será un análisis comparativo cualitativo además de una revisión bibliográfica de los acontecimientos.

Los estudios cualitativos se caracterizan por un proceso de construcción interactiva del argumento teórico y la evidencia empírica. Estos son estudios de tipo holístico en los cuales se trata de captar el núcleo de interés y los elementos clave de la realidad estudiada, facilitándose de esta manera el entendimiento de los significados, los contextos de desarrollo y los procesos (Maxwell, 1996 citado en Tonon, 2011).

El método comparativo tiene como objetivo la búsqueda de similitudes y disimilitudes. Las disimilaridades se presentan como lo que diferencia a la especie de su género, y esto no es lo mismo que señalar las variaciones internas de una misma clase; por lo cual se requiere de un trabajo sistemático y riguroso que implique la definición previa de las propiedades y los atributos posibles de ser comparados, afirma el autor (Sartori, 1984 citado en Tonon, 2011).

La utilización del método comparativo en estudios cualitativos en ciencias sociales y en ciencia política, requiere de un investigador que sea prudente en la selección de los casos a comparar, tarea que ha de desarrollar siguiendo criterios metodológicos, lo cual significa que los casos elegidos presenten variables similares que puedan ser consideradas constantes y variables disimilares interesantes de ser contrastadas (Tonon, 2011).

La elección del método comparativo reside en sus ventajas, pues como bien dice Nohlen (2020) este brinda mucha libertad, en este caso a la investigadora, para el desarrollo de un diseño propio de investigación en adecuación a la situación específica.

En el caso de la revisión bibliográfica la metodología propuesta podría ser aplicada a cualquier tema de investigación para así poder determinar la relevancia e importancia del mismo y asegurar la originalidad del estudio.

Además, permite que otros investigadores consulten las fuentes bibliográficas citadas, pudiendo entender y quizá continuar el trabajo realizado. Esta metodología se compone de cuatro fases según Gómez-Luna (2014): definición del problema, búsqueda de información, organización de la información y análisis de la información.

Por lo tanto el análisis empírico se realizará en base a 6 de las *apps* más descargadas tanto en la UE como en EEUU. De estas se obtendrán las siguientes variables: si estas comparten datos con terceros, qué tipo de datos, qué ocurre si hay una fusión de la empresa, si se pueden eliminar los datos almacenados o pedir una copia de ellos, si se menciona donde se encuentran los servidores de las *apps* o a qué ley dicen acogerse, si tienen en cuenta el RGPD, o si comentan la situación de otras regulaciones en sus políticas. Se hará hincapié en aquellos aspectos que puedan resultar relevantes para conocer cuál es la situación actual para las mujeres de EEUU y las de EU.

Durante esta revisión bibliográfica se ha hecho uso de una gran cantidad de bibliografía anglosajona, para así, desde mi punto de vista, poder mantener el rigor necesario que merece este Trabajo de Fin de Grado. Es posible que durante la investigación se encuentre alguna traducción incorrecta o matices de los que no he sido capaz de percatarme, y es por esto que pido disculpas de antemano.

Aún así considero muy importante la amplia bibliografía utilizada para este estudio ya que creo que ha podido enriquecer y dar puntos de vista que no hubieran sido posibles de otra forma.

Por otro lado y antes de finalizar este apartado me gustaría dejar claro que tengo presente que quizás haya mujeres que no se sientan identificadas con su género y por lo tanto puedan sentirse ofendidas a lo largo de la investigación por el hecho de nombrarlas o referirme a ellas con términos como “mujer” o “usuaria” pero no me gustaría que la investigación se vea afectada por ello.

Es cierto que en los estudios revisados con anterioridad, aunque relevantes, podrían considerarse incompletos si se centran únicamente en el binomio mujer-aborto. Me gustaría recalcar que a lo largo de la investigación podría haber hecho uso del término

“menstruador” el cual, según Pichon (2022) fomenta la inclusión de las personas que experimentan el proceso biológico de la menstruación, independientemente de su género (*idem*).

Sin embargo tomé la decisión de generalizar y usar la palabra mujer cuando quería referirme a una persona que biológicamente menstrua. Considero necesario apelar directamente a la mayoría, que quizás, si pueda verse identificada con los términos utilizados a lo largo de la investigación.

La menstruación, como gran delatora del aborto, forma parte de la intimidad de muchas mujeres y es por esto que ante el peligro, es mi intención alertarlas directamente tras la evidencia del problema.

Asimismo si algún colectivo se siente ofendido o quizás discriminado a lo largo del estudio sería de mi agrado que me lo hiciera saber para así poder incluirlo en esta investigación y poder avanzar de forma conjunta.

Estado de la cuestión

He decidido dividir el estado de la cuestión en cuatro apartados. En el primero desarrollaré algunos conceptos relacionados con las aplicaciones de control de ciclo, su surgimiento y representatividad. Más adelante estableceré una breve exposición de la historia de las leyes en materia de privacidad EEUU y Europa, así como un breve resumen de los acuerdos que han tratado de abarcar las transferencias de datos entre ambas potencias. Tras este punto, trataré de explicar los cambios legislativos de los últimos años entorno al derecho al aborto en EEUU. Por último, pasaré a hablar sobre cómo confluyen los temas anteriores dando pie a un panorama realmente distópico.

Aplicaciones de control de ciclo

Según el diccionario María Molinier la menstruación se define como "sangre procedente de la matriz que evacúan durante algunos días de cada mes las mujeres y también las hembras de otros mamíferos". Por otro lado la RAE, la considera "acción de menstruar", cuyo significado es "evacuar el menstruo", lo cual es, "sangre procedente de la matriz que todos los meses evacuan naturalmente las mujeres y las hembras de ciertos animales".

Si profundizamos algo más en las raíces de la palabra vemos como el diccionario de etimologías en línea de Chile sostiene que el término menstruación, aparece formado por los siguientes elementos latinos: *menstruus* (menstruo), compuesto con: la palabra *mensis* (mes, ciclo lunar, lunación), el sufijo - *estris* que indica propio de, el sufijo *–uus* (relación activa o pasiva), y el sufijo *–ción* que indica "acción y efecto".

Las aplicaciones de seguimiento menstrual forman parte de lo que se denomina la "Tecnología Femenina": *Software*, diagnósticos, productos y servicios que aprovechan el poder de la tecnología para mejorar la salud de las mujeres (Mcmillan, 2022). Según Statista (2023), se espera que el mercado global de productos y servicios de "Tecnología femenina" o como algunos llaman, *"Femtech",* crezca 60 mil millones de dólares para el año 2027.

Se puede intuir que el *target* de estas aplicaciones son mujeres que menstrúan y que por lo tanto se encuentran comprendidas entre los 12 y los 55 años. Este público objetivo parece sentir la necesidad de planificar su ciclo, por lo que decide instalar una de las *apps* del catálogo actual con el fin de que esta le ayude a recordar: cuándo será su próximo periodo, cuando ovulará, o qué días será más propensa a quedarse embarazada. Es cierto que varias aplicaciones contienen restricciones en cuanto a la edad y algunas de ellas no pueden ser utilizadas por menores de 16 o 18 años , lo que reduciría el público objetivo de este tipo de aplicaciones.

En muchas ocasiones las *apps* de seguimiento menstrual son consideradas por muchas de las usuarias un anticonceptivo natural ya que les ayudan a conocer su cuerpo y así poder planificar o prevenir futuros embarazos.

Asimismo algunos estudios muestran otros curiosos motivos por los que muchas mujeres parecen mostrar rechazo a métodos anticonceptivos médicos . Por ejemplo un estudio publicado por INSERM (Instituto Nacional de Salud e Investigaciones Médicas) y realizado por Catherine Vidal y Jennifer Merchant (2022) expone que el rechazo a las píldoras anticonceptivas también forma parte de una conciencia cada vez mayor de una ecología "global", que va desde el respeto de las funciones naturales del cuerpo hasta la protección del medio ambiente.

Ford (2021) habla de un "contexto de demanda de métodos anticonceptivos no médicos" por el cual se ha desarrollado el mercado de las aplicaciones de seguimiento menstrual. Además, según estos autores para muchas jóvenes el uso de tecnologías digitales para el seguimiento del ciclo menstrual y la fertilidad es percibido como fiable, con la ventaja de la facilidad de uso y un coste mínimo. Los servicios personalizados de las *apps* también se pueden interpretar como un vector de "empoderamiento", pues dan a la mujer menstruante la oportunidad de crear su "diario íntimo" (i*dem*).

El término empoderamiento también es mencionado por las investigadoras Levy y Romo-Avilés (2019), pues ambas revelan que el seguimiento de la menstruación a través de estas *apps* tiene potencial para ser una práctica empoderadora, ya que ayuda a las usuarias a ser más conscientes tanto de sus ciclos menstruales como de su salud.

Tras la investigación nos percataremos de que esta "facilidad" y "coste mínimo" y sensación de "empoderamiento" pueden no ser términos del todo adecuados para definir a este tipo de servicios digitales y sus efectos reales.

Otra razón que podría estar relacionada con el éxito de estas *apps,* hasta el momento, se debe a que la tendencia generalizada en el mercado es la abundancia de aplicaciones de atención médica orientadas a hombres y no a mujeres (Follows, 2018).

Un detalle que ejemplifica bien este hecho es que la *app* de Salud de iPhone, que tenía todo tipo de herramientas de monitorización como medidor de pasos, pulsaciones o nutrición, no incluyó la opción de salud reproductiva (como la menstruación) hasta el año 2015. Y es aquí donde las pioneras de la tecnología femenina se adelantaron (Serrano, 2019).

Debemos tener en cuenta que para las mujeres, una pregunta de admisión habitual en las revisiones clínicas es: "¿Cuándo fue el primer día de su última menstruación?" El

seguimiento menstrual se considera un signo vital crítico de la salud ginecológica y general. Por lo tanto el deseo de recopilar información exacta sobre el ciclo menstrual ha dado lugar a una creciente demanda de aplicaciones sanitarias para móviles. A causa de esto el mercado de este tipo de aplicaciones ha crecido exponencialmente en la última década. Se calcula que en 2016 se produjeron 200 millones de descargas de aplicaciones de seguimiento del periodo en todo el mundo (Eschler *et al.,* 2019).

No obstante, es cierto, que la anotación del ciclo menstrual es una práctica realizada durante décadas y por lo tanto algo que se ha considerado no tecnológico hasta hace más bien poco, los problemas han ido surgiendo desde que esto se ha pasado a ser una práctica digital.

Es por esto que la tecnología femenina también tiene ciertos detractores y es que algunos estudios señalan su baja fiabilidad médica y sus malas prácticas en cuanto a la recopilación de datos personales.

Por ejemplo Levy y Romo (2019) señalan que el seguimiento menstrual puede tener consecuencias negativas, ya que en algunos casos "provoca angustia y problemas de privacidad".

Varios autores advierten sobre la fiabilidad de dichas *apps* y afirman que aunque estas sigan aún proliferando, ya se conoce la existencia de problemas relacionados con la precisión y la eficacia de estas (Eschler *et al.,* 2019).

Además el Colegio de Médicos de Nueva York demostró que el 81% de estas aplicaciones son inexactas a la hora de predecir el embarazo (Setton *et al.,* 2016).

Asimismo un estudio alertaba sobre otro de los problemas de estas *apps*: la privacidad. Este reveló que el 79% de las aplicaciones de salud disponibles a través de Google Play Store**,** incluyendo las aplicaciones que ayudan a gestionar los medicamentos o la información de las recetas, regularmente compartían los datos de los usuarios y estaban "lejos de ser transparentes" (Grundy *et al.,* 2019).

En este sentido considero pertinente hablar en este punto del proyecto *Chupadatos*, lanzado en diciembre de 2016, el cual tiene como objetivo contar a la sociedad, a través de textos e infografías, cómo los equipos y servicios tecnológicos son usados en

América Latina para recolectar, almacenar e incluso vender datos personales, muchas veces sin el conocimiento de los usuarios.

Se trata de un proyecto que engloba la colaboración de periodistas e investigadores procedentes de Brasil, Argentina, Chile, México y Colombia, y busca producir contenido sobre privacidad, vigilancia y derechos digitales. La iniciativa surge gracias a la organización. Coding Rights, liderada por mujeres y creada en Brasil. Esta busca avanzar en el fortalecimiento de los derechos humanos en el mundo digital.

Al contrario de otros proyectos de Coding Rights, como Oficina Antivigilancia (más técnico y dirigido a activistas y entidades de defensa de derechos digitales), *Chupadatos* quiere atraer un público común al debate sobre privacidad y vigilancia en el ambiente digital.

En su artículo: *"Menstruapps -¿Cómo convertir tu menstruación en dinero (para los demás)?"* algunas de las investigadoras brasileñas comparten lo siguiente: "Alimentadas con nuestros datos, estas herramientas funcionan como laboratorios para la observación de patrones fisiológicos y de comportamiento, que van desde la frecuencia de la menstruación y los síntomas asociados con ella, hasta los hábitos de compras y navegación por Internet de todas sus usuarias" (Felizi y Varon, 2016).

Visto desde la perspectiva de Siamka y Biasin (2021) compartir datos con estas *apps* provoca a su vez que su valor aumente.

Según estas autoras belgas los frutos de la actividad de dichas usuarias se acaban convirtiendo en recursos que benefician a las empresas que procesan los datos. A medida que las usuarias se convierten en participantes activas en el proceso de producción, las líneas que delimitan entre quién produce, consume y se beneficia de sus datos se desvanecen y estas se convierten en *prosumidoras* (Siamka y Biasin, 2021).

De este modo, en dicho estudio Siamka y Biasin (2021) comparten que: "En términos más generales, incluso cuando el valor producido no es extraído directamente por los proveedores y socios de la aplicación, repercute indirectamente en el capitalismo (digital), cumpliendo la amplia definición de trabajo de Glazer (1984): `aquellas actividades que producen bienes y/o prestan servicios y/o facilitan la circulación de bienes y servicios que son directa o indirectamente para el capitalismo´".

Otra línea de investigación sería el tabú de la menstruación relacionado con lo digital. Lutz y Sivakumar (2020) se centran en los Estados Unidos y descubren que el diseño y el uso de las aplicaciones móviles de seguimiento menstrual parece verse influenciado por el hecho de que la menstruación se considere un tabú en la cultura estadounidense. Esta investigación cita a su vez un estudio que revela que algunas mujeres quieren características en las aplicaciones móviles de seguimiento menstrual que oculten su propósito: tres de cinco mujeres dijeron que preferían una aplicación móvil de seguimiento del periodo "con una apariencia y un nombre discretos".

Según Mcmillan (2022) debemos tener en cuenta que estas *apps* "operan en el ámbito de la salud reproductiva de las mujeres, una esfera de la atención sanitaria asolada por la criminalización y el control (en muchos países) en forma de leyes sobre el aborto".

Leyes en materia de privacidad en EEUU y la UE

Breve historia de las políticas de privacidad en EEUU

En el año 1890, cuando los juristas norteamericanos Samuel D. Warren y Louis Brandeis publicaron su artículo doctrinal *"The Right to Privacy"*. Dicho trabajo sería el comienzo de este término en EEUU, que si bien no estableció qué era la privacidad de una manera específica, fue lo que inició la regulación sobre la misma y abrió el debate jurídico en EEUU (Polo, 2022).

No obstante el Tribunal Supremo, a lo largo de una extensa y gradual jurisprudencia, ha considerado implícito este derecho a la privacidad en algunas de las enmiendas que se han ido haciendo a la constitución (Nieves, 2011).

Por ejemplo la Cuarta Enmienda da garantías frente a registros y requisas arbitrarias, lo que limita la intrusión del gobierno en las personas, domicilios, documentos y efectos personales, incluyéndose no sólo los supuestos de invasión material sino también de vigilancia electrónica (*idem*).

Según Alzate y Cotta (2020) esta Cuarta Enmienda en la Constitución de los Estados Unidos de América salvaguarda la libertad de las personas relacionada con la privacidad del individuo. Esta se refiere a los allanamientos a bienes inmuebles sin orden judicial de los que puedan ser objeto en un momento determinado por autoridades judiciales, lejano de concretar las violaciones de la privacidad de datos por entidades comerciales.

Por otro lado la obra de William Stuntz (1995) defiende que el propósito real de la Cuarta y la Quinta Enmienda es poner demasiado difícil determinadas formas de regulación, haciendo que sea materialmente imposible reunir las pruebas necesarias para poder aplicarlas (Stunz, 1995, citado en Lessig, 2009).

Si se combinan la Cuarta y la Quinta Enmienda imposibilitan la obtención de pruebas para un crimen como el de sedición, haciendo así inútil cualquier intento estatal de perseguirlo. Pero no sólo para la sedición pues el autor añade que: "El efecto de la Cuarta, la Quinta y la Sexta Enmienda era la restricción del alcance de la regulación que era posible en la práctica" (i*dem*).

En cuanto a la escasa promulgación de leyes de privacidad en EEUU encontramos la siguiente cita de Lessig (2009): "La gran diferencia entre el copyright y la privacidad, no obstante, es la política económica que busca una solución para cada problema. Con el copyright, los intereses amenazados son poderosos y están bien organizados; con la privacidad, los intereses amenazados son difusos y están desorganizados. Con el copyright, los principios situados al otro lado de la protección (el procomún o el dominio público) ni son imperiosos ni son bien comprendidos. Con la privacidad, los principios situados en el otro lado de la protección (la seguridad, la guerra contra el terrorismo) son imperiosos y han sido bien comprendidos. El resultado de estas diferencias, como cualquier teórico político pronosticaría, es que en los últimos diez años, al tiempo que veíamos numerosas modificaciones legislativas y técnicas para resolver los problemas relativos a los derechos de autor, hemos visto muy pocas que resuelvan los problemas de la privacidad."

No obstante el avance tecnológico acompañado de violaciones constantes de la privacidad, crea la necesidad de formular ciertas normas que acompañen al momento histórico y protejan la privacidad de la ciudadanía como es el ejemplo de la Privacy Act [2]en 1974 (Ley de protección de la intimidad).

2
Office of Privacy and Civil Liberties, 1974. Privacy Act of 1974. https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974%2C%20as%20amended%2C%205%20U.S.C.,of%20records%20by%20federal%20agencies

Esta la normativa más general que otorga a las personas físicas el derecho a proteger su intimidad, frente a la información contenida en los registros del gobierno federal. Dicha Ley prohíbe la divulgación de un registro sobre un individuo sin su consentimiento por escrito, a excepción de algunas condiciones legales. También concede a las personas la oportunidad de modificar sus registros y establecer requisitos sobre cómo quieren mantenerlos. Asimismo se crea con el fin de obtener un código de buenas prácticas de información relacionado con la recopilación, mantenimiento, uso y difusión de información sobre los sistemas de registros manejados por agencias federales (Alzate y Cotta, 2020).

Debemos recordar que existen otras leyes que abordan aspectos concretos de la privacidad para sectores específicos como el financiero (FCRA) o la salud (HIPPA).

La Health Insurance Protability and Accountability Act (HIPAA) llegó en 1996 . Esta legislación estadounidense establece disposiciones sobre privacidad y seguridad de los datos para así poder salvaguardar la información médica de los usuarios (Lutkevitch,s.f).

Más adelante surgió la que sería el precedente de la Cloud Act: Ley de 1986 Stored Communications Act (SCA), la cual prohíbe a los proveedores compartir comunicaciones electrónicas con cualquier persona o entidad, pero también contiene excepciones,como, por ejemplo, cuando el gobierno obliga a facilitar la información (Balser y Attorney, 2022).

En cuanto a legislaciones más concretas también encontramos a lo largo de la historia de EEUU la Children´s Online Privacy Protection Acten (COPPA) en 1998. Esta Ley fue adoptada con el fin de proteger la privacidad de los niños menores de 13 años y fue dirigida a sitios web que interaccionan con niños, cuyos operadores deberán tener el consentimiento de los padres para su utilización. La Ley obliga a la Comisión a promulgar normas que exijan a los operadores de sitios web comerciales y servicios en línea dirigidos a menores de 13 años o que recojan a sabiendas información personal de menores de esa edad (Federal Trade Comission, s.f).

Para finalizar la Fair and Accurate Credit Transactions Act (FACTA) de 2003 protege la información crediticia de los consumidores frente a los riesgos relacionados con el robo de datos. Esta Ley se promulga como enmienda a la Ley de Información Crediticia

Justa. Fue diseñada para “mejorar la exactitud de los registros relacionados con el crédito de los consumidores" según la Comisión Federal de Comercio (FTC) (Spicer, 2021).

Cloud Act

En la actualidad nos encontramos con la Cloud Act, acrónimo de “Clarifying Lawful Overseas Use of Data Act”, una ley federal estadounidense promulgada el 23 de marzo de 2018. Esta Ley principalmente modifica el Capítulo 121 del Título 18 del Código de los Estados Unidos, conocido como la Ley de Comunicaciones Almacenadas, al permitir que EEUU obtenga información almacenada en los servidores de proveedores americanos de servicios en la nube, independientemente de que los datos se encuentren en servidores en EEUU o en el extranjero, vulnerando así las garantías del RGPD (Rodríguez, 2019).

Dicho de otra manera se trata de una ley que regula el acceso de las autoridades estadounidenses a los datos almacenados en servidores de empresas de dicho país (como correos electrónicos, mensajes de texto o chats) con independencia de su ubicación, lo que significa que se incluyen territorios fuera de sus fronteras (incluida la UE). Esto podrá realizarse bajo el amparo de una orden judicial. Al final esto se traduce en la práctica en el permiso de realizar transferencias de datos internacionales con destino a EEUU basándose en esta norma (Cordero, 2019).

A veces es posible encontrarse la Cloud Act renombrada como nueva Ley de “privacidad”, aunque esta sea más bien limitante o atacante de la misma. Además se podría decir que esta amplía la soberanía de EEUU, sobre sus ciudadanos

Según Peirano (2022) esta Ley podría conllevar riesgos pues “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”.

Rodríguez (2019) afirma que EEUU justifica esta Ley con la supuesta lucha contra el terrorismo, al igual que lo hace con la *Patriot Act*, Ley promulgada en 2001 que obliga a los proveedores de tecnología americanos a estar dotados de capacidades de escucha o puertas traseras (*backdoors)*.

A este respecto, es oportuno recordar cómo Lessig (2009) afirma que aunque esta Ley fue promulgada 45 días después de los ataques terroristas del 11-S, la mayor parte de su contenido había sido redactado mucho antes de su fecha. El académico piensa que los autores de dicha Ley eran conscientes de que hasta que no se produjera un grave ataque terrorista, no existiría suficiente voluntad política para modificar significativamente el sistema legal.

Esta Ley autoriza, entre otras cosas, a la escucha de cualquier tipo de comunicación electrónica. Es por esto que las agencias gubernamentales de los EEUU piden a los proveedores de tecnología americanos que operan en territorio americano o en cualquier otra parte del mundo que su tecnología vaya provista de puertas traseras (*backdoors)* , medios de recopilación de datos. Todos estos elementos constituyen propiamente agujeros de seguridad por diseño, esto es, formas preestablecidas para poder entrar en un sistema informático sin ser detectados. Esta Ley, que se ha revisado y actualizado en diferentes ocasiones, ha sido impugnada por grupos de los derechos civiles por vulnerar los derechos de privacidad y confidencialidad de la información (Poyato, 2020).

Lessig (2009) pone de ejemplo a "un gusano" e invita al lector a que imagine lo siguiente: este es capaz de registrar algunas maquinas bajo una orden judicial, para el autor esto supondría que quedara así liquidada la cuestión de la necesidad de contar con sospechas previas. Ahora bien, Lessig propone imaginarse que esta regla incluye la siguiente cláusula: "el Estado exige que las redes informáticas se construyan de modo que permitan instalar en cualquier ordenador un gusano, siempre que medie una autorización judicial". Bajo este régimen, las máquinas habrán de ser aptas para gusanos, aunque éstos sólo se introduzcan con un mandato judicial.

La situación tras la *Patriot Act*, se enfatizó después de las revelaciones de Snowden en 2013 con la grabación de las videollamadas Skype dentro del programa PRISM. "Dentro de este programa se espiaron a través de las backdoors de skype, las videoconfernecias de las Naciones Unidas, de la Agencia Internacional de la Energía Atómica con sede en Viena, del consulado de la Unión Europea en Nueva York y más de 80 embajadas y consulados de todo el mundo, incluidas las de países aliados" (Poyato, 2020).

Snowden (2019) en su libro menciona textualmente lo siguiente:

> " El FISC (*Foreign Intelligence Surveillance Court* o Tribunal de Vigilancia de Inteligencia Extranjera), que supervisa la vigilancia de inteligencia dentro de Estados Unidos, es un organismo especializado que se reúne en secreto y solo celebra audiencias con el Gobierno. Este tribunal se diseñó para emitir órdenes judiciales individuales en materia de recopilación de inteligencia extranjera, y siempre se ha mostrado especialmente complaciente ante la NSA: […] pasaba a utilizarse para legitimar toda la infraestructura combinada de PRISM y la recopilación Upstream. La revisión judicial de esa infraestructura se reducía, en palabras de la ACLU, a un tribunal secreto que apoyaba programas secretos reinterpretando, en secreto, la ley federal".

Además el experto apunta en su obra:

> "Cuando grupos de la sociedad civil como la ACLU trataron de poner en entredicho las actividades de la NSA en tribunales federales ordinarios, en audiencia pública, ocurrió algo curioso. El Gobierno no se defendió arguyendo que las actividades de vigilancia fuesen legales o constitucionales. […] Y lo que era más: que la ACLU no podía recurrir al litigio para buscar pruebas de esa vigilancia, porque la existencia, o no, de dichas pruebas era «un secreto de Estado» y las filtraciones a periodistas no contaban. […] Para mi indignación, en febrero de 2013 el Tribunal Supremo de Estados Unidos decidió, por cinco votos a cuatro, aceptar el razonamiento del Gobierno y desestimar una demanda de la ACLU y Amnistía Internacional contra la vigilancia masiva, sin ni siquiera plantearse la legalidad de las actividades de la NSA" (*idem*).

En relación con esto me parece interesante citar a Laura Poitras documentalista y productora estadounidense con una amplia filmografía entre la que se encuentra el documental *"Citizenfour",* por el cual recibió un Oscar al mejor documental largo de 2015 (Pulver, 2015).

Este cuenta la historia de Edward Snowden y sus revelaciones sobre el espionaje de la NSA. En él aparecen escenas históricas como aquellas en que Snowden revela en el hotel Mira de Hong Kong a los periodistas Glenn Greenwald y Ewen MacAskill los documentos filtrados acerca de la vigilancia mundial llevada a cabo por diversas agencias de inteligencia de Estados Unidos. Poitras junto al citado Greenwald es una de las dos personas que tuvieron un acceso completo en 2013 a los archivos del programa de vigilancia masivo revelado por Edward Snowden (Mass, 2013).

Volviendo a la Cloud Act se puede observar que esta incumple el artículo 48 del RGPD titulado "Transferencias o comunicaciones no autorizadas por el Derecho de la Unión" y que dispone lo siguiente:

> "Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo".

Como se puede observar este artículo especifica que haría falta un acuerdo internacional para transferir datos fuera de la UE. Al no existir semejante acuerdo válido entre EEUU y la UE solo existe una posibilidad: una orden judicial justificada por motivos de seguridad nacional (Cordero, 2019).

Según un informe de 2019 del Consejo de Abogacía Europea el Tribunal Europeo de Derechos Humanos se requiere una definición clara de la "naturaleza de los delitos que pueden dar lugar a una orden judicial" y otra de "las categorías de personas que pueden ser objeto de seguimiento".

Además hay que tener en cuenta que esta Ley conlleva que el proceso de una investigación criminal por parte de EEUU ya no se dependan de los llamados tratados de asistencia legal mutua entre países para poder solicitar acceso a datos alojados en el extranjero, un trámite que podía extenderse en el tiempo (ACLU, 2018)

Los acuerdos MLAT (Tratado Mutuo de Asistencia Legal) suelen ser negociados por el poder ejecutivo y debían ser aprobados por dos tercios de los votos del Senado. Por el contrario, la Ley Cloud permitiría al poder ejecutivo firmar acuerdos con gobiernos extranjeros sin la aprobación del Congreso.

La Unión Americana de Libertades Civiles (ACLU, por sus siglas en inglés)[3] publicó una "Carta de Coalición sobre la Ley Cloud" el 12 de marzo de 2018, donde se

3 Aclu.org (2018). Coalition Letter On Cloud Act. https://www.aclu.org/letter/coalition-letter-cloud-act

explicaba que el proyecto de Ley, "socavaba la privacidad y otros derechos humanos, así como importantes salvaguardas democráticas" y "colocaba la autoridad en manos del poder ejecutivo".

Dicha declaración pública especificaba algunas de sus preocupaciones más destacadas sobre lo que por entonces era aún un proyecto de ley. La Ley Cloud despojaría de poder al Congreso y pondría la autoridad en manos del poder ejecutivo. Además otorgaría al poder ejecutivo discreción para suscribir acuerdos con países que no protgen los derechos humanos, permitiéndoles obtener información sensible de los usuarios sin más revisión por parte de cualquier organismo o entidad estadounidense.

Por último la Unión Americana de Libertades Civiles ya decía que esta no protegería los derechos constitucionales de los ciudadanos y otras personas que residan dentro de Estados Unidos.

Como era de esperar todo esto ha hecho saltar algunas alarmas y muchas personas se han rebelado contra la aprobación de esta controvertida Ley.

Mr. Jérôme Tassi (2021), abogado asociado de propiedad intelectual, recomienda en una entrevista para IntoTheMinds, tener cuidado, y de ser posible, no almacenar datos ni en Google, Amazon ni Microsoft. El célebre abogado afirma que en su país, Francia, el gobierno publicó una doctrina denominada "Cloud at the Center" la cual prohíbe almacenar datos de la administración francesa en lugares que no estén certificados con SecNumCloud. Las grandes empresas mencionadas anteriormente, las cuales poseen un 69% del mercado de almacenamiento en la nube, no cuentan con el beneficio de dicha certificación y por lo tanto se encuentran excluidas de la administración francesa (Schwab, 2021).

Esto me recuerda al caso de la Comisión Europea, que en el año 2020 vetó el uso de WhatsApp entre sus trabajadores y les solicitó que, en su lugar, emplearan Signal, otra aplicación de mensajería instantánea más segura, programada con código abierto. La Comisión Europea no es la única en tomar medidas pues la Organización de las Naciones Unidas también prohibió el uso de WhatsApp anteriormente, tras el hackeo que sufrió el CEO de Amazon, Jeff Bezos, en el que se vieron implicados cargos políticos de Arabia Saudí (Moreno, 2020).

Retomando la Cloud Act, según Tassi (2021), esta nació como fruto de una disputa entre las autoridades federales de Estados Unidos y Microsoft. Tras un conflicto, la empresa tecnológica se acogió a la ubicación de los datos (Irlanda) para negarse a entregarlos al gobierno americano. Como se puede observar la ley surge, por parte del gobierno americano, para así poder ejercer un control completo según la nacionalidad de la empresa en lugar de por su ubicación geográfica (Schwab, 2021).

Sobrino (2021) también sostiene que dicha Ley mantiene su origen en 2013 tras el caso entre Microsoft y el Gobierno de los EEUU.

Según los autores del artículo *"The Microsoft Ireland case, the cloud act and the cyberspace sovereignty trilemma"* el caso de Microsoft y sus efectos pueden considerarse un caso paradigmático, en el que converge la sociedad, la tecnología y las relaciones internacionales de tal forma que ponen en tela de juicio la soberanía de los actores implicados. "Los flujos de datos y los gobiernos transgreden fronteras con una creciente aceptación de la inadecuación de las antiguas comprensiones territoriales del orden internacional" (De Hert y Thumfart, s.f).

En resumen, el 4 de diciembre de 2013, un juez del distrito sur de Nueva York se encontraba a cargo de un caso relacionado con el tráfico de drogas y la evidencia parecía encontrarse en la nube. Como parte de esta investigación, emitió una orden judicial en la que ordenaba a Microsoft que presentara todos los correos electrónicos y la información asociada a una cuenta de cliente individual. Sin embargo, el sospechoso, a pesar de ser residente en EEUU, había registrado su cuenta como residente en Irlanda y por lo tanto sus datos estaban siendo tratados como los de un ciudadano de allí. Por lo tanto mientras que la información de la cuenta se encontraba en servidores de Nueva York, los correos se encontraban alojados en un servidor de Irlanda. Microsoft se negó a ceder la información de estos correos justificándose en que un juez de EEUU no tenía autoridad para emitir una orden judicial sobre información almacenada en el extranjero (*idem*).

En mayo de 2014, un juez federal discrepó de Microsoft y le ordenó que entregara los correos electrónicos. Microsoft siguió con una serie de apelaciones, que acabaron ante el Tribunal Supremo de Estados Unidos a principios de 2018. Esto atrajo el interés público (289 grupos e individuos diferentes de 37 países firmaron 23 escritos legales apoyando la postura de Microsoft) (*idem*).

Cómo forma de escapar del dilema el legislador de EEUU, Donald Trump, puso en marcha interviniendo con la aprobación de la Cloud Act en marzo de 2018. De esta manera se aclaró drásticamente el marco jurídico al hacer legalmente posibles las órdenes extraterritoriales siempre que algún servidor de la empresa se encontrara alojada dentro de EEUU (*idem*).

Como Lessig (2009) diría en este caso se da un claro problema de soberanía nacional, el lo explica de la siguiente forma: "Por lo general, cuando un estadounidense va a Europa, no se lleva consigo al gobierno federal, ni tampoco acarrea un conjunto de reglas para los estadounidenses de viaje por Europa. Si va a Alemania, está generalmente sujeto a la ley alemana, y EEUU posee normalmente muy pocas razones para preocuparse de regular su conducta allí. Pero a veces el gobierno de EEUU sí tiene una razón para regular a sus ciudadanos en el extranjero. Cuando es así, ninguna ley internacional puede detenerlo".

El problema reside en que cuando un gran número de ciudadanos vive en dos lugares distintos, y uno de estos lugares no está únicamente dentro de la jurisdicción de una soberanía concreta, no esta claro qué clase de reclamaciones debería poder hacer una soberanía frente a las demás, y qué clase de reclamaciones pueden hacer todas ellas al ciberespacio (*idem*).

Según el autor se trata de otra ambigüedad latente en el pasado constitucional de EEUU pero en este caso no hay un momento de fundación constitucional internacional al que atenerse. Ya que en el momento en que la Constitución estadounidense fue redactada, la gente común no vivía rutinariamente en múltiples jurisdicciones descoordinadas entre sí (*idem*).

Cronología de las políticas relacionadas con la privacidad en EU

La Constitución Española de 1978 dispone en el artículo 18.4, el mandato de que la Ley limitaría el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Cinco años más tarde, se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, popularmente conocida como LORTAD, en desarrollo de aquel mandato constitucional.

El 13 de diciembre de 1999 las cortes generales aprueban la LOPD 15/1999, de Protección de Datos de Carácter Personal (LOPD). Se trata de una ley orgánica española que acaba siendo derogada con la entrada en vigor el 5 de diciembre de 2018 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, de la que se hablará más adelante. Esta es la adaptación del Reglamento General de Protección de Datos de la Unión Europea.

En el año 2000, en el marco europeo, se aprueba la Carta de los Derechos Fundamentales que en su artículo 8, reconoce el derecho de toda persona a la protección de datos de carácter personal que la conciernan.

Años después llegamos al 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. Este menciona en su Artículo 6: La magnitud de la recogida y del intercambio de datos personales (…) permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

La ley europea se trasladó a la legislación española en forma de Ley Orgánica 3/2018, como se mencionó anteriormente, de Protección de Datos Personales y garantía de los derechos digitales (LOPD GDD). Por lo tanto la LOPD-GDD o Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales regula el tratamiento de datos de carácter personal en España (Cadenas, 2022). Esta modificación dejó obsoleta a la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de 1999.

Por lo tanto el Reglamento General de Protección de Datos (RGPD) es considerado el reglamento actual europeo relacionado con la protección de las personas físicas en los que respecta al tratamiento de los datos personales y a la libre circulación de los mismos en la UE y en el EEE (Espacio Económico Europeo). Este trata de abordar aspectos

como la transferencia de datos personales fuera de la UE y del EEE. Al tratarse de un reglamento y no de una directiva es directamente vinculable y ofrece cierta flexibilidad a los Estados miembros para ajustar aspectos del mismo.

Se considera que su principal objetivo principal es la mejora del control y los derechos de las personas sobre sus datos personales así como la simplificación del entorno normativo a la hora de la realización de negocios internacionales. Es importante destacar que las multas por el no cumplimiento del RGPD pueden llegar a los 20 millones de euros.

A pesar de la implantación de dicho reglamento hay autores, como es el caso de Max Shreem, que cuestionan sus efectos y por lo tanto su poder de acción en la práctica.

Según la organización austríaca en defensa de los derechos digitales (None Of Your Business) (NOYB, 2023a), ONG el RGPD se ve envuelto en un conflicto de ley y reguladores. En los últimos años esta ley ha sido víctima de la falta de aplicación y de tácticas disuasorias por parte de las grandes empresas tecnológicas. Incluso cuando finalmente las empresas son multadas los casos se prolongan años a causa de los recursos y obstrucciones de las empresas tecnológicas. A veces, para NOYB, infringir la ley sale rentable a las "grandes tecnológicas". En definitiva, para la organización, el RGPD supone un reto, ya que los casos transfronterizos requieren la cooperación entre las autoridades. En este sentido Max Schrems (2023), abogado de privacidad austriaco y fundador de NOYB destaca: "Incluso las autoridades activas se encuentran a menudo en una pérdida, ya que la aplicación del RGPD es tan fuerte como su eslabón más débil″.

En esta misma línea, NOYB afirma que los Estados miembros no aplican en gran medida esta nueva legislación europea, lo que conduce a una “privacidad sobre el papel” pero no en los móviles y ordenadores de los usuarios.

Para Schrems (2021) tras 5 años de la aprobación del RGPD aún existe un choque de la legislación de la UE con la práctica nacional. Y es que aunque este Reglamento se aprobó en el Parlamento Europeo con una mayoría del 96%, Schrems afirma que casi todos los Estados miembros tienen algún truco o cuestión de procedimiento para socavar el RGPD: desde añadir conceptos como un "umbral" para las violaciones de la

privacidad, hasta considerar que "tramitar" una reclamación también puede significar simplemente tirarla a la basura. Por todo ello, el abogado austríaco concluye que, con respecto al RGPD, “tener derechos y obtener justicia son dos cosas muy diferentes”. [4]

Vidal y Merchant (2022) abundan en esta idea señalando que el RGPD se aplica a las empresas que publican aplicaciones de seguimiento menstrual cuya sede social se encuentra en Europa. Sin embargo para las autoras el hecho de que las aplicaciones estén disponibles en países europeos no garantiza la seguridad de los datos personales.

Por su parte la doctora en Ciencias políticas, Jimena Valdez, explica que EEUU es un país profundamente federal, con leyes que cambian de estado a estado y sin una ley nacional de protección de datos. La experta considera que en caso de que se avanzara en la criminalización del aborto y los gobiernos comenzaran a pedir datos, sin duda estas aplicaciones se las entregarían (Valdez, 2022 citada en Cadenas, 2022).

Según un informe del 2021 del Consejo Internacional de Responsabilidad Digital (IDAC) ,en EEUU, las *apps* no tienen que cumplir la mencionada HIPAA, esto es, la Ley federal de portabilidad y responsabilidad del seguro médico, la cual regula las normas de privacidad de los pacientes a las que están sujetas médicos, hospitales, laboratorios y aseguradoras médicas. Para más inri, no hay ninguna normativa que defina lo que constituye información sanitaria sensible.

Volviendo a la UE, la red EDRi, colectivo de ONGs, expertos y académicos que defienden y promueven los derechos digitales en todo el continente, se ha pronunciado sobre la situación del RGPD apuntando que que, a pesar del resultado globalmente positivo muchas de las grandes expectativas iniciales depositadas en el reglamento no se han hecho realidad. En coherencia con lo ya expuesto, la organización con sede en Bruselas cree que existen numerosas flexibilidades nacionales contenidas en el texto del Reglamento.

---

4. En su web podrás encontrar un "Mapa de trampas del GDPR" elaborado por ellos mismos: https://noyb.eu/en/trapmap

Ante esta indefensión varios grupos (Digital Defense Fund, Repro Legal Helpline y Electronic Frontier Foundation) han publicado guías ciudadanas para evitar que la información íntima pueda ser controlada cuando se pretende abortar o recibir atención sanitaria reproductiva.

Conflictos históricos relacionados con las transferencias de datos de EEUU – Casos Schrems I (2015) y Schrems II (2020)

Las relaciones comerciales a lo largo de los años entre la UE y EEUU han generado un elevado número de transferencias internacionales de datos, lo cual derivó en negociaciones entre el Departamento de Comercio estadounidense y la Comisión Europea para acordar la protección mutua de dichos datos.

De este modo, en 1999 EEUU y la UE iniciaron las negociaciones para poder determinar un sistema que permitiera la adecuación normativa de ambas potencias y así alcanzar un nivel adecuado de protección de datos personales de acuerdo a los requerimientos de la mencionada Directiva 95/46/CE.

El *Safe Harbor* o Puerto Seguro fue uno de los primeros intentos de establecer ciertas normas a la hora de estas transferencias internacionales de datos con fines comerciales entre la UE y EEUU.Este acuerdo reconoció los estándares de transferencia de datos a través de un sistema de autocertificación de empresas procedentes de EEUU. Para obtener dichas certificaciones las entidades debían cumplir una serie de principios. Sin embargo, estos podrían ser limitados en la medida necesaria, en atención a los requisitos de seguridad nacional, interés público o aplicación de la ley.

En el ámbito estadounidense se promovió la autorregulación al dejar que las empresas decidiesen si adoptar o no los principios europeos, pues la UE reconoció la realidad política de EEUU y la improbabilidad de la promulgación de un estatuto general de privacidad (Sobrino, 2021).

Las insuficiencias en la seguridad del sistema de Puerto Seguro hicieron saltar las alarmas en las instituciones europeas cuando en junio de 2013 las revelaciones de E. J. Snowden a los diarios The Guardian y The Washington Post alertaron de operaciones de vigilancia masiva llevadas a cabo por la Agencia de Seguridad Nacional norteamericana (NSA por sus siglas en inglés) (Ruiz, 2021)

En junio de 2013 tras las divulgaciones de los programas de vigilancia de la National Security Agency de EEUU y posteriores denuncias de otras actividades de inteligencia de EEUU en Europa, la Comisión advirtió que muchas empresas autocertificadas no cumplían con los principios del *Safe Harbor*. De hecho, Sobrino (2021) añadió que varias comunicaciones al Parlamento Europeo y al Consejo señalaron que este incumplimiento permitía a las autoridades estadounidenses acceder a los datos personales transferidos y tratarlos de manera incompatible con las finalidades establecidas.

Esta situación desembocó en la sentencia Schrems I de 2015, que marcó un hito en la historia de las decisiones de adecuación. El Tribunal de Justicia de la Unión Europea (TJUE) confirmó que EEUU participaba en una vigilancia masiva indiscriminada de los ciudadanos europeos y que el *Safe Harbor* no proporcionaba un nivel adecuado de protección (Sobrino, 2021).

Los principales motivos que causaron la invalidación de este sistema fueron dos: la falta de un marco legislativo específico en EEUU para casos en los que se restringen los derechos y libertades de los ciudadanos europeos en relación con la protección de datos (ej., por motivos de seguridad nacional), así como la ausencia de mecanismos judiciales que permitan a los ciudadanos europeos ejercitar sus derechos en ese país (Lopez, 2017).

La Sentencia Schrems I debe su nombre al jurista y activista Max Schrems, mencionado anteriormente. Su fama en las instituciones europeas empezó a labrarse con esta primera sentencia del TJUE, a la que se sumaría años después la referida al *Privacy Shield*, del que se hablará a continuación.

Tras ser interrogado por varios medios sobre si no consideraba que su trabajo deberían hacerlo los propios políticos, contestó: “En un mundo ideal no existiríamos, pero ahora mismo el gran problema que tenemos en Europa no son las leyes, sino hacer que se cumplan. Las autoridades no tienen el dinero, la capacidad o el personal para hacerlas cumplir, y sobre todo les falta la voluntad para que eso suceda” (Schrems, 2021).

Tras la sentencia Schrems I, la invalidez del sistema *Safe Harbour* dejó un vacío que se debía llenar con una solución política, sin la cual muchas empresas se encontraron desamparadas al no disponer de alternativas fáciles. Esto llevó a la negociación y

posterior aprobación por la Comisión Europea en julio de 2016 del acuerdo de adecuación para las transferencias de datos a EEUU denominado *Privacy Shield* (Escudo de Privacidad) (López, 2017) del que se hablará en el siguiente apartado.

Este fue también invalidado en julio de 2020 ya que el TJUE, en su sentencia Schrems II, sigue entendiendo que las exigencias de seguridad nacional de EEUU prevalecen sobre el marco legal de transferencias internacionales con la UE de manera intrusiva (Sobrino, 2021).

Uno de las principales críticas del *Privacy Shield* tiene que ver con el método desarrollado en cuanto a la autorregulación, pues este no proporcionaba un control en las actuaciones de las empresas por parte de la autoridad nacional, que se conformaba con un compromiso ético de cada empresa al realizar dichas transacciones (Alzate y Cotta, 2020).

Además este no había solucionado el principal problema, pues se seguía permitiendo la transferencia de datos personales de los europeos a EEUU. “Por lo tanto, también daba manga ancha a las agencias de vigilancia estadounidense para analizarlos sin las mismas garantías judiciales que en Europa debido a las facilidades aprobadas por Washington” (Del Castillo, 2023).

En su sentencia de 2020, el TJUE precisa que las transferencias de datos personales realizada con fines comerciales no pueden quedar de ninguna manera fuera del ámbito de aplicación del RGPD. De este modo, el dictamen explica que el país destinatario debe ofrecer un "nivel de protección sustancialmente equivalente al garantizado dentro de la Unión", refiriéndose principalmente a los "elementos pertinentes del sistema jurídico de dicho país" (Pérez 2020).

A día de hoy sigue sin haber una regulación clara para dicho cometido. He de decir que aún mientras me encontraba realizando este Trabajo de Fin de Grado, el 22 de mayo de 2023, fue publicada en varios medios la noticia de que la Comisión de Protección de Datos de Irlanda ha impuesto a Meta una multa de 1.200 millones de euros por quebrantar la normativa europea en materia de privacidad.

Se trata de una sanción histórica ya que es la más cuantiosa impuesta por la UE a una multinacional por infracciones relacionadas con la protección de datos, a excepción de la multa de 746 millones de euros que recibió Amazon por las autoridades de

Luxemburgo en 2021 tras la denuncia de la asociación francesa de defensa de las libertades en Internet La Quadrature du Net. El elevado precio de dicha sanción se debe a que la empresa liderada por Mark Zuckerberg ha continuado con su mala práctica anteriormente sancionada por el TJUE en su sentencia sobre el caso Schrems 2 de julio de 2020 (Lastra 2023).

El conflicto actual entre las leyes de privacidad de la UE y de EEUU son también un problema para los demás grandes proveedores de nube de EEUU, como son Microsoft, Google o Amazon. Para todos ellos la presión de cambios en sus políticas de privacidad no ha hecho más que aumentar tras las primeras multas importantes de las autoridades de protección de datos de la UE basadas en el RGPD.

En el caso concreto de Meta, para todas sus transferencias futuras espera pasar a un nuevo acuerdo que actualmente está negociándose entre Washington y Bruselas pero que ya ha sido duramente criticado por el Parlamento Europeo (Lastra, 2022). En todo caso, sobre la viabilidad de dicho acuerdo planea una *amenaza* bien conocida: "El nombre de Schrems se ha convertido en el principal temor para las dos partes". No en vano, la propia NOYB (2023) ya ha expresado su descontento y ve probable que el acuerdo sea invalidado por el TJUE, al igual que los dos acuerdos anteriores "Puerto Seguro" y "Escudo de Privacidad". Frente a ello, Max Schrems defiende una "solución más sencilla" en estos términos:

> "La solución más sencilla sería establecer limitaciones razonables en la legislación estadounidense sobre vigilancia. A ambos lados del Atlántico se entiende que necesitamos una causa probable y la aprobación judicial de la vigilancia. Sería hora de conceder estas protecciones básicas a los clientes de la UE de proveedores de servicios en la nube estadounidenses. Cualquier otro gran proveedor estadounidense de servicios en la nube, como Amazon, Google o Microsoft, podría verse afectado por una decisión similar en virtud de la legislación de la UE".

Cambios legislativos en el derecho al aborto en EEUU

En este apartado propongo un recorrido por algunas de las sentencias más significativas relacionadas con el derecho al aborto en los EEUU.

Pérez (2023) ,investigador de la Cátedra Martínez Marina de Historia Constitucional Universidad de Oviedo, resume los diferentes escenarios por los que ha pasado EEUU en cuanto a legislación relativa al aborto. Su repaso comienza en la década de los 60 del siglo XX, cuando unos veinte Estados contaban con legislación penal, en algunos casos, procedente del siglo XIX, que tipificaba como delito la práctica de abortos. Algunos movimientos trataron de reivindicar el papel de la mujer y su derecho a decidir libremente la interrupción de su embarazo.

El 7 de junio de 1965 el Tribunal Supremo dio uno de los primeros pasos, pues resolvió el asunto "Griswold contra Connecticut", declarando inconstitucional la criminalización del uso de anticonceptivos en el seno del matrimonio, por entender que ello vulneraba el derecho a la intimidad (i*dem*).

En esos mismos años, dos abogadas activistas llamadas Weddington y Coffee se lanzaron en busca de una demandante que diera rostro a su causa hasta que finalmente dieron con una de las muchas jóvenes embarazadas que en ese momento no deseaba continuar con la gestación. La iniciativa de dichas abogada implicaba pronunciarse sobre la constitucionalidad de la legislación penal de Texas, la cual consideraba delito la práctica de abortos (excluyendo tan sólo los llevados a cabo por prescripción facultativa en supuestos donde la continuación del embarazo hiciese peligrar la vida de la madre).

El 3 de marzo de 1970, Weddington y Coffee interpusieron en el juzgado federal de distrito norte de Texas la correspondiente demanda en representación de Norma Leah McCorvey (encubierta con el seudónimo de Jane Roe). Henry Wade, fiscal de distrito del condado de Dallas por aquel entonces, fue la parte demandada. El objetivo del asunto era aclarar si "la tipificación penal de la interrupción del embarazo cercenaba el derecho a la intimidad por conculcar derechos garantizados por la primera, cuarta, quinta, novena y decimo cuarta enmiendas constitucionales" (i*dem*).

La demanda contenía una pretensión declarativa (la inconstitucionalidad de la ley) y otra de condena, pues solicitaba al juzgado que se ordenase al estado de Texas abstenerse de ejecutar la legislación penal sobre el aborto. El 17 de junio de 1970, el juzgado dictó sentencia, estimando parcialmente la demanda: aceptó la pretensión declarativa ya que estimó inconstitucional la tipificación del aborto como delito, tanto por vulnerar la novena enmienda de la constitución como por la imprecisión de su contenido. Sin embargo la petición de condena fue desestimada.

Mediante apelación directa, el asunto llegó ante el Tribunal Supremo. En este momento dicho órgano se encontraba reducido a 7 miembros pero aceptó tramitar el asunto. Tras varias vistas orales en las que se oponían las opiniones de diferentes jueces la sentencia de "Roe contra Wade" se hizo pública el 22 de enero de 1973.

Su núcleo doctrinal se ubica en los apartados VIII y X, que tratan de alcanzar un equilibrio entre las posturas sostenidas por los jueces, entre ellos ideológicamente muy dispares. Pese a ello, todos coincidían en algo fundamental: que la Constitución de EEUU no contemplaba el derecho al aborto, y que este quizás podría adherirse al derecho a la intimidad. (Aquí vemos cómo convergen los dos grandes nucleos de este trabajo de Fin de Grado, pues este derecho a la intimidad relacionado con el derecho al aborto se encuentra extremadamente relacionado con la privacidad y la protección de datos, en este caso vinculados a su traslación a la esfera digital).

Por lo tanto, el caso "Roe contra Wade" de 1973 logró que el aborto fuera un derecho constitucional, pues reguló la capacidad de los estados de prohibirlo.

El caso "Doe contra Bolton" interpuesto en Georgia podría considerarse un "hermano siamés" del asunto "Roe contra Wade", incluso por el hecho de que su sentencia apareció el mismo 22 de enero de 1973. No obstante, se dio en Georgia. su principal diferencia es la forma en la que el Tribunal Supremo comparó el procedimiento de aborto con otros procedimientos quirúrgicos, haciendo hincapié en que la ley de Georgia regulaba el aborto de una forma que era inimaginable para otros procedimientos quirúrgicos (McGee, 2015).

Sandra Bensing, residente en Georgia en 1970, se quedó embarazada de su cuarto hijo y decidió abortar. En esta época en dicho Estado esta práctica estaba prohibida excepto en casos de peligro para la vida de la madre o la posibilidad de una lesión incapacitante, casos de violación o casos en los que era probable que el feto naciera con una anomalía grave o una discapacidad mental. Cada una de estas excepciones estaba acompañada de una carga de la prueba casi insuperable (por ejemplo una mujer violada debía documentarlo, y la familia o los amigos podían acudir a los tribunales para prohibirle el procedimiento). Además en dicho Estado se requería de la autorización de 3 médicos y un comité especial de personal del hospital para poder abortar. Asimismo la ley permitía realizar abortos únicamente a las residentes en Georgia.

Los abogados de la Sociedad de Ayuda Legal y la Unión Americana de Libertades Civiles reclutaron a Bensing para un caso de prueba y demandaron al fiscal general de Georgia, Arthur Bolton cuando un hospital se negó a proporcionar a Bensing un aborto terapéutico.

Los abogados argumentaron que no sólo se debería haber aprobado el aborto de "Mary Doe" (el seudónimo que adquirió la demandante) debido a una discapacidad psiquiátrica, sino que la ley infringía su derecho constitucional a la intimidad y a la autodeterminación e impedía a los profesionales médicos hacer su trabajo.

Finalmente la demandante acabó abortando en un hospital privado que no se encontraba sujeto a las mismas leyes que el público, pero aun así la demanda siguió adelante.

El Tribunal Supremo estableció el veredicto en el caso “Doe contra Bolton” y reiteró que pese a que "el derecho constitucional de la mujer a un aborto no es absoluto", era extremadamente restrictivo exigir que más de un médico o comités hospitalarios opinaran sobre la necesidad de dicho procedimiento. El Tribunal también consideró que los Estados no podían prohibir en ningún momento del embarazo los abortos que se considerasen necesarios para proteger la salud de la mujer, lo que podía incluir "todos los factores físicos, emocionales, psicológicos, familiares (y la edad de la mujer) relevantes para el bienestar de la paciente" (Peterson, 2022).

En 1988 y 1989, la Commonwealth de Pensilvania, dirigida por el gobernador Robert Casey, promulgó nuevas leyes sobre el aborto. Estas exigían una serie de condiciones a las mujeres que decidieran abortar. Entre estas disposiciones se encontraban requisitos como el consentimiento paterno en caso de ser menor, que la mujer casada notificara a su marido su intención de abortar y, que las clínicas proporcionaran determinada información a la mujer y esperaran 24 horas antes de realizar el aborto (McGee, 2015).

Antes de que ninguna de estas leyes entrara en vigor, Planned Parenthood of Southeastern Pennsylvania presentó una demanda contra el gobernador, protestando por la constitucionalidad de los estatutos. Planned Parenthood es una organización estadounidense sin ánimo de lucro que ofrece servicios de salud reproductiva, educación sexual, planificación familiar y de aborto en EEUU y en el mundo. Esta ha liderado la lucha por el acceso de las mujeres a la atención reproductiva en los EEUU durante más de un siglo. Sin embargo, no fue hasta 1992 con la interposición de esta querella y su

elevación hasta el Tribunal Supremo, cuando empezó a ser muy célebre, dando nombre a la histórica sentencia "Planned Parenthood contra Casey" (McGee, 2015; Sharp, 2022; Gamboa-Bernal, 2022).

Es importante recalcar que dicha sentencia llevó a revisar el caso "Roe contra Wade", considerando que había que mantener lo decidido previamente y que no era necesario cambiar la interpretación de la protección constitucional al aborto. Sin embargo, el Supremo hizo algunos cambios como anular el marco trimestral que tenía "Roe contra Wade" y remplazarlo por un marco de viabilidad por el cual "se podrían realizar abortos antes de que el feto alcanzara la posibilidad de vida extrauterina" (Gamboa-Bernal, 2022).

Llegando ya a nuestros días, el 24 de junio de 2022 se pronunció el caso "Dobbs contra Jackson Women´s Health Organization" que dirimía la constitucionalidad de la ley de Misissippi que prohibía el aborto libre tras la quinceava semana de gestación. En este caso el Supremo revertió su jurisprudencia de casi cinco décadas fundamentando su decisión en la no existencia de un derecho constitucional al aborto. Con este dictamen, el Supremo derogaba los precedentes de "Roe contra Wade" y "Planned Parenthood contra Casey" (Didier, 2022).

En efecto, en la sentencia "Dobbs contra Jackson Women's Health Organization"**,** de 213 páginas, se indica taxativamente: "La Constitución no confiere el derecho al aborto; Roe y Casey son anulados; y la autoridad para regular el aborto se devuelve al pueblo y a sus representantes electos" (Gamboa-Bernal, 2022).

Didier (2022) hace una división de los diferentes tipos de argumentos que el Tribunal Supremo de EEUU usó para declarar la validez constitucional de la ley de Mississippi. Estos son los siguientes:

1. Argumento lingüístico: este se acogió a que la Constitución no hace referencia expresa al derecho a abortar, por lo que quienes afirmen que protege tal derecho deben demostrar que este se encuentra de alguna manera implícito en el texto constitucional.

2. Argumento basado en la historia y la tradición: se prosiguió el razonamiento señalando que para considerarlo como un derecho mencionado de manera implícita en la Constitución, debería demostrarse que está "profundamente arraigado en la historia y

tradición", como así también que "es esencial para el esquema de libertad ordenada de la Nación".

3. Argumento basado en los precedentes: El Supremo también rechazó que el derecho al aborto pueda sustentarse en los precedentes, derogando los fallos "Roe contra Wade" y "Planned Parenthood contra Casey". Según su dictamen, ninguna de las dos sentencias fueron fundadas sobre precedentes aplicables al caso del aborto, ya que ninguno de ellos se refirió a la destrucción de lo que tales fallos denominan "vida humana potencial" y lo que la ley de Mississippi denomina "ser humano no nacido".

4. Argumento basado en el *stare decisis:* La sentencia destacó que la adhesión al precedente es la norma, pero a su entender, no es un mandato inexorable, por lo que desarrollaron diversos fundamentos para demostrar por qué razón tales fallos estaban "terriblemente equivocados". Entre los fundamentos, se invocaron argumentos vinculados con una crítica a los conceptos de "carga indebida", "confianza" y "viabilidad" propuestos en "Planned Parenthood contra Casey". Con relación a este último, señaló que la viabilidad depende de diversos factores que impiden determinar un límite claro y no discutible, tales como las instalaciones médicas, la edad gestacional, el peso del feto, la salud y nutrición de la mujer.

5. Argumento basado en la incompetencia del tribunal: se afirmó que "el aborto presenta un problema moral profundo sobre el cual los estadounidenses tienen puntos de vista profundamente contradictorios" y se añadió "es hora de hacer caso a la Constitución y devolver el tema del aborto a los representantes electos del pueblo", quienes en definitiva, según su opinión, deberían establecer la regulación sobre la prohibición o permisión del aborto.

6. Argumento basado en el test de constitucionalidad aplicable: El Supremo también se ocupó de responder un argumento invocado por algunos partidarios de declarar inconstitucional la ley de Mississippi, los cuales propusieron fundar el derecho al aborto en la Décimocuarta Enmienda. Al respecto la sentencia argumentó que "ni Roe ni Casey consideraron adecuado fundar el derecho a obtener un aborto en la cláusula de la igual protección de la Décimo Cuarta Enmienda".

A modo de síntesis, me parece interesante incluir abajo la siguiente tabla donde se establecen las características y diferencias de las 3 sentencias mencionadas

anteriormente: “Roe contra Wade”, “Planned Parenthood contra Casey “y “Dobbs contra Jackson Women’s Health Organization”:

Tabla 1. Cuadro comparativo de tres sentencias de la Corte Suprema de los Estados Unidos

	Roe vs. Wade	Planned Parenthood vs. Casey	Dobbs vs. Jackson Women's Health Organization
Año	**1973**	**1992**	**2022**
Antecedente	'Jane Roe', seudónimo legal de Norma McCorvey, presentó una demanda contra el fiscal de distrito de Texas, Henry Wade, arguyendo que las leyes de aborto de ese estado eran inconstitucionales.	Cinco clínicas de abortos demandaron que se derogaran las disposiciones de Pennsylvania relativas a restricciones al aborto, por considerarlas inconstitucionales.	Thomas E. Dobbs III, director del Departamento de Salud de Mississippi, recibió una demanda en 2018 de la única clínica de abortos de ese estado, para que se revisara la restricción del aborto en ese estado a partir de la semana 15 de gestación.
Alcance	En todos los estados es viable el aborto.	Sigue siendo viable el aborto en todos los estados.	Cada estado tiene la potestad de decidir.
Qué se decretó	Establecer el aborto como un derecho constitucional.	No se reconsideró el análisis histórico de los defectos en Roe vs. Wade.	Eliminar el aborto como un derecho constitucional.
Núcleo biojurídico	Interpretar que el derecho al aborto estaba protegido por la Constitución.	Mantenerse en lo decidido (*stare decisis*).	Demostrar que en la Constitución no se habla de derecho al aborto. La competencia de la decisión vuelve a los ciudadanos a través de sus legisladores.
Núcleo bioético	Se desconoció la dignidad del embrión humano, poniendo por encima la autonomía de la mujer.	Negar la pendiente resbaladiza y fortalecer la mentalidad antivida (cultura de la muerte).	Se reconoció la dignidad de la mujer y de cada embrión. Se fortalece una cultura a favor de la vida.
En la práctica	Se legalizó el aborto en los Estados Unidos.	Se extendió la práctica del aborto.	Se restringirá la práctica del aborto.
Actores clave	Bernard Nathanson, Betty Friedman, Larry Lader, Cyril Means, Sarah Weddington, Linda Coffee, Mildred Jefferson, Norma McCorvey ('Jane Roe') y Henry Wade.	Kathryn Kolbert y Linda J. Wharton.	Donald Trump y Lynn Fitch.
Votación	7 a 2	5 a 4	6 a 3
Jueces a favor	William O. Douglas, William J. Brennan Jr., Potter Stewart, Warren E. Burger, Thurgood Marshall, Harry Blackmun, Lewis F. Powell Jr.	Harry Blackmun, John P. Stevens, Sandra Day O'Connor, Anthony Kennedy y David Souter.	Samuel Alito, Neil Gorsuch, Brett Kavanaugh, Amy Coney Barrett, Clarence Thomas y John Roberts.
Jueces en contra	William Rehnquist y Byron White.	William Rehnquist, Antonino Scalia, Clarence Thomas y Byron White.	Stephen Breyer, Sonia Sotomayor y Elena Kagan.

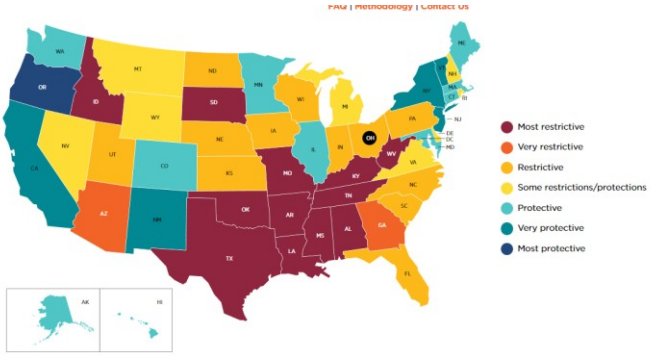
Fuente: Gamboa-Bernal, 2022.

Cabe destacar que años antes de esta sentencia varias autoras venían anticipándola, entre ellas Cynthia Conti-Cook (2020), quien en su artículo *“Surveilling the Digital Abortion Diary”*afirmaba: “Si el Tribunal Supremo de Estados Unidos vota a favor de anular el caso Roe contra Wade y un número de Estados apuestan por criminalizar el aborto, las investigaciones y enjuiciamientos de las embarazadas dependerán cada vez más de estos rastros digitales desprotegidos”. Volviendo pues al foco de este Trabajo de Fin de Grado, comprobamos cómo dos años antes de la sentencia del Supremo ya había advertencias sobre cómo la tecnología podría facilitar la vigilancia, persecución e investigación de aquellas mujeres embarazadas que buscaran o no acabar con su embarazo.

Según Vidality (2023) tras la sentencia “Dobbs contra Jackson Women’s Health Organization”, una docena de Estados donde gobierna el Partido Republicano han

aprobado legislaciones que restringen de manera casi absoluta el derecho al aborto, como es el caso en Alabama, Arkansas, Idaho, Oklahoma o Virginia Occidental, si bien en algunos casos queda pendiente una revisión judicial. En otros Estados, simplemente no hay acceso al derecho al aborto de ninguna manera: En el caso de Wisconsin, debido a la incertidumbre legal que rodea a la situación de los médicos que lo practiquen; y en Dakota del Norte, porque la única clínica que lo ejercía se trasladó a otro Estado.

El mapa elaborado por el instituto Guttmacher (2022) que incluyo a continuación (y que se actualiza cada día en la *web* de dicho instituto) refleja las políticas estatales vigentes a partir del 16 de abril de 2023.



Fuente: Instituto Guttmacher, 2022.

Actualmente ya hay 12 Estados con medidas muy restrictivas, por no decir prohibitivas, frente al aborto pero estas políticas aún no surgen efecto. Estos Estados serían: Virginia occidental, Kentucky, Tennesse, Alabama, Mississippi, Louisiana, Arkansas, Missouri, Texas, Oklahoma, Dakota del Sur e Idaho.

En la mayoría de estos Estados, donde las leyes se asemejan a la aprobada en Texas el 1 de septiembre de 2021 y se prohíbe abortar pasadas 6 semanas de embarazo, cuando todavía las propias mujeres no están seguras de estar embarazadas. Además, la ley de Texas incita a la ciudadanía a ejercer de policía contra sus propios vecinos/as y familiares, al ofrecer una recompensa de 10.000 dólares a quienes denuncien a cualquier persona sospechosa de ayudar a abortar. Pero todavía más dura es la ley de Alabama, que prohíbe el aborto en cualquier supuesto a partir del momento en que "se sabe que la mujer está embarazada", sin ninguna excepción.

Según el Instituto Guttmacher (2022), se da por seguro que 26 Estados son susceptibles de prohibir el aborto, mientras que otros 12 mantendrían la ley estatal , y finalmente 10

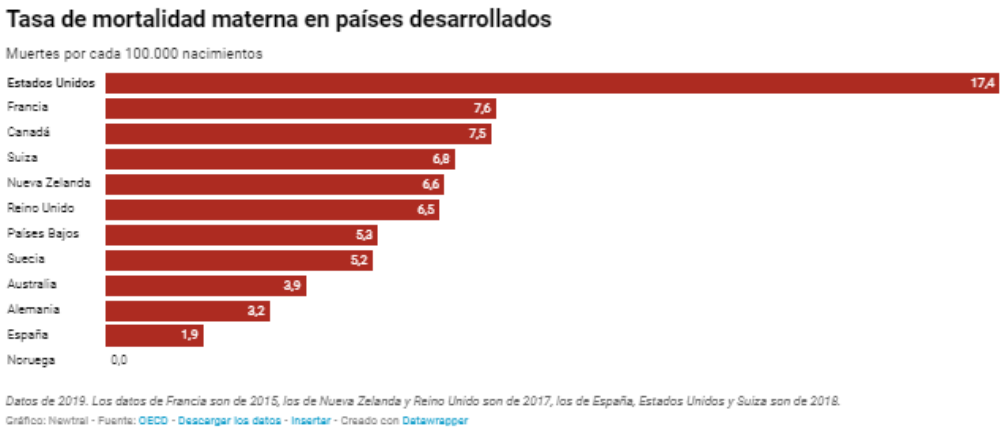
tampoco lo prohibirían pero su población no dispone de clínicas cercanas capaces de atender a pacientes de otros Estados.

Newman (2021) corrobora esta información y señala que, aunque desconoce cómo se aplicarán las leyes, lo que es seguro es que millones de personas que no tenían nada que ocultar se enfrentan ahora a la posibilidad de incluso ir a la cárcel por un tema relacionado con su salud reproductiva. Asimismo la autora apunta que el cifrado integral será esencial para su autodefensa.

En este punto, me gustaría poner el acento en que Amnistía Internacional (2022) sostiene que actualmente EEUU posee la mayor tasa de mortalidad materna de los países desarrollados y en particular en los Estados con leyes más restrictivas sobre el aborto.

Según la OMS (1992) la mortalidad materna "es la muerte de una mujer mientras que está embarazada o dentro de los 42 días de haber terminado un embarazo, independientemente de la duración y la localización del embarazo, por cualquier causa vinculada o agravada por el embarazo o su manejo, pero no por causas accidentales o incidentales".

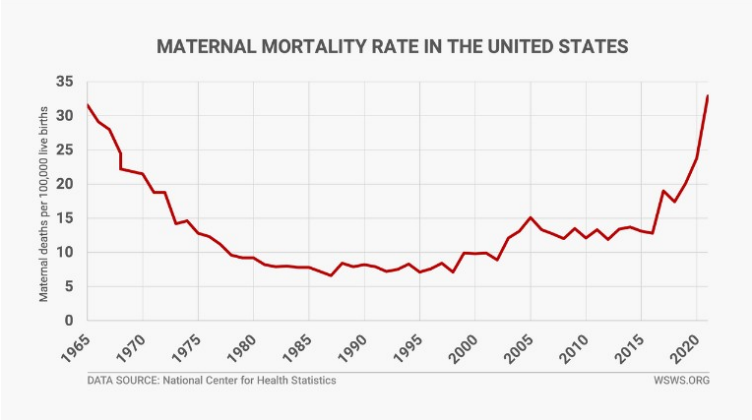
Asimismo, la OCDE (Organización para la Cooperación y el Desarrollo Económicos) comparte que la tasa en EEUU es de 17,4 muertes por cada 100.000 nacimientos y coincide que esta es la más alta entre los países desarrollados, según las estadísticas de dicha organización en 2019. Además, el país norteamericano duplica la tasa del segundo país con una mayor mortalidad materna, Francia, que tiene una tasa de 7,6. En el caso de España, la ratio es nueve veces menor.



Fuente: OCDE, 2019.

Por su parte, Patrick Martin (2023) elabora la siguiente gráfica con datos del Centro Nacional de Estadísticas de Salud. El autor sostiene que las muertes maternas en Estados Unidos aumentaron en un 40% en 2021, según un nuevo informe de los Centros para el Control y la Prevención de Enfermedades. Martin destaca que la cifra de muertes maternas aumentó de 754 en 2019 a 861 en 2020 y 1.205 en 2021. "La tasa de mortalidad materna, de casi 32 por cada 100.000 nacimientos, regresó al nivel de 1965, un retroceso enorme de más de medio siglo" describe el autor.

La gráfica que incluyo continuación muestra cómo desde el año 2015 ha habido un crecimiento en la tasa de mortalidad materna en EEUU:



Fuente: Martin, 2023.

En conclusión, Martin (i*dem*) apunta lo siguiente:

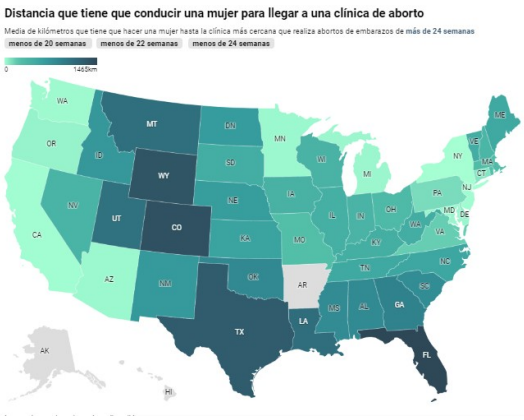
> "El abandono sistémico de las mujeres pobres y de clase trabajadora se verá agravado en gran medida por las consecuencias bárbaras de la campaña fascistizante que se está librando contra el derecho al aborto. En condiciones en las que el embarazo pone cada vez más en peligro la vida de las mujeres, la ultraderecha está buscando nuevas leyes y procedimientos para imponer el embarazo forzado, incluso a mujeres que se enfrentan a importantes peligros de salud".

Para Amnistía Internacional (2022) el gran problema que supone brindar a los gobiernos de cada Estado la libertad de decidir sobre este aspecto es principalmente la gran desigualdad que esto genera entre las mujeres del país hasta el punto de que vivir en un Estado u otro puede marcar definitivamente su futuro.

Es destacable comentar que hace simplemente unos años casi todas las mujeres estadounidenses podían vivir a unas pocas horas de una clínica para abortar de forma

legal. Pero una vez revocado el derecho constitucional las clínicas han ido cerrando progresivamente, empezando por los Estados menos permisivos, provocando esto que grandes extensiones de territorio queden sin cobertura de estos centros médicos. En este sentido, Nash (2023) afirma:"Ahora que el Tribunal Supremo de EEUU ha revocado `Roe contra Wade', el acceso a los servicios de aborto será prácticamente inexistente en muchos Estados, forzando a las pacientes a viajar largas distancias para acceder a proveedores en Estados que sí apoyen los derechos al aborto".

El siguiente mapa muestra la distancia que tendría que recorrer una mujer embarazada (según de las semanas de las que esté) para poder acudir a una clínica de aborto en EEUU actualmente. A principios del mes de junio de 2022, una mujer que vivía en Texas tenía que recorrer de 80 a 240 km de media (por trayecto) para abortar de manera legal en una clínica especializada, de acuerdo con la investigación de *The New York Times* en la que se analiza el mapa del aborto en Estados Unidos. Tras la derogación de "Roe contra Wade", ahora deberá recorrer 402 km de media si es un embarazo de menos de 20 semanas, aproximadamente el doble que antes, de acuerdo con las estadísticas de Guttmacher.



Fuente: Instituto Guttmacher, 2022

Ante esta dificultad, hay casos como el de la doctora Rebecca Gomperts, la cual fundó Aid Access, una organización que ha estado ofreciendo misoprostol y mifepristona por correo en todo el país a partir de marzo de 2018. Aid Access informó que atendía principalmente a mujeres pobres y de bajos ingresos procedentes de los Estados con menos acceso al aborto.

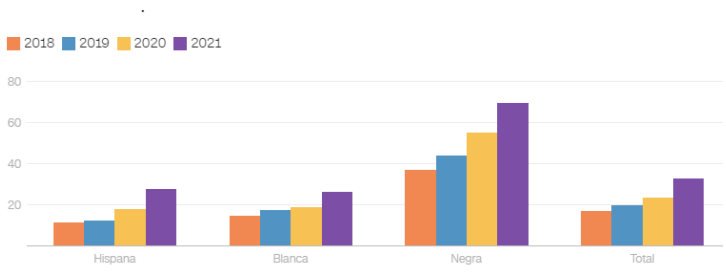
Esto llamó la atención de la Administración de Alimentos y Medicamentos (FDA, por sus siglas en inglés), que emitió una carta de cese y desistimiento en marzo de 2019.

Desafiando a la FDA, Aid Access ha seguido proporcionando acceso a abortos con medicamentos a través de su consulta en línea y programa de pedidos por correo (Conty-Cook, 2020).

Por su parte, Peterson (2022) alude apunta en su artículo para *National Geographic* que, según las estadísticas del Centro de Control de Enfermedades, anteriormente a las sentencias Roe y Doe, había unos 130.000 abortos ilegales al año en EEUU, mientras que tras ellas esa cifra se vio reducida a 17.000 en 1975. El número de mujeres que se determinó formalmente que habían muerto a causa de un aborto ilegal descendió de 39 en 1972 a tres en 1975.

Howard (2023) también comparte datos del Centro Nacional de Estadística publicados en marzo de 2023 por los Centros para el Control y Prevención de Enfermedades de EE.UU, según los cuales el número de mujeres que murieron por causas maternas en EEUU aumentó a 1.205 en 2021, lo que representa un fuerte incremento respecto a años anteriores: 658 en 2018, 754 en 2019 y 861 en 2020. Junto a ello, Howard menciona disparidades raciales significativas en la tasa de mortalidad materna en los EEUU. Así, en 2021 la tasa de mortalidad materna de mujeres negras fue de 69,9 por cada 100.000 nacidos vivos,mientras que la de las mujeres blancas estuvo en 26,6 por cada 100.000 (Howard, 2023).

En la siguiente gráfica elaborada por el Centro Nacional de Estadísticas de Salud de los Centros para el Control y la Prevención de enfermedades de EEUU se puede observar cómo la tasa de mortalidad materna entre las mujeres negras fue más del doble del promedio en EEUU.



Fuente: Stiles y Vu, 2023.

Por lo tanto tras el análisis de dichos datos se observa cómo tras la derogación de la sentencia “Roe contra Wade” las mujeres en territorio estadounidense se pueden

encontrar con dificultades aún mayores para poder decidir sobre su cuerpo, hasta el punto de poner en peligro sus propias vidas.

Colisión entre legislación represiva de los derechos de las mujeres y aplicaciones invasivas de su privacidad

Tras la derogación de la sentencia "Roe contra Wade" por el Supremo de EEUU la situación de muchas mujeres en ese país ha dado un giro de 180 grados, pues ahora sus decisiones se encuentran obstaculizadas y su futuro afectado por una gran incertidumbre. Ello se vio reflejado tempranamente con la aparición en Instagram y TikTok de múltiples publicaciones que mezclaban las etiquetas #roewade y #periodtrackingapps, lo cual pone ya de relieve que estos conceptos no están aislados y pueden converger de tal manera que han levantado sospechas entre las usuarias.

Sin embargo esto no es nada nuevo, pues tiempo atrás ya se podía suponer que este momento llegaría. Por ejemplo, Newman, redactora *The Wired*, ya proponía en mayo de 2022 en su artículo titulado *"How to Protect Your Digital Privacy if Roe v. Wade Falls"* algunos conceptos de privacidad que adoptar si los derechos en EEUU dejaban de estar garantizados tras las decisiones del Supremo. En él, habla sobre la existencia de organizaciones como Digital Defense Fund y Electronic Frontier Foundation que ofrecen guías detalladas sobre los pasos que puedes dar para proteger tu privacidad digital mientras investigas y buscas datos o servicios relacionados con el aborto.

Según el *New York Times,* cuando en mayo de 2022 la decisión del Supremo fue filtrada por primera vez, muchas mujeres estadounidenses alertadas por las redes sociales, pasaron a la acción y se desinstalaron la *app* de menstruación de sus teléfonos (Hill, 2022).

Tras esta investigación fueron varias las mujeres estadounidenses que alertaron por Twitter sobre el peligro que se avecinaba tanto antes como tras la derogación de dicha sentencia. Así, Gina Neff, socióloga y directora del Centro Minderoo para la Tecnología y la Democracia de la Universidad de Cambridge, publicó dos tuits relacionados donde declaraba, por un lado, "Ahora, y me refiero a este instante, borra todo el rastreo digital de todas las aplicaciones de seguimiento menstrual. Por favor", y a continuación añadía "Lo digo como alguien que escribe sobre política y economía del autoseguimiento: borra estas aplicaciones ahora".

Fuente: Neff, 2022.

Tras captar la atención de su comunidad, esta experta decidió hacer lo que se llama un "hilo" [5]de Twitter (varios tuits conectados de una misma persona) explicando lo que hasta ese momento sabía sobre la delicada situación a la que se enfrentaban. En este Neff (2022) compartió que fuerzas y cuerpos de seguridad ya se estaban centrando en las búsquedas de Google de píldoras abortivas**,** relacionándolas con mensajes de texto y bases de datos de ADN para enjuiciar a las mujeres por abortos. Además dio algunos consejos para aquellas mujeres que desearan proteger su privacidad.

Esta información la corrobora Newman (2021), quien explica que el uso de aplicaciones, motores de búsqueda y navegación por Internet son actividades que pueden exponer datos personales, lo que supone un gran reto a la hora de controlar el flujo de información personal cuando la gente investiga o busca abortos. A menudo, cuando una persona busca abortar, ya ha generado datos que podrían revelar su estado de salud.

Por otro lado la usuaria *@evacide*, o por su nombre Eva Galperin, directora de ciberseguridad de Electronic Frontier Foundation (EFF) escribió en su muro de Twitter: "Si estás en Estados Unidos y estás usando una aplicación de seguimiento menstrual, hoy es un buen día para eliminarla, antes de crear un tesoro de datos que se utilizará para procesarte si alguna vez decides abortar".

5. Hilo de Twitter de Gina Neff disponible en el siguiente enlace: https://twitter.com/ginasue/status/1540354137304760321

Fuente: Galperin, 2022.

Por otro lado, la periodista estadounidense conocida en Twitter como *@_megconley*, escribió lo siguiente en su perfil: "La mayoría de aplicaciones de seguimiento menstrual comparten tus datos con terceros. Esto significa tu ciclo, los síntomas que registras, todo. En un mundo post Roe, ello puede ser usado como evidencia contra ti o contra gente que te asista en un aborto. Borra las *apps*"

Fuente: Conley, 2022.

Asimismo *@jkbibliophile*, escritora en EEUU, simplemente comparte con su comunidad de Twitter: "Borra tus aplicaciones de seguimiento menstrual hoy"

Fuente: Khoury, 2022.

Sin embargo, para algunas expertas borrar las aplicaciones no es suficiente. Así,Andrea Downing, fundadora de la organización sin ánimo de lucro Light Collective e investigadora de seguridad y privacidad, afirma:

> "Muchas de las actividades de generación de datos que ya se han llevado a cabo en el pasado ya están ahí fuera (…) Puedes eliminar aplicaciones de aquí en adelante, desactivar los servicios de localización, dejar de usar una aplicación de fertilidad, y todos esos son grandes pasos. Pero también es razonable que la gente no pueda recordar todo, todo el tiempo. Las poblaciones de pacientes son susceptibles y vulnerables en línea, y tenemos que centrarnos en protegerlos." (Citada en Newman, 2022)

En esta misma línea, Natasha Singer (*@natashanyt*) cita el tuit de Neff para añadir a continuación: "Las aplicaciones de seguimiento menstrual pueden verdaderamente tratar con datos de salud sensibles. Pero, incluso si pudieras borrar los datos de tu cuenta de la aplicación de fertilidad, los servicios de seguimiento de la localización pueden ubicar a las personas que fueron a Planned Parenthood y cuánto tiempo estuvieron allí"

Fuente: Singer, 2022

Por otro lado, tanto en entrevistas en medios generalistas como en diversas investigaciones y estudios los expertos han manifestado diversos posicionamientos sobre las implicaciones que pueden abrirse tras el dictamen de "Dobbs contra Jackson Women's Health Organization".

Para empezar, quiero enfatizar cómo Fowler y Hunter (2022), redactores del *Washintong Post*, aseveran que la decisión del Tribunal Supremo de revocar el derecho al aborto convierte años de advertencias sobre la vigilancia digital en una realidad innegable. Los autores afirman que de la noche a la mañana búsquedas en Google,

información de ubicación,aplicaciones de seguimiento de periodos y otros datos podrían usarse como evidencia de un delito.

Ciertos datos son un blanco fácil para citaciones u órdenes judiciales, y muchas compañías tecnológicas no son claras a la hora de aclarar qué tipo de información estarían dispuestas a entregar. Por ejemplo, según los redactores de *The Washintong Post (idem*), Google informa que recibió más de 40.000 citaciones y órdenes de registro en los EEUU en la primera mitad de 2021.

Para Cooper Quintin (citado en Bhuiyan, 2022), tecnólogo del grupo de derechos digitales Electronic Frontier Foundation, el mayor problema será que toda esa información que se está recopilando sobre ubicación, salud menstrual y embarazos ahora se utilizará para encontrar y procesar a las personas que pueden estar buscando estos servicios.

Por otro lado, Kat Green (citada en Sabin, 2022), directora ejecutiva de Abortion Access, afirmó lo siguiente: "Si sabes que estás haciendo algo que es arriesgado, sé prudente sobre cómo hablas en Internet, o no hables de ello en absoluto". Por su parte, , Erin Matson (citada en i*dem*), cofundadora y directora ejecutiva de Reproaction, un grupo de defensa que educa sobre los abortos autogestionados, señaló: "Nuestras vidas están en línea, nuestras conversaciones están en línea, y hay gente con una agenda que quiere utilizarlo".

La doctora en Ciencias políticas y profesora en la City University de Londres. Jimena Valdez (citada en Cadenas, 2022), explica que algo que no tiene precedentes es el nivel de vigilancia y control que se puede ejercer a partir de la tecnología. "En aquellos Estados donde está prohibido abortar, sin duda todas las aplicaciones y el mundo digital van a ser clave para perseguir y controlar a las mujeres".

La ya citada Cynthia Conti-Cook (2020), en un análisis legislativo publicado en la revista de la Universidad de Baltimore, apuntó que no solo se trata de la criminalización del aborto a través de los datos de salud de las mujeres, sino de otras conductas vinculadas a la gestación que en el futuro podrían ser tipificadas como delito, como automedicarse o no medicarse, beber alcohol o fumar tabaco. Estas, según la abogada, son decisiones individuales que podrían ser criminalizadas en algún momento y que también podrían ser vigiladas digitalmente.

La abogada y experta en Ciberseguridad Paloma Llaneza (citada por Peña, 2022) expone que en 2021 el Consejo Internacional de Responsabilidad Digital (IDAC) descubrió que "los rastreadores de menstruación enviaban información personal sin cifrar o que compartían datos con terceros sin revelarlo (de forma previa) en sus políticas de privacidad". Llaneza menciona *apps* muy conocidas como Flo, que fue investigada por haber prometido mantener los datos de sus usuarios protegidos para luego compartirlos con Facebook y Google. Curiosamente la experta recuerda que estas *apps* "pueden sustituirse fácilmente por un calendario en papel".Evan Greer (citado en Garamvolgyi, 2023), subdirector del grupo de defensa sin fines de lucro Fight for the Future, comenta que otra forma de intentar proteger los datos de salud sensibles es utilizar únicamente aplicaciones que almacenen los datos de forma local y no en la nube.

Otros autores como Córcoles (citado en Meseguer, 2022), director de posgrado de Desarrollo de Aplicaciones Web, abren sus miras más allá de las fronteras de EEUU para insistir en que se debe mirar más allá de las *apps* menstruales yel **caso "**Roe contra Wade", ya que según él: "estamos ante un cambio de paradigma, los datos ya no tienen fines económicos, sino que ahora pueden conllevar lindes penales".

En este sentido, Meseguer (*idem*) subraya que el negocio silencioso de la compra y venta de datos se puso en manifiesto cuando Facebook compró la aplicación WhatsApp por más de 21.800 millones de dólares, o cuando Google adquirió YouTube por 1.650 millones de dólares.

Según los expertos, ni Facebook ni Google desembolsaron esas cantidades por la estructura tecnológica de estas plataformas, sino que lo que realmente marcaba la diferencia era el número de usuarios que tenían detrás. Asimismo Córcoles (citado en *idem*) diferencia entre que Facebook trate los datos y los explote para insertar publicidad segmentada, a que les dé acceso a terceras empresas sin el consentimiento del usuariom siendo este último punto el que abre el debate de las *apps* menstruales.

Greer (citado en Garamvolgyi, 2023), por su parte, apunta que no hay que centrarse solo en este tipo de *apps*, pues cree que estas no son la única forma que la tecnología tiene de conectar a alguien con un aborto. Este autor invita a ponerse en la siguiente situación: alguien está sentado en la sala de espera de una clínica que ofrece servicios de aborto y está jugando a un juego en su teléfono, esa aplicación podría estar recopilando datos de

ubicación. Además añade que lo mismo podría hacer Google Maps o cualquier otra *app* que requiera de permisos de ubicación. Sin embargo, el autor no piensa que toda la responsabilidad debería recaer únicamente en los individuos, pues cree que las empresas y los legisladores deberían actuar para proteger a las personas .

La asesora de políticas tecnológicas Blum-Dumontet (citada en *idem*) también destacó que en su opinión estas *apps* deberían ser las que cambiaran sus prácticas y no las usuarias. La asesora cree que, para empezar, dichas *apps* nunca deberían haber poseído tantos datos y que si estas se limitaran a almacenar la información necesaria no estaríamos teniendo este debate en este momento. Pese a todo, la visión idealista de esta autora le hace pensar que estas *apps* aún pueden recapacitar y ver que no han actuado de la mejor manera. En este sentido, Blum-Dumontet cree que la única forma de que estas puedan sobrevivir es que se vuelvan dignas de confianza mejorando su política de privacidad y dándole a las usuarias un mayor control sobre sus datos.

Otras autoras no son tan optimistas y piensan que los datos pueden encontrarse alojados en cualquier sitio, incluso en lugares que ni las propias *apps* de menstruación controlen, incluso si ese fuera su compromiso verosímil. En esta línea, Jason Hong (citado en Torchinsky, 2022, profesor de la Facultad de Informática de la Universidad Carnegie Mellon, advierte que los datos que una usuaria ingresa en una aplicación de seguimiento de períodos podrían llegar mucho más allá del teléfono o la aplicación que está utilizando. "Es realmente difícil entender cómo se utilizan sus datos y dónde se comparten porque podrían ser muchos terceros, y esos terceros también pueden revender a otros terceros ", dice Hong. "Sus datos podrían estar en toda la Red en este momento. Y es realmente difícil rastrear lo que está sucediendo" .

La periodista y activista Marta Peirano (citada en Serrano, 2019), por su parte, asegura que los datos sobre salud que introducimos en estas *apps* podrían estar en cualquiera sitio. Además añadió lo siguiente: “La aplicación más popular en Estados Unidos se llama Flo y le vende datos a Procter and Gamble y a Bayer. Su rival, Glow, dice que le parece inmoral vender publicidad segmentada, pero comparte sus datos con laboratorios. Los datos son comprados, reempaquetados y vendidos por empresas de *data brokers* al mejor postor, y la relación entre los datos que filtramos y sus consecuencias es más sistémica que específica, como un problema medioambiental”.

Otros autores se centran en puntualizar aspectos más concretos, como es el caso de Chloé Berthélémy (citada en Gonzalo y López, 2022) quien apunta que la tecnología es capaz de facilitar que la Policía ejerza vigilancia discriminatoria en función de la raza, el género y la clase pero con un falso barniz de objetividad. Para Berthélémy, cómo resultado, el derecho a un juicio justo y la presunción de inocencia de determinados grupos minorizados se ven aún más socavados .

Cabe mencionar asimismo a Kristina Durante, psicóloga social que lleva años estudiando el factor biológico sobre las decisiones de compra en el marco del llamado *marketing* biológico. En uno de dichos estudios Durante descubrió que las mujeres se sentían más inclinadas a comprar determinados productos en función del momento del ciclo menstrual en el que se encontrasen. "Básicamente nos movemos entre el apareamiento y el anidamiento: desde el día 1 en que nos baja la regla hasta el día 15 es cuando las mujeres tienen mayor nivel de estrógenos" añade la experta (Durante, citada en Serrano, 2019).

Además de puntualizar en ámbitos como la raza y la biología hay estudios que se centran en la financiación de ciertas *apps,* información que también puede ofrecer respuesta a algunas de nuestras preguntas. Este es el ejemplo de FEMM *app*, la cual resultó estar financiada y controlada por inversores católicos antiabortistas, según una investigación del diario británico *The Guardian* en 2019. Este estudio afirmó que dentro de esta *app* supuestos profesionales médicos, entre ellos dos médicos chilenos de la Pontificia Universidad Católica, alertaban a las usuarias de los efectos nocivos de las píldoras abortivas y realizaban verdaderas campañas en contra del aborto (Pozo, 2019).

The Alliance (2021), organización enfocada a la defensa de los derechos reproductivos en EUUU, complementa esta información en su informe *"The CPC Industry as a Surveillance Tool of the Post-Roe State".* En él revela cómo algunos autodenominados "grupos próvida" han creado "una sofisticada red nacional digital, financiada por el gobierno, que ficha a las personas embarazadas con bajos ingresos que puedan o no estar considerando un aborto, registra su información médica y personal sensible y la comparte con organizaciones antiaborto que almacenan grandes cantidades de datos sin salvaguardas de privacidad" (Murtha, 2022).

En el año 2016,*The Wall Street Journal,* publicó información sobre cómo algunas empresas tecnológicas compartían datos con Facebook con fines publicitarios. Una de

estas aplicaciones era Flo. La información compartida tenía un identificador que permitía conectar a las usuarias con su perfil en la red social, para así mostrar en sus muros anuncios que les pudieran interesar (Serrano, 2019).

Un estudio muy representativo en este sentido es el realizado en 2022 por la organización Eticas Foundation, centrada en el asesoramiento y auditorías tecnológicas, titulado "Mi cuerpo, mis datos sus normas". En él la fundación analizó la política de datos y el uso de datos íntimos de doce de las aplicaciones de seguimiento menstrual más populares, incluyendo Mi calendario menstrual, Flo, Clue o Cycles**.**. La conclusión del estudio no dejaba lugar a dudas: la mayoría de dichas aplicaciones comparte datos con terceros para fines comerciales. "La recopilación de datos sobre el ciclo menstrual y especialmente el hecho de compartirlos con terceros, resulta especialmente peligrosa, ya que puede suponer una vía de acusación y persecución de aquellas personas que se estén planteando recurrir a esta práctica" (Eticas Foundation, 2022).

Para comprobar cuánto garantizaban la protección de la intimidad las investigadoras responsables del estudio tuvieron en cuenta cinco parámetros: si estas contaban con una política de privacidad de fácil acceso, si eran claras y comprensibles, si era necesario otorgarles permisos invasivos, si recopilaban datos personales innecesarios y si compartían estos datos con terceros. Precisamente los resultados que obtuvieron provenientes de estas dos últimas variables fueron de lo más alarmantes. Tan solo una de las *apps* analizada, Womanlog**,** no vendía ni compartía datos. My Fitness, Period Tracker y Calendario menstrual resultaron ser las menos respetuosas con la información que aportaban las usuarias.

"Cuatro de las doce aplicaciones estudiadas no cuentan con una política de privacidad de fácil acceso y cinco de ellas utilizan una estructura y un lenguaje complejos y poco intuitivos", apuntan desde Eticas Foundation (*idem*). Además, recuerdan que en 2021 la aplicación Flo fue sancionada por romper con lo recogido en su política de privacidad y vender los datos de sus usuarias a empresas como Facebook o Google.

Sin embargo Flo no es un caso aislado de filtración de datos. Un informe del año 2020 titulado "Out of Control" realizado por el Consejo de Consumidores de Noruega reveló que las aplicaciones de seguimiento de fertilidad, Clue y MyDays, entre otras enfocadas a otras temáticas, compartían datos con los gigantes de la tecnología publicitaria Facebook y Google (Forbrukerradet, 2020). Entrando en detalles, dicho informe expone

que los datos compartidos incorporan ubicaciones de GPS y direcciones IP, así como detalles personales sobre género, sexualidad y opiniones políticas (Romero, 2020).

El estudio de Eticas Foundation advierte de que el tráfico de datos de las aplicaciones sobre menstruación y su difusión con terceros supone que puedan utilizarse no solo con fines comerciales, sino también en procedimientos judiciales relacionados con el aborto en países como EEUU, donde recientemente se ha revocado este derecho.

Ante esta situación, varios grupos activistas han publicado guías ciudadanas para evitar que la información íntima pueda ser controlada cuando se pretende abortar o recibir atención sanitaria reproductiva. Entre estas organizaciones se encuentran el Digital Defense Fund, la Repro Legal Helpline y la Electronic Frontier Foundation (Cadenas, 2022).

Un caso que extrapola todo lo comentado anteriormente a la realidad es el caso de una madre y una hija en el estado de Nebraska. En agosto de 2022 saltó a medios extranjeros y también españoles la noticia de que Facebook había entregado a las autoridades estatales estadounidenses una conversación privada entre una madre y su hija después de recibir una orden judicial por un caso de aborto. Esta conversación resultó ser decisiva a la hora de presentar una acusación contra ellas. En efecto, la policía de Norfolk comenzó a investigar a Celeste Burgess y su madre, Jessica Burgess, a finales de abril de 2022 después de que una supuesta amiga de la joven señalara a las autoridades que la había visto tomar una píldora abortiva. La acusada afirmó que había dado a luz prematuramente a un feto muerto y que su madre le había ayudado a enterrar el cuerpo. Después que ambas fueran acusadas, la policía continuó investigando y obtuvo mensajes de Facebook entre madre e hija que parecían hacer referencia a la píldora abortivas y la quema "de la evidencia" (O'Brien y Duffy, 2022).

Como apuntaba arriba, un elemento probatorio decisivo provino de la solicitud de los investigadores para que Facebook les proporcionar información sobre las cuentas de Celeste y su madre. Los datos proporcionados por la compañía el 9 de junio de ese año incluyeron más de 250 MB de datos relacionados con el perfil de Celeste y más de 50 MB de datos sobre la cuenta de la madre (*idem*).

El portavoz de ese momento de Meta (la empresa matriz) defendió la acción de Facebook diciendo que nada en las órdenes válidas que recibieron de la policía local a principios de junio, antes de la decisión del Supremo, mencionaba el aborto. Además añadió que los documentos judiciales indican que la policía estaba investigando en ese momento la supuesta quema ilegal y el entierro de un bebé muerto (*Idem*).

Después de la solicitud inicial a Facebook, los fiscales presentaron una orden de allanamiento adicional el 16 de junio que solicitó evidencia de búsquedas en Internet o la compra de medicamentos utilizados para el aborto espontáneo, entre otras cosas. Trece dispositivos tecnológicos pertenecientes a la madre y la hija también fueron incautados en respuesta a esa orden, según los documentos judiciales.

En junio, Celeste y Jessica fueron acusadas de un delito grave de actos prohibidos con restos esqueléticos humanos, así como de dos delitos menores ligados a la ocultación de la muerte de otra persona y a la provisión de información falsa. La madre también fue acusada de dos delitos graves adicionales, por "inducir" a un aborto ilegal y por "realizar" un aborto sin tener licencia de médico. Nebraska en ese momento prohibía los abortos después de 20 semanas, una ley que ha estado vigente desde antes de que Roe v Wade fuera revocado (O'Brien y Duffy, 2022).

Tanto Celeste como su madre se declararon inocentes y se mantienen en la espera de una respuesta, pero en paralelo el gobernador republicano de Nebraska, Jim Pillen, ha aprobado una ley estatal que prohíbe el aborto tras las 12 semanas de embarazo, lo que viene a confirmar el retroceso de los derechos reproductivos de las mujeres con el paso de los años (Caballero, 2023).

Resultados

Tras comparar las políticas de privacidad de las 6 *apps* escogidas, y ello tanto en su versión para la UE como en la propia para EEUU, se ha podido saber que estas son capaces de recoger datos relacionados con: ubicación, código de país de la tarjeta SIM, dirección IP, información sobre *Hardware* y *Software* del dispositivo, información personal (nombre, correo electrónico, *ids* de usuario), información financiera (historial de compra de App store o Google Play), información de salud y *fitness*, mensajes, fotos

y videos, interacciones/actividad en la *app*, navegación web (historial), información y rendimiento de aplicaciones e *ids* de dispositivo o de otro tipo.

Tras saber qué datos generales podían recoger pasamos a analizar qué permisos son los más comunes entre la muestra. Esta información se ha obtenido gracias a que antes de descargar una de estas *apps* en Google Play o App Store aparece una serie de información esquemática sobre los datos que se recogen y con qué finalidad. En resumen, se observa que dos de las *apps* de la muestra (Flo y Clue) recogen datos de ubicación por el simple hecho de usar las *app* y el resto te da la opción de poder activarla para ofrecerte distintos servicios.

En cuanto al código de país de la tarjeta SIM, Meet you es la única que afirma recopilarlo. Si hablamos de dirección IP, todas menos Calendario Menstrual guardan datos sobre la misma directamente. Algo común es que todas las aplicaciones de la muestra recogen datos sobre *Hardware* y *Software* del dispositivo en el que se encuentran instaladas y ninguna de ellas lo niega.

Sin embargo, eso no es todo, pues hay más información de interés para este tipo de *apps, c*omo por ejemplo la personal o financiera. En cuanto a la personal, suelen pedir a las usuarias el nombre y/o el correo electrónico, aunque solo en Clue esto sería un requisito indispensable. En cuanto a información financiera, se dividen en mitad y mitad, pues 3 de ellas recopilan información sobre el historial de compras de App Store o Google Play (Meet You, Flo y Alerta Periodo).

En lo relativo a información sobre salud y *fitness*, se ha descubierto que esta podría ser transparente para la mitad de aplicaciones de la muestra (Flo, Clue y Meet You), siendo en el resto algo opcional. Los mensajes de texto en diferentes aplicaciones también parecen ser una opción de recopilación de información, aunque a priori no se especifica qué tipo de mensajes o en qué *apps* serían recopilados. Tan solo una de ellas establece este requisito como obligatorio antes de su descarga (Mi Calendario Menstrual).

El contenido multimedia que alberga nuestro teléfono puede cederse de manera opcional a 3 de las 6 *apps* (Flo, Meet You y Alerta Periodo). Las interacciones que tiene la persona usuaria en la aplicación es información requerida por todas, menos una (Alerta Periodo). El historial de navegación, al parecer, solo es revisado por *Meet You* aunque, cuando se indaga en sus políticas de privacidad, como se hará más adelante,

estas *apps* suelen hacer uso de herramientas de medición como Google Analytics, lo que podría generar una revisión del motor de búsqueda. Por último, todas las *apps* acceden a información y rendimiento de aplicaciones y a *ids* de dispositivo o de otro tipo sin ningún tipo de excepción y sin ser esto una opción.

Tanto en Google Play como en App Store, antes de la descarga del servicio tratan de explicar con qué finalidad recogen cada tipo de dato, distnguiendo entre: funcionalidad de la aplicación, análisis de comunicaciones del desarrollador, publicidad o *marketing*, prevención de fraudes, seguridad y cumplimiento, personalización y gestión de cuentas.

Además, es importante destacar qué *apps* muestran explícitamente antes de su descarga que compartirán datos con terceros, pues solo dos de ellas lo admiten *a priori* (Meet You y Alerta Perido). Sin embargo, tras revisar las políticas de privacidad de cada una, todas afirman hacerlo en ocasiones. Otro rasgo compartido por todas ellas es que justifican la recopilación de datos con la mejora de la experiencia del usuario al interactuar con la *app.* Me gustaría destacar que en todo momento la responsabilidad de lo que pueda ocurrir recae en el usuario.

Otro dato importante es que antes de descargar cualquiera de esta *app*, excepto Meet You, informan de que los datos se cifran en tránsito, esto es, de que estos permanecen "ocultos" por el camino desde el emisor al destinatario.

Por otro lado, se ha querido ir un poco más allá y analizar dentro de cada *app* qué datos puede proporcionarle una usuaria para obtener a cambio un "mejor seguimiento". Todas te dan la opción de apuntar tu peso, y dos de ellas, Clue y Meet You, te ofrecen registrar tu altura. En cuanto al estado de ánimo, todas poseen diferentes sistemas para registrarlo mediante emoticonos, palabras clave, etc.

La temperatura corporal es algo que puedes apuntar en todas menos en Flo. Además en todas puedes llevar un registro de síntomas relacionados con el ciclo menstrual o el embarazo, fecha de inicio y fin ciclo menstrual, cantidad de sangrado, días de ovulación, tipo de flujo vaginal y periodo fértil.

Meet You te permite apuntar incluso el apodo y el género del bebé esperado. La actividad o el comportamiento sexual es algo que puedes anotar en todas menos una (Alerta Periodo). Los orgasmos que tiene la usuaria parecen interesarle a Mi Calendario Menstrual y a Alerta Periodo, mientras que la masturbación puede ser de interés para

Calendario Menstrual. Saber si la usuaria tuvo sexo con protección o sin ella es algo que puedes apuntar en todas menos en Meet You, incluso se puede anotar en qué posiciones has estado durante el sexo en Alerta Periodo. Los recordatorios de la llegada del periodo o si existe retraso son algo que registran todas. Además si tomas tratamientos anticonceptivos puedes registrarlo en 4 de las apps: Mi Calendario Menstrual, Flo, Clue y Calendario Menstrual.

Junto a ello, las heces parecen revelarse como algo también relevante, ya que 2 de las *apps* piden este dato (Clue y Meet You). Por otro lado, todas menos Meet You recogen datos sobre acné o manchas en la piel, horas de sueño/insomnio, solo Clue hace lo propio con el apetito, los dolores de cualquier tipo/estado físico y el estado del cabello, . En cuanto a los antojos, parecen interesar a todas menos Meet You y Calendario Menstrual, al tiempo que Alerta Periodo atiende en exclusiva al número de pasos diarios y los tratamientos de fertilidad, Clue hace lo propio con el tipo de actividad de ocio y Flo con las pruebas de embarazo y la ingesta de alcohol. Más allá, todas menos dos preguntan por tratamientos anticonceptivos,, Flo y Clue lo hacen sobre el tipo de deporte que has realizado, Clue y Calendario Menstrual se interesan por los medicamentos tomados y finalmente solo Clue permite conectar datos con otras personas en el foro ubicado dentro de la *app*.

Ahora bien, tras revisar la información que ofrecen las plataformas de descarga previamente a la instalación de una *app* y la información que puede proporcionar una usuaria mediante su empleo, se decidió profundizar en todas y cada una de las políticas de privacidad.

Es de estos documentos de donde se ha podido extraer la siguiente información: todas y cada una de las *apps* seleccionadas afirman compartir datos con proveedores de servicios y con servicios de terceros, y solo Alerta Periodo niega que al compartir esos datos con terceros la persona usuaria queda inmediatamente sometida a las políticas de privacidad que estos tengan. Todas sin excepción comparten datos con fines publicitarios y cuatro de ellas afirman compartirlos con compañías de análisis o estadística, con Flo y Clue especificando que entre los fines de compartir con terceros hay propósitos científicos. Es igualmente cierto que todas reconocen que, en virtud del reglamento RGPD, las usuarias pueden solicitar la eliminación de los datos aunque hay excepciones en cuatro de las seis aplicaciones. En este sentido, hay que en cuenta que

los datos eliminados podrían mantenerse en servidores de terceros al cederlos a dos de las aplicaciones (Mi Calendario Menstrual y Calendario Menstrual).

En cuanto a la eliminación de datos, tan solo dos de las *apps* afirman que estos desaparecerían por completo (Clue y Alerta Periodo). El resto elude posicionarse sobre la cuestión, o incluso expresa que depende de la situación podrían mantenerlos por un tiempo. Todas menos una (Calendario menstrual) comparten que las usuarias, acorde con la legislación europea, tienen derecho a solicitar los datos personales que se han recopilado y a recibir una copia de los mismos. Por otro lado, es curioso que tan solo dos de ellas mencionan abiertamente dónde se encuentran los servidores de las *apps* (Clue y Meet You), aunque saber este dato tampoco es de vital importancia si desconocemos donde se encuentran los de terceros con los que comparten los datos.

La mitad de *apps* de la muestra especifican que los datos no son vendidos (Mi Calendario Menstrual, Flo y Clue), mientras que el resto no menciona el tema o expone abiertamente que sí realizan esta práctica en alguna ocasión. Más de la mitad de las *apps* hace una distinción entre datos que se recopilan automáticamente y entre los que la usuaria acepta mientras utiliza la *app*, siendo Clue y Calendario Menstrual las que no lo hacen.

Algo que destacar es que tres de las *apps* (Mi Calendario Menstrual, Clue y Meet You) informan de que si inicias sesión con una cuenta de un tercero, se podrá recopilar información automáticamente.

Todas excepto Clue afirman que si la empresa se sometiera a una fusión, traspaso, venta de activos o financiación externa los datos serían compartidos con la otra parte. Algo que destacar es que solo la mitad afirma avisar a las usuarias de que se han efectuado cambios en la política de privacidad (Mi Calendario Menstrual, Flo y Meet You), con una de ellas defendiendo que son las usuarias quienes deben mantenerse informadas y revisar la política de vez en cuando para asegurarse.

Solo Mi calendario Menstrual expone que los datos se almacenan en la nube únicamente si se decide hacer copia de seguridad, y que de lo contrario estos se mantendrían tan solo en el dispositivo. En la misma línea, todas menos una (Alerta Periodo) mencionan en su política la transferencia de datos entre diferentes regiones y reconocen que los datos podrían estar ubicados fuera del estado, provincia, país, u otra jurisdicción

gubernamental donde las leyes de protección de datos pueden diferir de las de su jurisdicción.

Algunas de ellas ofrecen la opción de no registro, lo que a priori podría parecer la solución para que ninguno de tus datos corriera peligro, o por lo menos para que si se comparten lo sean de forma "anónima", pese a lo cual cabe recordar cómo Lessig (2009) destaca que "aquel relativo anonimato de los `viejos tiempos´ actualmente ha desaparecido en la práctica". En efecto, el catedrático de Harvard subraya que dondequieraque naveguemos en Internet, queda registrado por la dirección IP o las *cookies*: "Se nos conoce por nuestros clicks de ratón". Ello se podría extrapolar a los *clicks* dentro de una *app,* Sin embargo Clue y Calendario Menstrual hacen hincapié en que los datos que comparten son anónimos.

En este punto, es fundamental recordar que, según el RGPD, a veces los datos personales pueden ser anonimizados, cifrados o presentados con un seudónimo, sin excluir la posibilidad de que se puedan utilizar para volver a identificar a una persona. En este caso el RGPD los sigue considerando datos personales y por lo tanto se inscriben en el ámbito de aplicación de dicho reglamento.

Quiero aclarar que en todas estas políticas parece resultar evidente que es **a** la usuaria a quien se transfiera la responsabilidad casi exclusiva de desactivar la mayoría de permisos aceptados automáticamente por el simple hecho de descargar la *app.*

En todas las *apps* menos una (Alerta periodo) se explica que existe una relación directa con Google o que se hace uso de alguna de sus funciones **(**Google Fit, Google Analytics,Google AdSense, AdMob de Google, Google Ads O Google reCAPTCHA,Google LLC**).** Al margen de ello, Flo y Meet You afirman que, **e**n algunas situaciones, contratan a otras compañías para procesar los datos personales en el nombre de la *app*. Entre estos "procesadores" destacan AWS , Cloudflare, Auth0, BigID, ElasticSearch ,SendGrid EEUU, SurveyMonkey EEUU o, Looker EEUU.

Cuatro de las aplicaciones de la muestra (Flo, Clue, Meet You y Calendario Menstrual) especifican que trabajan con *apps* FLYER y sus socios integrados con fines de *marketing* y promoción *(*Pinterest, Google Ads, Apple Search Ads, La red de *marketing* de Facebook y otros). A su vez, la mitad (Clue, Meet You y Calendario Menstrual) utiliza herramientas como Braze, Firebase, Sentry y Adjust (algunas de ellas con sede

en la UE y otras en EEUU). Flo, Meet You y Calendario Menstrual afirman precisar de servicios de Amazon. Finalmente, en caso de disponer de un dispositivo Apple, Mi Calendario Menstrual, Flo y Clue afirman que se podrían importar datos de Apple *HealthKit*.

Junto a lo anterior, cabe reseñar que todas las aplicaciones analizadas menos una (Alerta Periodo) dejan un correo de contacto y que la última actualización de estas políticas se realizó a lo largo de 2022, excepto la de Meet You que se realizó en 2023. Si profundizamos en esta cuestión, constatamos que solo algunas plataformas como Mi Calendario Menstrual dan la posibilidad de retirar el consentimiento de muchos de los permisos, si bien en ese caso dejan claro que no se podría hacer uso de la *app:* "Tiene derecho a retirar su consentimiento para usar sus datos personales. Si retira su consentimiento, es posible que no podamos proporcionarle acceso a ciertas funcionalidades específicas del Servicio". [6]

Como se puede observar, estas políticas contienen varias grietas que llevan a que ni las propias compañías garanticen al 100% su seguridad. No en vano, muchas de estas compañías aseveran en sus políticas de privacidad que no pueden controlar todos los "peligros de Internet". A continuación muestro algunos párrafos extraídos literalmente de los documentos de las políticas de privacidad de las aplicaciones seleccionadas:

"La seguridad de su información es importante para nosotros, pero tenga en cuenta que todos los métodos de transferencia y almacenamiento de datos basados en Internet no son 100% seguros. Existen riesgos asociados con cualquier transferencia de información personal. Seguimos trabajando para desarrollar técnicas adicionales para proteger su información, pero es difícil para nosotros garantizar la seguridad absoluta de Internet".[7]

"La Compañía utiliza salvaguardas físicas, administrativas y técnicas para preservar la integridad y seguridad de sus datos. Desafortunadamente, la transmisión de información a través de Internet y plataformas móviles no es completamente segura. Cualquier transmisión de información personal es bajo su propio riesgo". [8]

6 Mi Calendario Menstrual, 2022. Privacy Policy. http://simpledesign.ltd/privacy/my_calendar.html

7Mi Calendario Menstrual, 2022. Privacy Policy. http://simpledesign.ltd/privacy/my_calendar.html

8 Calendario Menstrual, 2022. Privacy Policy. https://www.simpleinnovation.us/my-calendar/privacy-policy

“Cualquier información (que incluya datos personales) que comparta en cualquier área de la comunidad en línea o discusión en línea está abierta por diseño a la comunidad de Flo. Debe pensar detenidamente antes de publicar cualquier dato personal en cualquier foro público. Lo que publique puede ser visto, revelado o recopilado por terceros y puede ser utilizado por otros de maneras que no podemos controlar o predecir, incluso para contactarlo con fines no autorizados”.[9]

“Con respecto a los Estados Unidos, específicamente, es poco probable que la información que tanto nosotros como nuestros procesadores manejamos sea sujeto de investigación por parte de algún organismo en EE. UU. que aplique las leyes que podrían obligar a un procesador a entregar información personal. Sin embargo, no se puede descartar el riesgo de dicha divulgación”.[10]

“Tenga en cuenta que, aunque nos esforzamos por proporcionar seguridad razonable para la información que procesamos y mantenemos, ningún sistema de seguridad puede evitar todas las posibles infracciones de seguridad”. [11]

Además de estas formulaciones de renuncia de responsabilidad sobre la seguridad, todas las aplicaciones afirman que sus datos serían compartidos si así se les requiriese legalmente. Aquí dejo algunas citas textuales obtenidas de los documentos de políticas de privacidad de algunas de las *apps* analizadas:

“Compartimos información con las agencias de aplicación de la ley, las autoridades públicas u otras organizaciones si la ley nos exige que lo hagamos o si dicho uso es razonablemente necesario” [12]

“La *app* puede compartir algunos datos personales en las siguientes circunstancias especiales: en respuesta a citaciones, órdenes judiciales o procesos legales, en la medida

9 Flo, 2022. Política de privacidad. https://flo.health/es/politica-de-privacidad
10 Clue, 2022. Política de Privacidad de Clue. https://helloclue.com/es/privacidad

11 Alerta Periodo, s.f. Privacy Policy. https://gpapps.com/support/privacy-policy/

12 Mi Calendario Menstrual, 2022. Privacy Policy. http://simpledesign.ltd/privacy/my_calendar.html

permitida y restringida por la ley (incluido el cumplimiento de la seguridad nacional o los requisitos de aplicación de la ley)" [13]

Clue expone que indirectamente si que alguno de sus terceros aliados podría compartir datos en ciertas ocasiones: "Google analiza esta información para ofrecerle a Clue informes sobre el uso del sitio web y el uso de los servicios en línea asociados. De acuerdo con los términos del servicio analítico de Google, Google también podría transferir esta información a terceros siempre que la ley así lo requiera o en caso de que Google contrate a empresas externas para procesar los datos" [14]

En cuanto a las leyes a las que cada una de las *apps* afirma someterse, tras profundizar en sus políticas se ha podido saber que solo la mitad menciona el RGPD y lo que se deriva de él (Mi Calendario Menstrual, Flo y Clue), mientras que la otra mitad menciona a la CCPA (Mi Calendario Menstrual, Clue y Calendario Menstrual). Más allá, solo dos (Flo y Clue) mencionan y hacen hincapié en la situación de EEUU y en que podría afectar su política actual de privacidad.

Además de las aclaraciones mencionadas, en estos documentos las *apps* dejan caer que una vez tus datos son compartidos, debes atenerte a las políticas de privacidad de esos terceros. La mayoría incluso dejan enlaces de estos documentos para que el usuario pueda entrar y leer cada una de las políticas a las que se atiene. En definitiva parece que al hacer "un pacto" con la *app* haces a su vez otro con toda una lista de empresas desconocidas que prestan servicio a la que tú has descargado inicialmente.

Por ejemplo, Meet You especifica resumidamente que la recogida y el tratamiento de datos personales por parte de los proveedores y prestadores de servicios están sujetos a sus propias políticas de privacidad y, por lo tanto, no se aplican a la presente política de privacidad.

Incluso en el caso de Clue se especifica que los mismos terceros pueden transferir a otros terceros: "Google también podría transferir esta información a terceros siempre

13 Flo, 2022. Política de privacidad. https://flo.health/es/politica-de-privacidad

14 Clue, 2022. Política de Privacidad de Clue. https://helloclue.com/es/privacidad

que la ley así lo requiera o en caso de que Google contrate a empresas externas para procesar los datos".[15]

Cada una de estas *apps* parece atenerse a una legislación distinta aunque suelen hacer referencia las normas más comunes del RGPD o Ley de California, como especifico a continuación:

Para empezar, Mi calendario menstrual, fundada en Reino Unido, tiene presente el RGPD y la Ley de California a la hora de desarrollar su política. En ella se explican por encima las bases legales para procesar datos bajo RGPD entre las que se encuentran las siguientes: consentimiento por parte del usuario, ejecución de un contrato, obligaciones legales, intereses vitales, intereses públicos o legítimos.

Además, explica los derechos de las usuarias de la *app* bajo el RGPD y especifica que aquella persona que se encuentre dentro de la UE tiene derecho a solicitar acceso a los datos personales almacenados, la corrección de dichos datos, la eliminación de los mismos, etc. Aquí se deja claro que aunque te descargues una *app* de procedencia europea, van a existir diferencias y desigualdades dependiendo en qué territorio te encuentres durante su uso. La política de esta *app* comparte que la usuaria tiene derecho a presentar una queja ante una autoridad nacional de protección de datos vinculada a la recopilación y el uso de datos personales.

Mi Calendario Menstrual también habla de la CCPA (Ley de California) y especifica que si el usuario es residente en California tiene una serie de derechos incluidos como puede ser el derecho de notificación, el de acceso y el derecho de solicitud, además de derecho a decir no a la venta de datos personales y a eliminarlos (solo los que se han recopilado en los últimos 12 meses). Eso cambia con el RGPD, ya que este no tiene en cuenta el citado plazo de 12 meses y contempla asimismo la posibilidad de pedir a la compañía que no venda sus datos personales a terceros.

Como se puede observar existe desigualdad entre una persona que hace uso de la *app* en California y en cualquier otro estado de EEUU, lo cual también queda patente en el caso de Calendario menstrual, aplicación estadounidense propiedad de Simpleinnovation,,

15 Clue, 2022. Política de Privacidad de Clue. https://helloclue.com/es/privacidad

que menciona también la Ley de California, el RGPD y algo sobre la EEUU. En cuanto a la CCPA, trata alguna de las ventajas que tendrían las ciudadanas de California como: solicitar el envío de las categorías de información personal que recopilan sobre el usuario, corregir o eliminar la información personal que recopila la *app* o recibir una copia de la misma. Resulta curioso que esta *app* en concreto hace el siguiente apunte: "No vendemos ni compartimos ningún dato de usuario. Sin embargo, podemos proporcionar ID de publicidad desde su dispositivo a los anunciantes. Según ciertas leyes, incluida la ley de California, la provisión de ID de publicidad puede constituir una venta de información de la persona".[16]

También hace la siguiente mención: "Los destinatarios de los datos se autocertifican regularmente en la UE/Escudo de privacidad de EEUU (si se encuentra en EEUU) o puede haber acordado con nosotros aplicar el Controlador de cláusulas modelo de la UE". Ello evidencia que, pese a que el Escudo de Privacidad fuera invalidado por el TJUE en julio de 2020, se mantuvo la validez de las Cláusulas Tipo para no dejar en un vacío total las transferencias internacionales de datos.

Alerta periodo*, app* californiana, menciona las legislaciones de California y EEUU en sus políticas. En esta *app,* al parecer, todos los usuarios se someten a la ley de California "Estos Términos y condiciones se regirán por las leyes del Estado de California sin tener en cuenta sus disposiciones sobre conflictos de leyes. Usted y la compañia acuerdan someterse a la jurisdicción exclusiva de los tribunales ubicados dentro del condado de Riverside, California, para resolver cualquier asunto legal que surja de estos Términos y Condiciones".[17]

La política de esta *app* es muy escueta y poco clara. Relacionado con EEUU tan solo menciona lo siguiente: "La Aplicación puede estar sujeta a controles o restricciones a la exportación por parte de los Estados Unidos u otros países o territorios. Usted se compromete a cumplir todas las leyes y normativas de exportación estadounidenses e internacionales aplicables. Estas leyes incluyen restricciones sobre destinos, usuarios finales y uso final". Por lo tanto, deja claro que la empresa hará lo que tenga que hacer y que la usuaria puede estar tranquila mientras "cumpla la ley".

16 Calendario Menstrual, 2022. Privacy Policy. https://www.simpleinnovation.us/my-calendar/privacy-policy
17 Alerta Periodo, s.f. Privacy Policy. https://gpapps.com/support/privacy-policy/

Clue, procedente de la UE, tiene una de las políticas más completas ya que habla de legislaciones de EEUU, de la CCPA y, por supuesto, del RGPD, que se evidencia como la principal ley reguladora de esta *app* en este extracto de su política de privacidad: "Las bases legales que regulan el procesamiento de los datos anteriormente mencionados están en el Artículo 6, sección 1(b) del Reglamento General de Protección de Datos Europeo (RGPD). Clue puede usar estos datos con el fin de mejorar la aplicación de Clue, los servicios que te ofrecemos y prevenir el uso abusivo de nuestro servicio. De acuerdo con el Artículo 6, sección 1(f) del RGPD, consideramos que tenemos un interés legítimo de ofrecer un servicio funcional y sin errores".

Sin embargo, Clue se apresura a puntualizar que su política de transferencia de datos a EEUU se rige en estos momentos por la excepción articulado en torno a las cláusulas contractuales estándar: "El Tribunal de Justicia de la Unión Europea declaró inválido el Escudo de Privacidad UE-EEUU, del cual dependíamos, así como también muchas otras compañías, para asegurar un nivel suficiente de protección de datos. Hemos entrado en Cláusulas Contractuales Estándar con todos los vendedores de herramientas de procesamiento de datos (procesadores de datos) que no pertenecen al EEE (Espacio Económico Europeo), para asegurar un nivel adecuado de protección de datos, de acuerdo con el Art 46 del RGPD".

Más adelante, Clue especifica en qué consisten dichas cláusulas y cómo les ayudan, aunque también mencionan sus limitaciones :

-"Las Cláusulas Contractuales Estándar nos ayudan a implementar un nivel adecuado de protección de datos entre Clue y nuestro procesador, el cual accede a seguir reglas estrictas de protección de datos. Sin embargo, estas no obligan a los órganos gubernamentales del país externo al EEE en el cual opera nuestro procesador. En algunos casos, los gobiernos pueden ejercer vigilancia que va en contra de los principios de protección de datosde las leyes europeas. Por lo tanto, el ambiente legal de los países que no perteneces al EEE, en particular el de Estados Unidos, crea el riesgo de que un procesador pueda verse legalmente obligado a actuar en contra de las obligaciones contenidas en las Cláusulas Contractuales Estándar y entregar información personal a funcionarios del gobierno local, con limitaciones para Clue y para tí como individuo de buscar ayuda legal en contra de estas acciones".

Al referirse a su política respecto a la legislación de EEUU, Clue hace la siguiente afirmación: "Con respecto a los Estados Unidos, específicamente, es poco probable que la información que tanto nosotros como nuestros procesadores manejamos sea sujeto de investigación por parte de algún organismo en EE. UU. que aplique las leyes que podrían obligar a un procesador a entregar información personal. Sin embargo, no se puede descartar el riesgo de dicha divulgación".

Me gustaría destacar la poca seguridad que transmiten este tipo de mensajes. No en vano, la *app* se ve obligada a dar una explicación sobre qué hace para mitigar el riesgo y se justifica con los siguientes argumentos "Primero, escogemos cuidadosamente nuestros procesadores. No trabajamos con procesadores que tengan sede en países que nos generen preocupación frente a las leyes de privacidad. Seguimos la guía del Comité Europeo de Protección de Datos sobre medidas contractuales y técnicas adicionales para garantizar un nivel adecuado de privacidad en diferentes situaciones"

Para finalizar esta aplicación menciona que sus funciones no pondrían desarrollarse sin los servicios provenientes de EEUU y que, por lo tanto, no hay desvinculación como tal: "Seguimos observando los desarrollos normativos y las mejores prácticas en esta área. Mientras tanto, algunos procesadores por fuera del EEE, en particular los procesadores con sede en EE. UU., son una parte vital de nuestro servicio, y no podemos brindártelo sin ellos, tal como se describe en las secciones 6, 7 y 8 de esta política de privacidad".

En cuanto a la ley de California, Clue se limita a mencionar algunos derechos exclusivos para residentes en dicho Estado, como por ejemplo que se permitirá solicitar una lista escrita de las categorías de información personal compartida con terceros a quienes Clue ha revelado información personal durante el año anterior.
Algo que destacar es que en este documento se especifica que tanto la aplicación de Clue como el sitio *web* también utilizan servicios externos de análisis y de seguimiento como Google Analytics, Google Adsense y Braze, todos con servidores en EEUU. En el caso de este último, se especifica que no es posible renunciar ya que es una herramienta esencial y necesaria para prestar los servicios.

En Flo, *app* creada en Reino Unido, las legislaciones mencionadas corresponden tanto a EEUU como a la UE. Flo afirma en ambos casos que los datos personales recopilados se transfieren y se procesan en los EEUU (donde rige la ley de EEUU) y otros países

(donde rigen las leyes de esos países), siendo curioso que no se menciona específicamente a cuáles se refiere. Flo asegura que la protección ofrecida por las leyes de los EEUU y de esos otros países misteriosos puede no ser igual que la legislación de la jurisdicción a la que algunas de sus usuarias estén sujetas.

La empresa hace una mención especial a la UE, el EEE y el Reino Unido, donde afirma que los datos personales están protegidos por el RGPD y la Ley de Protección de Datos de 2018. Aun así, advierte que en algunos países puede que no necesariamente tengan el mismo nivel de protección de sus datos personales. Flo afirma aplicar las cláusulas habituales del contrato y seguir las resoluciones de de la Comisión Europea.

Flo está certificada por el Marco del Escudo de Privacidad UE-EEUU. y el Marco del Escudo de Privacidad Suiza-EEUU, mencionando que se adhiere a los principios del Escudo de Privacidad para los Datos Personales transferidos hasta el 16 de julio de 2020, es decir el mismo día que se invalidó el mismo. A partir de ese momento, Flo afirma transferir los datos fuera de la UE aplicando cláusulas contractuales estándar, sin aludir en ningún momento a la Ley de California.

En cuanto a las leyes mencionadas en las políticas de Meet You, *app* radicada en Singapur, es destacable que solo se habla de la de California y muy por encima: "En el caso de los residentes en California, si revelamos sus datos personales a terceros con fines de *marketing* directo en el futuro, tendrá derecho a solicitar que le proporcionemos (a) una lista de las categorías de datos personales que hemos revelado a terceros con fines de *marketing* directo durante los 12 meses anteriores, y (b) la identidad de esos terceros".

"Usted entiende y acepta que los datos personales que recopilamos pueden ser almacenados y utilizados en servidores alquilados por la empresa en Singapur, según sea necesario para prestarle los servicios, y que tomaremos las medidas razonables para proteger sus datos personales y cumpliremos con los requisitos legales aplicables del país receptor. Al hacer clic en "Aceptar" esta política y utilizar el Servicio, usted consiente la transferencia de dichos datos personales fuera de su país y región" .[18]

18 Meet You, 2023. Política de Privacidad. https://www.meetyouintl.com/home/privacy.html

Esta aplicación deja claro en una de sus secciones que el acuerdo que se realiza entre el usuario y la *app* además de cualquier disputa que surja en relación con la ejecución del acuerdo se regirá por las leyes de Singapur.

En síntesis, tras abordar la presente investigación es posible afirmar el descubrimiento de que las únicas políticas que cambian según las busques desde EEUU o desde la UE son Flo y Meet You. En efecto, quien escribe esto ha realizado las pertinentes comprobaciones al respecto usando redes privadas virtuales (VPN, por sus siglas en inglés) ubicadas tanto en California, como en Nueva York, Dallas y Los Ángeles, tras lo cual se ha constatado que la política de privacidad de Flo disponible en los EEUU tiene como fecha de última actualización el 14 de septiembre de 2022. En contraste, que si buscamos la información con la ubicación real de Málaga donde me encuentro, se comprueba que esta cambió posteriormente, en concreto el 6 de diciembre de 2022.Asimismo se comprueba que las usuarias de la aplicación radicadas en EEUU ven sus datos traspasados de Google Fit mientras que en la UE dichos datos proceden de Google Health Connect.

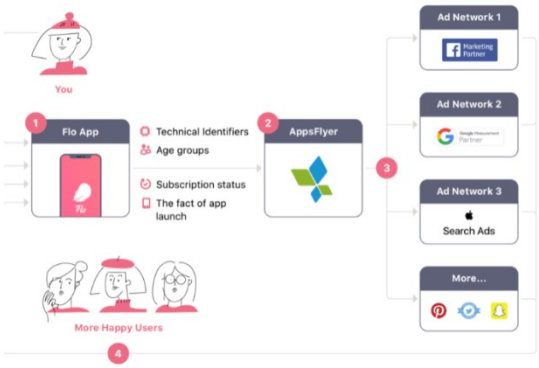
Otra de las grandes diferencias es que el uso de la *app* desde EEUU tiene como límite mínimo de edad los 13 años, en contraste con el Espacio Económico Europeo y Reino Unido, donde esta barrera se eleva hasta los 16 años. Con todo, algo común al marco regulador de la UE y de EEUU es que algunas funciones quedan restringidas hasta cumplir 18 años.

Otra disimilitud es que en la UE no hay ni rastro de aquellos "procesaores" que por contra están a la orden del día en EEUU, con empresas como BigID Inc, HubSpot Inc, ElasticSearch Inc, Looker Data Sciencies, Inc, EE.UU, Amplitude Inc, Customer Thermometer, Tecton Inc, PayPal (Europe) o AppsFlyer Inc.

En cuanto a aspectos comunes de estas políticas se encuentra por ejemplo la siguiente ilustración esquemática e ilustrativa de cómo utilizan AppsFlyer los socios integrados de Flo para fines de comercialización y promocionales.

AppsFlyer es una plataforma de atribución y análisis de *marketing* móvil del llamado *Software* como servicio (modelo de distribución de *Software* donde el soporte lógico y los respectivos datos que maneja se alojan en los servidores de un proveedor, cuyo acceso es a través de Internet) con sede en San Francisco, California. Asumiendo que

esta transferencia se hace de manera automática, se observa cómo aunque la *app* procede de Reino Unido trabaja con servicios californianos entre otros:



Fuente: Flo, 2022.

El número uno hace referencia al momento en el que una persona se convierte en usuario de Flo y con su consentimiento comienza a compartir los siguientes datos personales con AppsFlyer y sus socios integrados para fines de *marketing* y promocionales.

En segundo lugar, Flo envía los datos personales a AppsFlyer, que los analiza y proporciona informes e información sobre cómo optimiza las campañas promocionales.

Al mismo tiempo (indicado como número tres) AppsFlyer envía sus datos a algunos de sus socios integrados (Pinterest, Google Ads, Apple Search Ads, red de *marketing* de Facebook y algunos otros) con el fin de encontrar a otras personas en diferentes plataformas, incluidos las páginas *web* de redes sociales.

En cuarto lugar, proporcionan al presente y a los nuevos usuarios información sobre Flo, predicciones exactas del ciclo, información sobre el significado de las señales de su organismo e información fiable sobre su salud.

Por último, Flo ofrece opciones de exclusión voluntaria, por las cuales se puede retirar su consentimiento o excluir voluntariamente que se compartan los datos personales con AppsFlyer para fines de *marketing* y promocionales en cualquier momento modificando los ajustes del dispositivo en iOS o Android.

Sin embargo, como en todo hay excepciones, y es que hay que tener en cuenta que también se usan las AppsFlyer para integrar los datos entre la página *web* y la aplicación en relación con los usuarios que se incorporen, y de aquí no se podrá excluir voluntariamente el procesamiento por parte de AppsFlyer de los datos personales para estos fines.

En relación con Meet You, *app* procedente de Singapur, al igual que con Flo al comprobar mediante VPN estadounidense (de California, Nueva York, Dallas y Los Ángeles) las políticas de privacidad observamos leves diferencias. Por ejemplo con la VPN de Málaga la fecha de la última actualización de la aplicación es del 16 de mayo de 2023 mientras con la estadounidense es el 13 de abril del 2023.

Bajo las políticas que encontramos en la UE vemos cómo los datos que se proporcionan a Meet You son: correo electrónico, cuentas de terceros, contraseñas, apodos y fecha de nacimiento. Las excepciones por las que dicen que compartirán datos con terceros son las siguientes: cumplir con una obligación o solicitud legal, como una orden judicial, una citación u otro proceso legal; tratar asuntos relacionados con la seguridad o el fraude; en caso de emergencia que implique la muerte de una persona, riesgo de lesiones personales graves o cualquier riesgo de daño a los niños, todo ello siempre que la entidad que solicita los datos personales tenga jurisdicción válida para acceder a sus datos personales, etc.

Además se menciona que está permitida una retirada de consentimiento si el usuario considera que la empresa no usa sus datos para salvaguardar sus intereses legítimos. En la medida en que lo exijan las leyes y reglamentos aplicables, el usuario puede retirar cualquier consentimiento que haya proporcionado previamente.

En el caso de EEUU, los datos adicionales que recoge la aplicación a diferencia de lo que se aplica en la UE son los siguientes: número de teléfono y número de identificación de suscriptor móvil internacional IMSI e ID de Android.

Otra discrepancia es que en la política obtenida con VPN estadounidense no hay ninguna mención a restricción de edad. Sin embargo cuando accedemos a la misma política desde España vemos cómo Meet You se compromete a proteger la privacidad de los niños: “El servicio no está destinado al uso por parte de niños y no recopilamos conscientemente datos personales de niños menores de 13 años. El servicio no recoge

datos personales de ninguna persona que, según la empresa, sea menor de 13 años". Me parece interesante destacar el empleoo del adverbio "conscientemente".

Asimismo, los SDK en la política de EEUU son diferentes, ya que se menciona SDK Bugly, SDK QQ, SDK We chat, SDK Weibo, SDK Alipay, SDK Amap, etc. Cada uno con su correspondiente política de privacidad. Mientras que en la UE los SDK son diferentes: AppsFlyer SDK, Firebase SDK, GoogleSignIn SDK, Facebook SDK, Mi Push SDK y Google Mobile Ads SDK.

Algunos rasgos comunes en los documentos de privacidad de EEUU y la UE son las excepciones a la hora de no pedir permiso previo para compartir, transferir y divulgar públicamente la información personal. En efecto, esta *app* afirma que no pedirá permiso si la información solicitada trata un tema directamente relacionado con la seguridad nacional, pública o intereses públicos, investigación criminal, acusación, juicio y ejecución de sentencias.

Esas serían las diferencias encontradas entre las diferentes políticas de privacidad. Ahora me gustaría hacer hincapié en un punto clave y este es el ya apuntado arriba en torno al llamado SDK (S*oftware Development Kit*, o equipo de desarrollo de *Software*).

El concepto de SDK se refiere a un paquete de herramientas que ayuda al funcionamieno de la *app* (Bax *et al.,* 2021). En otras palabras, se trata de un conjunto de herramientas de desarrollo de *Software* que permite a un desarrollador crear una aplicación informática para un sistema concreto. Se cree que parte del éxito de las aplicaciones se debe a su forma de recopilar datos personales en nombre de SDK de terceros, al igual que las *cookies* en sitios *webs.* Estos ayudan a que si, por ejemplo, se quieren añadir servicios de ubicación a una aplicación, traducción automática u otro tipo de funciones, en vez de crearlas de cero se puede incorporar un SDK a la *app* para así proporcionar esos servicios.

Por ejemplo para crear una aplicación para Android se necesita SDK de Android. Otros SDK se utilizan para obtener información sobre el uso de tu aplicación a través de análisis (por ejemplo, Firebase Analytics, Facebook Analytics) (*idem*).

Los SDKs son fáciles de usar y en su mayoría gratis, y ofrecen a los creadores soluciones para construir sus *apps* rápidamente y de forma barata. Esto significa que esta práctica se da en la mayoría de las apps disponibles.. Por ejemplo, Calendario

Menstrual hace hincapié en las normas del RGPD y en el hecho de que se recopilan datos no personales: "Mediante el uso de SDK, permitimos que nuestros socios publicitarios en los EEUU recopilen datos que no sean PII".[19]

Existe un problema con el concepto PII (*Personally Identifiable Information*) ya que las diferentes diferentes pueden causar ambivalencias. El uso de este concepto puede quedarse obsoleto internacionalmente.

Para el RGPD el término "datos personales" es el principio para la aplicación del Reglamento General de Protección de Datos (RGPD). Este se aplica solo si un tratamiento de datos se refiere a datos personales, definidos en el Artículo 4 (1) del citado reglamento así: "Los datos personales son cualquier información relacionada con una persona física identificada o identificable".

El RGPD considera que las personas son identificables en caso de que puedan ser identificadas directa o indirectamente, particularmente mediante un identificador como un nombre, un número de identidad, datos de localización, dirección IP o una de varias características especiales que expresen la identidad física, fisiológica, genética, mental, comercial, cultural o social de dicha persona física.[20]

Lo destacable de este apartado es que el RGPD sí que considera la dirección IP como un dato personal que podría identificar a una persona. En este punto, conviene recordar que la dirección IP consiste en un identificador numérico que, vinculado al protocolo de Internet (o IP), define el modo en que dentro de una red regida por dicho protocolo se pueden identificar las distintas máquinas conectadas a ella. En pocas palabras, la dirección IP podría compararse con *la matrícula* para identificar a cualquier dispositivo cuando está conectado a una red bajo el protocolo homónimo.

Una vez recordado lo anterior, cabe subrayar que la consideración de la dirección IP como dato personal en la UE quedó plenamente fijado por el TJUE cuando las consideró como " datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios".

19 Calendario Menstrual, 2022. Privacy Policy. https://www.simpleinnovation.us/my-calendar/privacy-policy
20 Comisión Europea, (s.f). ¿Qué son los datos personales? https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

Además de los datos personales generales, según el reglamento se deben tener en cuenta las categorías especiales de datos personales, entre lo cuales figuran los genéticos, biométricos y de salud, así como los datos personales que revelan el origen racial y étnico, las opiniones políticas, las convicciones religiosas o ideológicas o la afiliación sindical.

Otra definición de identificación personal es la del Instituto Nacional de Estándares y Tecnología, que alude a "cualquier información sobre un individuo que conserve un organismo, incluyendo (1) cualquier información que pueda utilizarse para distinguir o rastrear la identidad de un individuo, como el nombre, el número de la seguridad social, la fecha y el lugar de nacimiento, el apellido de soltera de la madre o los registros biométricos; y (2) cualquier otra información vinculada o vinculable a un individuo, como información médica, educativa, financiera y laboral". Aquí la dirección IP de un usuario no se clasifica como PII por sí sola, pero sí como PII vinculada (McCallister *et al.,* 2010).

Para dirimir estos conceptos y las protecciones que llevan asociadas, más allá del RGPD hay que aludir a la ePD (ePrivacy Directive), otro importante instrumento legal para la privacidad en la era digital en el marco de la UE[21]. Más concretamente, el apartado 3 de su Artículo 5 dispone que almacenar información u obtener acceso a información ya almacenada en el equipo requiere de consentimiento previo (esto es aplicable a la tecnología de rastreo en un dispositivo). El consentimiento debe entenderse del mismo modo que en el RGPD, por lo que el uso de SDK no cumple este claro requisito (Bax *et al.,* 2021).

Aunque el artículo 5(3) ePD se ha denominado "disposición sobre *cookies*", por centrarse en su uso, su ámbito de aplicación es mayor. Por ejemplo, cubre la recopilación y el tratamiento de información a través de API y SDK, ya que estos sistemas acceden a información ya almacenada en, por ejemplo, un teléfono móvil. Por lo tanto el uso de SDK por desarrolladores de aplicaciones y terceros no cumple las normas relativas al consentimientol Ello contrasta con el hecho comprobado de que casi todas las aplicaciones investigadas que utilizan SDK no piden permiso en absoluto o lo hacen de tal manera que “hace imposible que los interesados den un consentimiento

21 European Data Protection Supervisor, (s.f) ePrivacy Directive. https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en

específico, informado, inequívoco y libre antes de la recogida y el tratamiento por parte de estos usuarios de SDK" (*idem*).

En cuanto al reglamento de EEUU, cuando se busca información sobre la PII se pueden encontrar diversas definiciones. Así, por ejemplo, la Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés) define PII como "información que puede utilizarse para distinguir o rastrear la identidad, como su nombre, número de seguridad social, registros biométricos, etc. por sí sola o combinada con otros información personal o identificativa que vinculada o vinculable a una persona individuo, como la fecha y el lugar de nacimiento, nombre de soltera de la madre, etc".

En cuanto a datos de salud, la mencionada Ley HIPAA protege la privacidad de la información sanitaria identificable individualmente, denominada información sanitaria protegida. Su regla de seguridad protege toda información sanitaria identificable individualmente que una entidad crea, recibe, mantiene o transmite en formato electrónico. La Norma de Seguridad llama a este tipo de información "información sanitaria protegida eléctronica".

La Regla de Seguridad exige a las entidades mantener salvaguardas administrativas, técnicas y físicas razonables y apropiadas para proteger ese tipo de información. En concreto, estas deben garantizar confidencialidad, identificar y proteger frente amenazas a la integridad de la información, proteger frente a divulgaciones no permitidas entre otras.[22]

Volviendo a los SDK, el informe citado (*idem*) afirma respecto a EEUU que en dicho ámbito una aplicación puede contener varios SDK que el usuario desconoce. Para los autores a través del SDK de terceros, el desarrollador del mismo obtiene acceso a los datos, en su mayoría ligados ala ubicación (GPS). El acceso a los datos personales de los usuarios de la aplicación se obtiene a través de partes (a veces ocultas) de los códigos del SDK que están diseñadas para rastrear al usuario y almacenar los datos.

Es posible que los SDK recopilen categorías especiales de datos personales, que por regla general están prohibidas, a menos que se cumplan determinados criterios. Los autores añaden que la elaboración de perfiles puede crear datos de categoría especial por

22 U.S. Department of Health and Human Services (s.f). Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

inferencia a partir de datos que no son datos de categoría especial por sí mismos, pero que pasan a serlo al combinarse con otros datos (*idem*).

Finalmente este informe realizada para la entidad NOYB afirma que, dependiendo del SDK, los datos pueden transmitirse a diversas empresas y organizaciones. Por lo tanto, los autores resumen que un desarrollador de SDK suele celebrar un acuerdo con el creador de la aplicación para que el propio desarrollador del SDK pueda utilizar los datos que recibe cuando, por ejemplo, le ayuden a mejorar la funcionalidad de la aplicación. Una vez que el desarrollador en cuestión ha recopilado los datos, suele utilizarlos para sus propios fines, pero también pueden venderlos a terceros con fines publicitarios. "Está claro que el proceso suele ser tan complejo que es imposible saber si se envían los datos recogidos por una sola *app*, cómo y a quién" (*idem*).

Conclusiones

Tras haber estudiado a fondo las políticas de privacidad de las *apps* de la muestra y la de algunos de los terceros con las que estas mantienen relación se pueden obtener algunas conclusiones que paso a exponer a continuación.

De entrada, de mi investigación empírica se desprende que Meet You y Calendario Menstrual afirman abiertamente usar SDK, esta segunda escudándose en excluir de ellas la denominada en EEUU PII. El resto de políticas afirma no usarlos directamente, por más que trabajan con terceros que los poseen, por lo que no se puede afirmar que las usuarias se encuentren totalmente aisladas de los mismos.

Como se ha mencionado, se ha podido observar que aunque las *apps* no reconozcan servirse de los SDK, algunas de las terceras entidades con las que colaboran sí que lo afirman. Ello implica que al transferir los datos personales a dichas entidades, se pretende que las usuarias pasen a acatar sus políticas al hacer uso de estos SDK, si bien quizá sea más preciso afirmar que son estos SDK los que empiezan a usar a dichas usuarias.

A continuación pongo algunos ejemplos sobre posibles SDK involucrados en cada una de las *apps*. Esto no quiere decir que sean los únicos ya que la infinidad de terceros hace de esto una ardua tarea.

El primer ejemplo remite a Clue, que afirma hacer uso del paquete de análisis de rendimiento y herramientas de monitoreo llamado Firebase, proporcionado por Google LLC Firebase. Este paquete de análisis es mencionado en el informe para NOYB (i*dem*) como ejemplo de SDK desarrollada por Google con funciones analíticas.

En cuanto a Flo, aunque al indagar en las políticas no sea posible encontrar la palabra SDK, se puede observar la manera en que presenta a sus procesadores como empresas que les ayudan a gestionar los servicios, a mantener la comunicación o a realizar otras actividades relacionadas con la aplicación. Entre ellos se encuentran servicios de pago de Apple y Google que han tenido que ser introducidos en la *app* mediante sus respectivos SDK. Además también menciona como procesadores a Survey Monkey y Databriks, famosos proveedores de SDK y otros servicios.

Por su parte, Mi Calendario Menstrual reconoce utilizar servicios de *remarketing* de Google Ads, Facebook y Twitter. Esto significa que indirectamente el usuario va a entrar en contacto con los SDK de la siguiente forma: Para empezar, con el fin de desarrollar un *remarketing* dinamico para una aplicación GoogleAds necesita identificar los eventos de conversión y de *remarketing* de los que se quiere hacer un seguimiento, para lo cual instala el SDK de Firebase o un SDK de terceros para segmentar las audiencias de las aplicaciones según los eventos que hayas configurado.[23]

Según Samsing (s.f), antes de empezar a realizar una campaña de *remarketing* es necesario que se tenga en cuenta la optimización de algunos elementos, entre ellos un equipo (o *kit*) de Desarrollo de *Software* (SDK) para móviles que permita rastrear y crear audiencias automáticamente de acuerdo con los comportamientos en la aplicación.

En cuanto al SDK de Facebook, este sirve para especificar a qué personas deseas llegar con tu campaña de *remarketing*, para lo cual ofrece observacioness sobre las personas que hacen uso de la aplicación donde se encuentra instalado y las acciones que realizan en ella. Al poner en funcionamiento este *kit*, se puede aplicar una nueva segmentación con el fin de buscar personas que hayan realizado determinadas acciones en tu

23 Support Google, (s.f). Acerca del remarketing dinámico para aplicaciones https://support.google.com/google-ads/answer/7538938?hl=es

aplicación. [24] Por lo tanto se observa que hacer una campaña de *remarketing* implica usar SDK.

Por último, Alerta periodo tiene una política tan escueta que no menciona ni siquiera los terceros con los que tiene relación. De este modo, la aplicación expone que pueden trabajar con compañías de análisis sin mencionar nombre alguno, y añade que trabajan con anunciantes y redes publicitarias de terceros. Según la *app* los anunciantes y sus redes usan alguna información recolectada por la aplicación, incluida la ID única de publicidad del dispositivo móvil.

Por lo tanto se puede concluir que los SDK podrían ser la raíz de un problema de gestión de datos por todos los motivos comentados anteriormente. Y es que aunque muchas de estas aplicaciones ni siquiera mencionen los SDK, se ha podido saber sus terceros sí hacen uso de ellos, por lo que si dicen que te atengas a sus políticas ello implica que también has de atenerte a sus SDK.

Me gustaría hacer hincapié en la cantidad de terceros que se ven involucrados cuando haces uso de un mínimo servicio de las *apps*, lo que nos lleva ineludiblemente a preguntarnos si no existen demasiados participantes en un juego que por lo demás presenta unas reglas muy complicadas para que todos los acaten a la perfección. Y por si todo ello no fuera suficiente, hay que tener en cuenta que la habitual derivación de estas aplicaciones a las políticas de privacidad de las terceras entidades con las que comparten sus datos acaba generando un bucle infinito por donde se acaba perdiendo cualquier perspectiva de control sobre los datos personales volcados en estos servicios y sus asociados.

Otro elemento que destaco tras leer las políticas en profundidad es que hay otras formas de obtener los datos de las usuarias más fácilmente y que quizás ni siquiera hiciera falta el uso de los mencionados SDK. Por ejemplo, en el momento en el que una usuaria inicia sesión en una *app* con un tercero es posible que los datos que derivan de una cuenta pase a la otra provocando así un intercambio: “Si abres sesión con un tercero, en

24

24 Meta (s.f). ¿Cómo puedes favorecer a tu empresa la nueva segmentación en Facebook?. https://es-es.facebook.com/business/goals/retargeting

este caso, Clue intercambiará ciertos datos con Facebook, como los datos de los dispositivos, tu dirección IP y la información que proporcionaste a Facebook cuando creaste tu cuenta con Facebook. Esto puede incluir una transferencia de tus datos personales a los servidores de Facebook situados fuera de la Unión Europea". [25]

Además es destacable que se ha observado que al final por un motivo u otro todas las aplicaciones recogen la dirección IP pese a que ha quedado claro que en la UEesta información debería considerarse como un dato personal y, por ende, manejarse con todas las salvaguardas previstas en la legislación y la jurisprudencia de la UE.

Como conclusión, quiero retomar una de las preguntas de investigación clave que planteé al inicio de este TFG: ¿Qué pasaría si una usuaria estadounidense se descarga una *app* de seguimiento menstrual con sede en Europa? ¿Y al contrario? En caso de que alguna de ellas se viera envuelta en algún problema legal ¿de qué forma se haría uso de sus datos? ¿Estarían ambos sujetos en una situación igualitaria?

Lo que se ha podido saber es que una *app* que se declare europea y haga uso de SDK relacionados con empresas estadounidenses, o que posea servidores en dicho territorio, no puede considerarse totalmente segura, ya que los datos no se mantienen durante todo el tiempo bajo la protección del RGPD. Que estos datos viajen solo genera dispersión y, con ella, una notable difuminación de los límites en cuanto a la legalidad.

Por todo ello, una mujer estadounidense no debería sentirse totalmente segura aunque descargara una *app* radicada en la UE, por todo lo que se ha comentado a lo largo de la investigación.

En cuanto a una mujer europea, se puede concluir que estando bajo el amparo del RGPD sería más complicado que tuviera algún conflicto, pero esto no quiere decir que deba pensar que sus datos están totalmente protegidos, pues estos pueden estar en cualquier parte, como se ha podido observar.

Por lo tanto determino que por supuesto que hay desigualdad, que comienza por la legislación de cada país y deriva en cada aspecto de la vida de las personas hasta en los considerados más íntimos. Pero, en última instancia, para que podamos considerarnos fuera de los muros de la Cloud Act el prestador de los servicios a los que accedamos

25 Clue, 2022. Política de Privacidad de Clue. https://helloclue.com/es/privacidad

debería estar exento de cualquier influencia o asociación con los proveedores de servicios de EEUU (por no hablar de potencias emergentes como China y los conflictos políticos y legislativos que existen o puedan existir con ellas, sean vinculados a la salud sexual y reproductiva de las mujeres o a otros derechos fundamentales). En ese caso, no existiría peligro de obligación a revelar datos personales en virtud de la Ley Cloud Act. Sin embargo, en el momento en que un proveedor de servicios de nube europeo es adquirido por una empresa de EEUU, este entra directamente en el ámbito de aplicación de la Ley Cloud Act.

Por lo tanto, ahora la única forma de evitar los problemas que podría atraer consigo la Cloud Act respecto a la protección de datos personales podría ser buscar un proveedor de servicios en la nube o de alojamiento en servidores que sea en su totalidad europeo, pues así, al menos hasta que no se reciba una orden de un juez europeo, no se podría facilitar el acceso a ningún tipo de información.

Aunque como se ha podido observar el papel de los terceros es demasiado importante, así como las localizaciones de sus servidores y por lo anterior podría no ser una solución.

Ahora supongo que el lector o la lectora se estará preguntando y entonces ¿Sería mejor dejar de registrar el periodo y pasarse de nuevo a “la libreta”?

Pues bien, por supuesto, no hay una respuesta única, pero cierto es que si no se quiere que se conozca un secreto lo que se suele hacer es no contarlo:.

"Las leyes pueden cambiar. Las normas sociales pueden cambiar. La conversación perfectamente inofensiva que mantuviste ayer puede volver a perjudicarte dentro de unos años" (…) Por eso no escribimos cada conversación hablada y la guardamos para siempre” (Hopkins, citado en Newman, 2022).

No obstante, hay que tener en cuenta que aquí solo se ha puesto el ejemplo de este tipo de aplicaciones, pero cada una es un mundo y conlleva tomar medidas ajustadas a cada caso. De nada serviría no tener un *app* de ciclo menstrual pero tener otras dedicadas a otros fines que conlleven las mismas delatoras filtraciones de datos personales.

Para finalizar y continuando con la conclusión me gustaría exponer la siguiente crítica: la vigilancia masiva no debería justificarse con mantener segura a la ciudadanía pues

ese es un argumento totalmente obsoleto. Como mencionan algunos autores, prohibir el cifrado en los servicios en línea quizás haga que los delincuentes solo tengan que reinventarse y construir otras herramientas. Deberíamos replantearnos si de verdad merece la pena pinchar todos los teléfonos (sacrificando con ello la privacidad de toda la ciudadanía) para buscar a un criminal o si por el contrario estos círculos de búsqueda deberían acotarse de tal forma que el objetivo de las pesquisas no fuera la población mundial.

Esto enlaza con la histórica cita de Phil Zimmermann (1990) "Si se proscribe la privacidad, solo los proscritos tendrán privacidad". En la misma línea, el citado Lessig (2009) afirmaría años más tarde lo siguiente respecto a los abusos de privacidad con el pretexto de investigar conductas ajenas a ella: “Del mismo modo que una ley que prohibiera el uso de preservativos tendería a promover el registro de dormitorios, una prohibición del registro de dormitorios tendería a desincentivar leyes que prohibieran los preservativos”.

En definitiva, con las reflexiones anteriores vuelvo a retomar a Lessig (2015) el cual afirma que existen formas para construir una infraectructura de vigilancia que proteja la intimidad de manera fundamental y que al mismo tiempo ofrezca al gobierno una mejor oportunidad de identificar los riesgos que se deben perseguir. Para el autor no es necesario elegir entre protegernos de la privacidad o enfrentarnos a terroristas.

Limitaciones

Como toda investigación, esta ha contado con ciertas limitaciones que han contribuido a que la misma no pueda desarrollarse en su totalidad. El primer problema con el que me he encontrado a lo largo de la investigación es la escasez de información académica, supongo que por ser un tema novedoso aún no se ha dado mucho margen para investigar a fondo sobre él. No obstante, también es interesante que no haya mucho donde acudir ya que esto proporciona un cierto grado de libertad expresiva y un aire de innovación que no se daría si ya hubiera mucho investigado sobre el tema.

Además, he encontrado mucha más bibliografía anglosajona que en castellano y es inevitable que la barrera del idioma se ha impuesto al interpretar todo de manera clara. Aun así, he tratado de realizar traducciones lo más acertadas posibles, donde apenas se perdiera contexto.

Quizás a lo largo de la investigación he pecado de sacar demasiada información de medios generalistas tanto españoles como estadounidenses. Aun así gracias a ellos pude percatarme de que este es un tema que verdaderamente está calando en la sociedad, y no ya solo en círculos académicos, y del que se habla en medios más a menudo de lo que pensaba. Es cierto que este uso masivo de medios generalistas puede hacer que exista un cierto sesgo político o falta de rigurosidad en algunas ocasiones.

Asimismo durante el estudio he tenido que lidiar con varias actualizaciones de información, ya que algunos de los puntos de los que hablaba se iban quedando obsoletos conforme iba avanzando en la investigación. Al ser un tema en pleno auge la información va mutando y esto ha hecho que me encuentre alerta durante todo el periodo de la realización del trabajo.

Quiero destacar también que es complicado hacer generalidades con sistema iOs y sistema Android ya que a veces los sistemas operativos difieren en sus funcionalidades. Quizás esto sería algo en lo que debería haber indagado más desde el principio para centrarme más en sus diferencias y no caer quizás en generalidades.

Me gustaría hacer hincapié en que la legislación de EEUU en esta materia no se puede limitar a las (escasas) normas federales, sino que la amplia gama de Estados se traduce en diferentes catálogos de leyes que es complicado analizar por separado. Es por esto que se ha contado con la Cloud Act como algo general pero sin centrarse en las leyes de cada Estado que quizás cambiarían las tornas en algunas situaciones concretas.

Además en varias ocasiones me he encontrado con una información dentro de las políticas de privacidad muy opaca, poco transparente y complicada de entender.

Por último, juzgo reseñable comentar que conforme iba avanzando la investigación veía que se podía profundizar demasiado en cada uno de los asuntos mencionados y quizás no he acertado a la hora de focalizar más en unos que en otros, dando la sensación quizás de pasar por alto algún tema de considerada relevancia.

Asimismo pienso que la muestra escogida ha sido demasiado amplia y no he podido profundizar en cada aplicación lo necesario para encontrar matices que pudieran cambiar las tornas de la investigación. Quizás con una muestra más reducida me habría resultado más fácil explicar las causas por las que cada una vulneraba el RGPD de forma más específica.

Verdaderamente conforme he ido avanzando la investigación me he dado cuenta de que había fuentes a las que debería haberles dado más importancia y por lo tanto haberlas usado para explicar ciertos conceptos.

Prospectiva o enfoque de investigaciones futuras

En cuanto a prospectiva o enfoque que daría a futuras investigaciones podrían surgir varias ramas en las que sería interesante seguir indagando. Por ejemplo estudiar a fondo quiénes son los dueños de las empresas impulsoras de estas *apps,* patrocinadores, empresas matrices, quiénes se encargan o se encargaron de su financiación, etc.

Además cada una de las *apps* escogidas daría para un estudio en profundidad, ya que cada política de privacidad contiene sus diferencias y hay muchos apartados en los que nos podríamos centrar mucho más a fondo, estudiando posibilidades y supuestas situaciones en la que la empresa se vería comprometida.

Para ampliar esta investigación también se podría seguir con las comparaciones con otros marcos legislativos de otros países (como por ejemplo China, a la que aludí arriba) y ver qué pasa cuando los servidores de las *apps* que instalamos están alojados en ese territorio o en cualquier otro.

Otro estudio interesante estaría relacionado con los usos comerciales que se les da a las *apps Femtech* o más concretamente a las *apps* de control de ciclo. Podría tratarse de una investigación empírica donde la persona investigadora compruebe mediante una observación participante qué tipo de publicidad recibe según efectúe unas acciones u otras en las *apps*.

Cómo se comunican estas *apps* entre sí y qué datos transmiten al exterior sería otra opción para indagar más en la temática. Como he apuntado, muchas de estas aplicaciones de control de ciclo han tenido que hacer frente a grandes polémicas o noticias que han perjudicado su reputación, y a raíz de ellas muchas usuarias han decidido desinstalar este tipo de *apps* de sus teléfonos móviles y estas empresas se han visto amenazadas, por lo que han decidido mostrarse más transparentes e indagar en diferentes puntos que consideran importantes en su política de privacidad.

En concreto, sería interesante centrarse en la comunicación de Flo tras el revuelo de noticias que acusaban a esta *app* de haber compartido datos con Facebook y de sus numerosas grietas en su política de privacidad.

Otro tema que igual se aleja algo de este estudio pero que no podríamos dejar a un lado sería hablar de las personas que menstrúan pero que no se identifican como mujeres. Sería curioso ver qué uso hacen de estos servicios (en la medida en que lo hagan), cómo reciben la información de dichas *apps* y qué aspectos les atraen o les molestan de la usabilidad de este tipo de *apps*.

Para finalizar, me gustaría subrayar que el solo hecho de analizar el avance de esta situación conforme pasa el tiempo sería muy beneficioso ya que es un tema que va cambiando día a día y que afecta a derechos fundamentales de las mujeres. Su dinamismo incita a seguir actualizando información sobre cómo va cambiando el panorama social, político y legislativo en cuanto al aborto y las políticas de privacidad tanto en la UE como en EEUU.

En suma, como reflexión final me gustaría citar esta frase sentencia realmente inspiradora para la realización de este trabajo:

"Decir que no te importa la privacidad porque no tienes nada que esconder no es diferente a afirmar que no te importa la libertad de expresión porque no tienes nada que decir" (Snowden, 2019).

Bibliografía

Alzate, V. A. y Cotta, S. (2020). *Estándar internacional para las transferencias de datos personales, un camino por recorrer hacia la seguridad y confianza en los negocios y entornos digitales.* [Tesis de maestría, Universidad Externado de Colombia]. Bdigital. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/ed12c6b2-ac93-4539-8060-e99d9a7d4c6e/content

Bax, M., Giebels, F. y Sepovan, S. (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

Bhuiyan, J. (2022, mayo 6). Abortion surveillance: in a post-Roe world, could an internet search lead to an arrest?. *The Guardian.* https://www.theguardian.com/world/2022/may/06/abortion-laws-surveillance-privacy-phone-data

Cabello, F. y Solera, F. (2021). Ofuscación algorítmica. Obnubilación táctica para una privacidad por las nubes. En A. Gostinski (Ed), *Algoritarismos.* 317-330. Tirant lo Blanch. https://dialnet.unirioja.es/servlet/articulo?codigo=7848157

Cardozo, R., Romano, E., Ortunio, M., Guevara, H. y Romano, A. (2016). Elaboración de los objetivos en la investigación. *Academia Biomédica Digital (65).* https://dialnet.unirioja.es/servlet/articulo?codigo=6455441

Castaño, J. (2022, julio 1). Los datos que recogen las apps menstruales, en el disparadero tras la sentencia del aborto en EE.UU. *La Vanguardia.* https://www.lavanguardia.com/tecnologia/20220701/8376886/negocio-datos-apps-controlan-ciclos-menstruales-son-mas-seguras-pmv.html#:~:text=Seg%C3%BAn%20un%20informe%20de%202021,del%20seguro%20m%C3%A9dico%20(HIPAA).

Leading period tracker and female health apps worldwide in April 2022, by downloads de Ceci, L. (2023). Statista. https://www.statista.com/statistics/1307702/top-period-tracker-apps-worldwide-by-downloads/

Comisión Europea. (2023). *¿Qué son los datos personales?.* Web Oficial de la Unión Europea. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

Conty- Cook, C., (2020). Surveilling the Digital Abortion Diary. *University of Baltimore Law Review (50)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3666305#

Cordero, C. (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. https://www.revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/view/54

De Hert, P. y Thumfart, J., (2020). The Microsoft Ireland case, the Cloud Act and the cyberspace sovereignty trilemma. *Jusletter, (21),* 373-417 https://jusletter-it.weblaw.ch/en/issues/2020/fses/19_s_373_418_de-hert_29c39cf0a6.html

Del Castillo (2019, septiembre 17). Hola, soy la app de tu menstruación y les cuento a otros lo que sé sobre ti. *El diario.es* https://www.eldiario.es/tecnologia/hola-app-menstruacion-vendiendo_1_1360976.html

Del Castillo, C. (2023, mayo 22). Histórica multa de 1.200 millones de euros a Meta por enviar datos de los europeos a EEUU. *El Diario.es.* https://www.eldiario.es/tecnologia/historica-multa-1-200-millones-euros-meta-enviar-datos-europeos-eeuu_1_10225583.html

Dewan, S. y Frenkel, S. (2022, agosto 18). A Mother, a Daughter and an Unusual Abortion Prosecution in Nebraska. *Way Back Machine.* https://web.archive.org/web/20221130040730/https://www.nytimes.com/2022/08/18/us/abortion-prosecution-nebraska.html

Didier, M. M. (2022). "Dobbs vs. Jackson: un giro copernicano en la jurisprudencia de la Corte Suprema de Estados Unidos". *Prudentia Iuris, (9),* 363-375. https://doi.org/10.46553/prudentia.94.2022.pp.363-375

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 respeta al tratamiento de datos personales y a la libre circulación de estos datos. Boletín Oficial del Estado, 281, de 23 de octubre de 1995. https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

Earle, S., Hadley, R., Marston, H y Banks, D (2020). Use of menstruation and fertility app trackers: A scoping review of the evidence. *BMJ Sexual & Reproductive Health, 47(2),* 90–101. Use of menstruation and fertility app trackers_ a scoping review of the evidence (BMJ Sexual & Reproductive Health) (2020).pdf

Eschler, J., Menking, A., Fox, S. y Backonja, U. (2019). Defining Menstrual Literacy With the Aim of Evaluating Mobile Menstrual Tracking Applications. *CIN: Computers, Informatics, Nursing 37*(12), 638-646, https://doi.org/10.1097/cin.0000000000000559

Etarque (2017, enero 4). Chupadatos: proyecto para América Latina muestra cómo las tecnologías pueden robar información personal. *Knight Center.* https://latamjournalismreview.org/es/articles/chupadatos-proyecto-para-america-latina-muestra-como-las-tecnologias-pueden-robar-informacion-personal/

Eticas (2019). Mi cuerpo mis datos sus normas qué hacen con nuestros datos las apps menstruales. Eticas Foundation. https://eticasfoundation.org/wp-content/uploads/2022/06/ETICAS_Mi-cuerpo-mis-datos-sus-normas-202206.pdf

Federici, S. (2018). La tecnología, el cuerpo y la construcción de los comunes. *Revista Casa de las Américas 291,* 88-98. http://www.casadelasamericas.org/publicaciones/revistacasa/291/5-Notas.pdf

Federici, S. (2022). Ir más allá. Repensar, rehacer y reivindicar el cuerpo en el capitalismo contemporáneo. *Buenos Aires: Tinta Limón*, *155*. http://dx.doi.org/10.35305/cc.v2i21.67

Felizi, N. y Varon, J. (s.f). *Menstruapps- ¿Cómo convertir tu menstruación en dinero (para los demás)?* Chupadatos. https://chupadados.codingrights.org/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

Fernández (2022, julio 22). Cuál es mi IP: qué es una dirección IP y cómo puedes saber la tuya. *Xataka.* https://www.xataka.com/basics/que-es-una-direccion-ip-y-como-puedes-saber-la-tuya

Flo (s.f). *Privacy policy.* https://flo.health/privacy-policy

Follows, T. (2018, marzo 9). The fast - growing femtech market will truly peak when it`s just "tech". *Campaignlive.* https://www.campaignlive.co.uk/article/fast-growing-femtech-market-will-truly-peak-when-its-just-tech/1459711

Forbrukerradet (2020, enero 14). Out of control. https://www.forbrukerradet.no/out-of-control/

Ford A., Togni, G., y Miller, L. (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

Gallagher, P. (2019, agosto 13). The CLOUD Act: Mooting the Microsoft Ireland Case, but Not Forecasting Clear Skies Just Yet. *Columbia Business Law Review.* https://journals.library.columbia.edu/index.php/CBLR/announcement/view/161

Gamboa Bernal GA. Derogada la sentencia Roe vs. Wade. Pers Bioet. (2022), 26 (2), 2621. https://doi.org/10.5294/pebi.2022.26.2.1

Garamvolgy, F. (2022). Por qué las mujeres estadounidenses están eliminando sus aplicaciones de seguimiento de ciclo menstrual. *La lista.* https://la-lista.com/the-guardian/2022/07/02/por-que-las-mujeres-estadounidenses-estan-eliminando-sus-aplicaciones-de-seguimiento-del-ciclo-menstrual

García, N. (2021). Discurso en torno a la menstruación. Representación social, vivencia del ciclo y medicalización de la fase premenstrual. [Tesis doctoral, Universidad de Sevilla, Universidad de Jaén y Escuela Andaluza de Salud Pública]. Idus. https://idus.us.es/bitstream/handle/11441/130658/Garc%c3%ada%20Toyos%2c%20Noelia%20tesis.pdf?sequence=1&isAllowed=y

Glazer, N. Y. (1984). Servants to Capital: Unpaid Domestic Labor and Paid Work. *Review of Radical Political Economics, 16(1)*, 60–87. doi: https://doi.org/10.1177/048661348401600106

Glenza, J., (2019, mayo 30). Revealed: women's fertility app is funded by anti-abortion campaigners. *The Guardian*. https://www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners

Gómez y Méndez J. M. (2017). Mattelart, Armand y Vitalis, André (2015): De Orwell al cibercontrol. *Estudios sobre el Mensaje Periodístico*, *23*(1), 703-704. https://doi.org/10.5209/ESMP.55624

Gómez-Luna, E., Navas, F., Aponte-Mayor, G. y Betancourt, A. (2014). Literature review methodology for scientific and information management, through its structuring and systematizacion. *DYNA*, *81 (184),* 158-163 https://doi.org/10.15446/dyna.v81n184.37066

Gonzáles, J. L., Covinos, M. R., y Cáceres, M. (2020). Formulación de los objetivos específicos desde el alcance correlacional en trabajos de investigación. *Ciencia Latina Revista Científica Multidisciplinar*, *4*(2), 237-247. https://doi.org/10.37811/cl_rcm.v4i2.73

Gonzalo, M. y López, N. (2022, septiembre 4). No solo hay riesgo en las apps de menstruación: así se instrumentalizan los datos de salud de las mujeres. *Newtral.* https://www.newtral.es/datos-salud-mujeres aborto-privacidad/20220904/

Gpass (s.f). *Support.* https://gpapps.com/support/eula/

Gren, L., Shay, N., Roberts, S., Pierce, J., Kape, B. y Boyd, P. (2019, junio 20). How your period is making other people rich. *The Guardian.* https://www.theguardian.com/society/video/2019/jun/20/how-your-period-making-other-people-rich-video

Grundy, Q., Chiu K., Held, F., Continella, A., Bero L. y Holz, R. Data (2019). Sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ*, 364. https://doi.org/10.1136/bmj.l920

Guttmacher Instituten. (2023, junio 6). *Interactive Map: US Abortion Policies and Access After Roe.* https://states.guttmacher.org/policies/ohio/abortion-policies

Halstuk, E. y Chamberlin, B (2006). The Freedom of Information Act 1966–2006: A Retrospective on the Rise of Privacy Protection Over the Public Interest in Knowing What the Government's Up To. *Communication Law and Policy, 11(4),* 511-564. https://doi.org/10.1207/s15326926clp1104_3

Hamui, A.(2016). La pregunta de investigación en los estudios cualitativos. *Revista de Investigación en Educación Médica. 5 (17),* 49-54. https://www.elsevier.es/es-revista-investigacion-educacion-medica-343-articulo-la-pregunta-investigacion-estudios-cualitativos-S2007505715000745

Hello Clue (s.f). *Privacidad.* https://helloclue.com/es/privacidad

Herranz, A. (2018, marzo 7). GDRP/RGPD: qué es y cómo va a cambiar internet en la nueva ley de protección de datos. *Xataka.* https://www.xataka.com/legislacion-y-derechos/gdpr-rgpd-que-es-y-como-va-a-cambiar-internet-la-nueva-ley-de-proteccion-de-datos

Hill, K. (2022). Borrar el registro de tu menstruación no te protege. New York Times. https://www.nytimes.com/es/2022/07/04/espanol/app-ciclo-menstrual.html

Hohmann-Marriot, B. y Starling, L. (2022). "What if it's wrong?" Ovulation and fertility understanding of menstrual app users. Ovulation and fertility understanding of menstrual app users, *SSM - Qualitative Research in Health, (2),* 1-9. https://doi.org/10.1016/j.ssmqr.2022.100057

Hohmann-Marriott, B. (2021). Periods as powerful data: User understandings of menstrual app data and information. *New Media & Society.* https://doi.org/10.1177/14614448211040245

Howard, J. (2022, marzo 16). La tasa de mortalidad materna en EEUU aumentó considerablemente en 2021, según muestran datos de los CDC. *CNN.* https://cnnespanol.cnn.com/2023/03/16/tasa-mortalidad-materna-eeuu-aumento-2021-cdc-problema-este-empeorando-trax/

Lauren Worsfold, L., Marriott, L. Johnson, L y Harper, J., C. (2021). Period tracker applications: What menstrual cycle information are they giving women? *Women's Health,* 17, 1–8 https://doi.org/10.1177/17455065211049905 7

Jole, V. y Petrosvki, A. (2016). Immaterial Labour and Data Harvesting. Share Lab. https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/

Kagan, J., (2023, febrero 27). How the Fair Credit Reporting Act (FCRA) Protects Consumer Rights. *Investopedia.* https://www.investopedia.com/terms/f/fair-credit-reporting-act-fcra.asp

Ko, S., Lee, J., y Woo, H. (2023). Menstrual Tracking Mobile App Review by Consumers and Health Care Providers: Quality Evaluations Study
JMIR Mhealth Uhealth (81). https://doi.org/10.2196/40921

Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C. y Shadbolt, N. (2021). Before and after GDPR: tracking in mobile apps. *Internet Policy Review, 10* (4). https://doi.org/10.14763/2021.4.1611

Lastra, E (2023). A Meta le cae una multa histórica de 1.200 millones de euros, la mayor sanción nacida al calor del RGPD. *Marketingdirecto.com.* https://www.marketingdirecto.com/digital-general/social-media-marketing/meta-cae-multa-historica-millones-euros

Lessig, L. (2009). *El código 2.0.* Traficantes de Sueños. https://traficantes.net/sites/default/files/pdfs/El%20c%C3%B3digo%202.0-TdS.pdf

Levy, J. (2020). In_equalities, digitized: practices, experiences and consequences of app-supported menstrual tracking. Granada: Universidad de Granada. http://hdl.handle.net/10481/59386

Levy, J. y Romo Avilés, (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). https://doi.org/10.1186/s12889-019-7549-8

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del estado, 294, de 6 de diciembre de 2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial del Estado, 262, de 31 de octubre de 1992. https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Liceras, L. (2022, mayo 5). *Derecho al aborto en EEUU.* Amnistía Internacional. https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/el-derecho-al-aborto-en-peligro-en-estados-unidos/

Llaneza, P. (2022, junio 16). Cómo contarle tus ciclos menstruales a una app puede llevarte a la cárcel. *El Pais.* https://elpais.com/tecnologia/2022-06-16/como-contarle-tus-ciclos-menstruales-a-una-app-puede-llevarte-a-la-carcel.html#:~:text=Un%20informe%20de%202021%20del,que%20tampoco%20nadie%20se%20lee.

López-Lapuente, L. (2017). La transferencia de datos a EEUU la transición del Safe Harbor al Privacy Shield y un paso más allá. *Actualidad jurídica Uría Menéndez.* (45), 36-38. https://dialnet.unirioja.es/servlet/articulo?codigo=6017135

Lupton D (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality, (17)*, 440-453. https://doi.org/10.1080/13691058.2014.920528

Lupton, D. (2016). The use and value of digital media for information about pregnacy and early motherhood: A focus group study. *BMC. Pregnacyand Childbirth, 16* (1), 1-10. https://doi.org/10.1186/s12884-016-0971-3

Lutz, S. y Sivakumar, G. (2019). Leaking the secret: women's attitudes toward menstruation and menstrual-tracker mobile apps. *New Media & Society,* (113), 362-377 https://doi.org/10.1080/09718524.2020.1786990

Lutz, S. y Sivakumar,G. (2020). Leaking the secret: women's attitudes toward menstruation and menstrual-tracker mobile apps, *Gender, Technology and Development, 24 (3),* 362-377. https://doi.org/10.1080/09718524.2020.1786990

Maass, P. (2013, agosto 13). How Laura Poitras Helped Snowden Spill His Secrets. *The New York Times Magazine.* http://mobile.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?smid=tw-nytmedia&seid=auto&

McGee, A., (2015). "The Politics of Protection: The Forgotten History of Georgia Feminists and Doe v. Bolton." [Tesis, Georgia State University]. Semantic scholar. http://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1098&context=history_theses

McMillan,C (2022). Monitoring Female Fertility Through 'Femtech': The Need for a Whole-System Approach to Regulation. *Medical Law Review*, *30 (3),* 410–433. https://doi.org/10.1093/medlaw/fwac006

Meet You (s.f). *Privacy.* https://www.meetyouintl.com/home/privacy.html

Meseguer, N. (2022, julio 21). Las apps menstruales a debate tras la abolición del aborto en EE.UU: ¿afecta en España? *UOC News.* https://www.uoc.edu/portal/es/news/actualitat/2022/189-apps-control-menstrual-aborto.html

Murtha T. (2022, febrero 15). Statement on our New Brief: The CPC Industry as a Surveillance Tool of the Post-Roe State. Women´s Law Project https://www.womenslawproject.org/2022/02/15/statement-on-our-new-brief-the-cpc-industry-as-a-surveillance-tool-of-the-post-roe-state/

Montalto, M. (2018, abril 12). Cuidado con tus datos más íntimos: el negocio de las aplicaciones para la menstruación y el embarazo. *Euronews.* https://es.euronews.com/2018/04/12/cuidado-con-tus-datos-mas-intimos-el-negocio-de-las-aplicaciones-para-la-menstruacion-y-el

Moreno, E. (2017). Entrevista a Silvia Federici. *Filanderas*, *(2)*, 97–105. https://doi.org/10.26754/ojs_filanderas/fil.20172231

Moreno, M. (27 de enero 2020). La Comisión Europea prohíbe usar WhatsApp a sus empleados. *TreceBits.* https://www.trecebits.com/la-comision-europea-prohibe-usar-whatsapp-a-sus-empleados/

Navarro, L. (2022, junio 29). El nuevo mapa del aborto en Estados Unidos tras la derogación de Roe vs Wade. *Newtral.* https://www.newtral.es/mapa-aborto-estados-unidos/20220629/

Nieves, M. (2011). El derecho a la privacidad en los Estados Unidos : aproximación diacrónica a los intereses constitucionales en juego. *Teoría y realidad constitucional, segundo semestre,* (28), 279-312. http://e-spacio.uned.es/fez37/public/view/bibliuned:TeoriayRealidadConstitucional-2011-28-2070

Nohlen, D. (2020). Antologías para el estudio y la enseñanza de la ciencia política. *Universidad Nacional Autónoma de México.* https://archivos.juridicas.unam.mx/www/bjv/libros/13/6180/5.pdf

Noyb. (2021, mayo 25). *Declaración: Tercer aniversario del RGPD*. https://noyb.eu/es/declaracion-tercer-aniversario-del-rgpd

NOYB. (2023, Enero). *Día de la Protección de Datos: ¿Están realmente protegidos los europeos?*https://noyb.eu/es/dia-de-la-proteccion-de-datos-estan-realmente-protegidos-los-europeos

NOYB. *(*2023, Mayo*) 5 años del GDPR: Las autoridades nacionales defraudan al legislador europeo*. https://noyb.eu/es/5-years-gdpr-national-authorities-let-down-european-legislator

NOYB. (2023, Mayo). *Victoria de Noyb: multa de 1200 millones de euros a Meta por las transferencias de datos entre la UE y EEUU* https://noyb.eu/es/decision-de-la-jepd-sobre-las-transferencias-de-datos-ue-eeuu-de-facebook-suspension-de-las

Office for Civil Rights (OCR). (2009, Noviembre).*Summary of the HIPAA security rule*. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Palop, M. (2017). Protección jurídica de menores víctimas de violencia de género a través de internet. [Tesis doctoral, Universidad Jaume I]. Dialnet. https://dialnet.unirioja.es/servlet/tesis?codigo=146608

Peirano, M. (2022 febrero, 1). El derecho de los datos en la era post-derechos civiles. *Muy Interesante.* https://www.muyinteresante.es/tecnologia/26244.html

Peirano, M. (2022). Hacia una nueva ilustración digital europea. Fundación Carolina. https://www.fundacioncarolina.es/hacia-una-nueva-ilustracion-digital-europea/

Peña, P. (2022, junio 24). Aplicaciones de menstruación: claves para evaluar su tratamiento de datos privados. *RTVE*. https://www.rtve.es/noticias/20220624/menstruapps-consejos-proteger-privacidad-datos-intimos/2385227.shtml

Perez, E. (2020, julio 16). La Justicia Europea anula el "Privacy Shield": los datos personales europeos ya no podrán transferirse a servidores de los EEUU. *Xataka.* https://www.xataka.com/privacidad/justicia-europea-anula-privacy-shield-datos-personales-europeos-no-podran-transferirse-a-servidores-ee-uu

Perez, J. (2023). Crónica de la batalla judicial en torno al abortode Roe v. Wade a Dobbs v. Jackson. *Teoría y realidad constitucional, (51),* 529-564.https://dialnet.unirioja.es/servlet/articulo?codigo=8940546

Peterson, M. (2019). *Aborto ¿qué fue el caso Roe v. Wade y por qué fue una sentencia histórica?* National Geographic. https://www.nationalgeographic.es/historia/2022/06/aborto-que-fue-el-caso-roe-v-wade-y-por-que-fue-una-sentencia-historica

Pichon, A., Jackman, K., Bobel, C. y Elhada, N. (2022). The Messiness of The Menstruator: Assessing Personas and Functionalities of Menstrual Tracking Apps, *Journal of the American Medical Informatics Association, (29),* 385–399. https://doi.org/10.1093/jamia/ocab244

Polo, A. (2022). Privacidad, intimidad y protección de datos: una mirada estadounidense y europea. Derechos y Libertades*: Revista De Filosofía Del Derecho Y Derechos Humanos*, *(47),* 307-338. https://doi.org/10.20318/dyl.2022.6884

Por qué vemos mensajes instando a las mujeres a eliminar sus apps de control menstrual en Estados Unidos. (2022, junio 30). *Malditatecnología.* https://maldita.es/malditatecnologia/20220630/eeuu-eliminar-apps-control-menstrual/

Poyato, M. (2020, enero 20). Us Patriot Act, una amenaza para la privacidad de las empresas europeas. *Cybersecuritynews.* https://cybersecuritynews.es/us-patriot-act-una-amenaza-para-la-privacidad-de-las-empresas-europeas/

Pozo, A. (2019, junio 12). Polémica app de fertilidad es financiada por grupos antiaborto y asesorada por médicos chilenos. *JGM.* https://radiojgm.uchile.cl/polemica-app-de-fertilidad-es-financiada-por-grupos-antiaborto-y-asesorada-por-medicos-chilenos/

Privacy Interational (2020, octubre, 7). No Body´s Business But Mine: How Menstruation Apps Are Sharing Your Data. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

Pulver, A. (2015, febrero 23). Edward Snowden documentary Citizenfour wins Oscar. *The Guardian*. https://www.theguardian.com/film/2015/feb/23/edward-snowden-documentary-citizenfour-wins-oscar

(2019). CCBE Evaluación de CLOUD Act de EE.UU. https://www.abogacia.es/wp-content/uploads/2020/04/Evaluaci%C3%B3n-de-CCBE-sobre-la-CLOUD-Act-de-EE.UU_.-respecto-al-Derecho-de-la-UE.pdf

Qué relación hay entre las aplicaciones que monitorizan la menstruación y la derogación del aborto legal en EEUU. (2022, junio 30). *Malditatecnología.* https://maldita.es/malditatecnologia/20220630/aborto-eeuu-apps-menstruacion/

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. Diario Oficial de la Unión Europea L119, de 4 de mayo de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Rodriguez, S. (2019). La Cloud Act: motivo de preocupación para las autoridades las empresas y los ciudadanos de la Unión Europea. *Ciberseguridad news.* https://cybersecuritynews.es/la-

cloud-act-motivo-de-preocupacion-para-las-autoridades-las-empresas-y-los-ciudadanos-de-la-union-europea/

RTVE (2023, mayo 22). Irlanda multa a Facebook con 1.200 millones de euros, la mayor sanción en Europa por infringir la privacidad de datos. *Rtve.es* https://www.rtve.es/noticias/20230522/irlanda-multa-facebook-vulnerar-privacidad-datos/2447035.shtml

Ruiz, S. (2021). La Sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems II o cómo los datos personales pueden terminar viajando sin equipaje. *Revista Española De Derecho Europeo, (76),* 111–162. https://doi.org/10.37417/REDE/num76_2020_532

Sabin, S. (2022, julio 6). 'Lock it down right now': Abortion rights advocates prepare for a new wave of digital security threats. *Político.* https://www.politico.com/news/2022/06/17/abortion-rights-advocates-digital-security-threats-00040654

Sánchez, M. (2020, agosto 14). Shoshana Zuboff: "La forma de socavar el dividendo que genera la vigilancia tecnológica es haciéndola ilegal". *ElDiario.es.* https://www.eldiario.es/tecnologia/shoshana-suboff-forma-socavar-dividendo-genera-vigilancia-tecnologica-haciendola-ilegal_128_6137458.html

Schechner, S. (2019, febrero 22). You Give Apps Sensitive Personal Information. Then They Tell Facebook. *The Wall Street Jornal.* https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

Schwab, P. (2021, 17 de abril). *Cloud Act y GDRP ¿Podemos guardar nuestros secretos en la nube?* Into the minds. https://www.intotheminds.com/blog/es/cloud-act-gdpr/

See You (s.f). *Privacy.* https://view-seeyouyima-com.translate.goog/users/privacy.html?app_id=1&_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es

Serrano, B. (2019, agosto 8). Para clínicas de fertilidad o seguros privados: así usan las compañías tecnológicas tus datos sobre la regla. *El País.* https://smoda.elpais.com/feminismo/como-las-companias-tecnologicas-usan-tus-datos-sobre-la-regla/

Setton, R., Tierney, C. y Tsai, T. (2016). The Accuracy of Web Sites and Cellular Phone Applications in Predicting the Fertile Window. *Obstetrics & Gynecology 128*(1), 58-63. https://doi.org/10.1097/aog.0000000000001341

Siapka, A. & Biasin, E. (2021). Bleeding data: the case of fertility and menstruation tracking apps. *Internet Policy Review, 10*(4). https://doi.org/10.14763/2021.4.1599

Simple Design (s.f). *Privacy.* http://simpledesign.ltd/privacy/my_calendar.html

Simple Innovation (s.f). *Privacy policy.* https://www.simpleinnovation.us/my-calendar/privacy-policy

Snowden, E. (2019). *Vigilancia Permanente.* Planeta. https://catedradatos.com.ar/media/Vigilancia-permanente-Edward-Snowden.pdf

Sobrino, I. (2021). Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos. *Revista de Derecho Comunitario Europeo, (68),* 227-256. https://dialnet.unirioja.es/servlet/articulo?codigo=7880244

Stuntz, W. (1995). Privacy's Problem and the Law of Criminal Procedure, *Michigan Law Review, (* 93), 1016-1026 (Citado por Lessig en el Código 2.0)

Supremo de EEUU desestima caso de Microsoft sobre las fronteras de Internet (2018, junio 17). *La Vanguardia.* https://www.lavanguardia.com/vida/20180417/442667169436/supremo-de-eeuu-desestima-caso-de-microsoft-sobre-las-fronteras-de-internet.html

Romero, S. (2022 febrero 3). Tinder y otras apps comparten nuestros datos, según un nuevo estudio. *Muy Interesante.* https://www.muyinteresante.es/tecnologia/11009.html

Tonon, G. (2011). La utilización del método comparativo en estudios cualitativos en ciencia política y ciencias sociales: diseño y desarrollo de una tesis doctoral. *Revista de Temas Sociales. (27)* https://dialnet.unirioja.es/descarga/articulo/3702607.pdf

Torchinsky, R. (2022, junio 24). How period tracking apps and data privacy fit into a post-Roe v. Wade climate. *NPR.* https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

Vaquero, E. (2023 enero 18). Nuestras reglas en los tribunales. *Pikaramagazine.* https://www.pikaramagazine.com/2023/01/nuestras-reglas-en-los-tribunales/

Varea, R. (2019, junio 7). Pontificia Universidad Javeriana, la huella de Colombia en la región. *El País.* https://elpais.com/sociedad/2019/06/03/actualidad/1559522175_313057.html

Vidal, C. y Merchant, J. (2022). Ethical challenges of using digital menstrual tracking apps for birth control and conception. *Inserm.* https://www.hal.inserm.fr/inserm-03830965/document

Worsfold L, Marriott L, Johnson S, Harper JC. (2021). Period tracker applications: What menstrual cycle information are they giving women? *Women's Health, (17),* 1-8 https://doi.org/10.1177/17455065211049905

Zimmerman (1999). Why I wrote PGP. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Zuboff, S (2020). *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder.* Paidos. https://cloudflare-ipfs.com/ipfs/bafykbzacedsz5wvf6mb7wugrbxznbkiya6pkpgf2rofnbcdanief37fv7e2mg?filename=Shoshana%20Zuboff%20-%20La%20era%20del%20capitalismo%20de%20la%20vigilancia-Paid%C3%B3s%20%282020%29.pdf

ANEXO

INFORMACIÓN GENERAL SOBRE LAS APPS	EMPRESA DESARROLLADORA	FUNDADORES/AS DE LA EMPRESA	UBICACIÓN DE EMPRESA MATRIZ	UBICACIÓN DESARROLLADOR DE LA APP	PATROCINADORES DE LA APP	DESCARGAS EN PLAY STORE	VALORACIÓN EN PLAY STORE (SIENDO 5 EL MÁXIMO)
MI CALENDARIO MENSTRUAL	Simple Design Ltd			Tortola (British Virgin Isla		Más 100 M	4,9
FLO	Flo Health In	Dmitry y Yuri	Reino Unido	Reino Unido	Flint Capital,	Más 100 M	4,7
CLUE	BioWink	Ida Tin, Hans	Alemania	Berlin (Alem	Union Squar	Más 10M	4,7
MEET YOU	Meet you-Period tracker		Xiamen,Chir	Serangoon road (Singapur		Más 10M	4,9
CALENDARIO MENSTRUAL	SimpleInnovation			Redmond (EEUU)		Más 10M	4,9
ALERTA PERIODO	GP International LLC			Murrieta, California (EEUU		Más 10M	4,6

DATOS QUE RECOGE LA APP EN EUROPA	UBICACIÓN	CÓDIGO DE PAIS DE LA TARJETA SIM	DIRECCIÓN IP	INFORMACIÓN SOBRE HARDWARE Y SOFTWARE DE TU DISPOSITIVO	INFORMACIÓN PERSONAL (Nombre, correo electrónico, Ids de usuario)	INFORMACIÓN FINANCIERA (Historial de compras app store o google play)	INFORMACIÓN DE SALUD Y FITNESS	MENSAJES	FOTOS Y VÍDEOS	INTERACCIONES/ACTIVIDAD EN DE LA APLICACIÓN	NAVEGACIÓN WEB (Historial)	INFORMACIÓN Y RENDIMIENTO DE APLICACIONES	IDS DE DISPOSITIVO O DE OTRO TIPO
MI CALENDARIO MENSTR	NO	NO	SI	SI	SI (Nombre y	NO	SI (opcional)	SI	NO	SI	NO	SI	SI
FLO	SI	NO	SI	SI	SI (Nombre y	SI (opcional)	SI	SI (opcional)	SI (opcional)	SI	NO	SI	SI
CLUE	SI	NO	SI	SI	SI	NO	SI	NO	NO	SI	NO	SI	SI
MEET YOU	NO	SI	SI	SI	SI (Correo el	SI	SI	SI (correos e	SI (opcional)	SI	SI	SI	SI
CALENDARIO MENSTRUAL	NO	NO	NO	SI	SI (Nombre y	NO	SI (opcional)	NO	NO	SI (opcional)	NO	SI	SI
ALERTA PERIODO	NO	NO	SI	SI	SI (opcional)	SI (opcional)	SI (opcional)	SI (opcional)	SI (opcional)	NO	NO	SI	SI