EL IMPACTO DE LA TRANSFORMACION DIGITAL EN EL SISTEMA DE JUSTICIA PENAL

Ana Isabel Cerezo Domínguez

Introducción

El rápido desarrollo de las nuevas tecnologías ha propiciado una repercusión importante en todos los sectores de la sociedad. La ola de transformación digital que embulle a nuestra sociedad es palpable en nuestra vida diaria, e imparable, ya no hay forma de impedir su evolución constante. Disponemos de los medios tecnológicos más avanzados en nuestra vida personal, para comunicarnos y relacionarnos con los demás. Y también para cometer delitos. Nadie pone ya en duda que la red es un nuevo espacio en el que surgen nuevas oportunidades delictivas y las nuevas tecnologías son unos instrumentos idóneos para facilitar la comisión de determinados delitos. Sin embargo, apenas ha trascendido el enorme esfuerzo que se está llevando a cabo desde el sistema de justicia penal en utilizar estas tecnologías para detectar, prevenir, identificar, perseguir y castigar estas nuevas formas criminales, que muchos denominan ciberdelincuencia (Chapman, 2016). Y subrayo lo del enorme esfuerzo, porque se trata de uno de los sectores de la administración pública en los que esta transformación digital está costando más de lo esperado, ya que en determinados aspectos parece encontrarse anclada aún en el siglo XX.

La evolución llevada a cabo en los últimos años en el sistema de justicia penal hace necesaria la puesta en marcha de programas para la transformación digital que incorporen las tecnologías disruptivas precisas. Toda esta transformación digital, conocida como cuarta revolución industrial, se define como "aquella que se basa en la disponibilidad en tiempo real de toda la información relevante al producto, proporcionada por una red accesible en toda la cadena de valor" (Barona, 2019). Esto se consigue con la digitalización y la unión de tecnologías tales como Internet, *big data* y la ciberseguridad. Quisiera destacar en este sentido la importancia que ha ido adquiriendo especialmente la inteligencia artificial (*big data*). El almacenamiento de datos no es nuevo. Lo que es novedoso es la capacidad de almacenamiento de los datos, que se ha incrementado exponencialmente en los últimos años, permitiendo que las administraciones dispongan de enormes bases de datos. La pregunta es por qué esos datos no se utilizan de forma apropiada dadas las enormes ventajas que nos pueden proporcionar. El potencial de la aplicación de las tecnologías basadas en inteligencia artificial especializadas en el ámbito del sistema de justica penal puede contribuir sin duda y de forma notable a una mejora del mismo.

El objetivo del presente capítulo es destacar aquellos programas en los que la transformación digital ha calado en este sector de la administración pública, tanto en el ámbito policial como en el judicial o en el penitenciario. Como es del todo imposible profundizar en este trabajo en cada uno de estos aspectos, vamos a enumerar en esta

introducción algunos ejemplos de aplicación de las nuevas tecnologías en estos entornos. De este modo podemos aludir a las cámaras de videovigilancia en la vía pública, al uso de drones, al uso de redes sociales, al reconocimiento facial, al análisis de teléfonos móviles para rastrear el patrón de movimientos de un sospechoso o al uso de imágenes satélites para la teledetección de delitos, entre muchos otros.

Dada la limitada extensión del presente trabajo nos vamos a centrar únicamente en aquellos aspectos que en nuestra opinión merecen ser comentados de forma más exhaustiva, ya que se trata de programas que han sido más desarrollos que los anteriormente mencionados. Así, aludiremos al sistema de información geográfica (SIG), al sistema de seguimiento integral en caso de violencia de género (VioGen), a la modernización de los tribunales de justicia (e-justice) y a la aplicación de las nuevas tecnologías en el sistema penitenciario español (el control telemático).

1. El sistema de información geográfica (SIG)

El SIG se puede definir como una base de datos que tiene la capacidad de manejar datos específicos sobre el mundo real y representarlos en forma de imágenes. Es decir, el SIG es una tecnología que maneja información geográfica a través de equipos informáticos. Este sistema se puede incluir en lo que se denomina criminología ambiental, ya que consiste en analizar los datos geográficos de la delincuencia y trazar tendencias delictuales a raíz de ellos.

Su antecedente más remoto se sitúa alrededor de los años 60, cuando los mapas del delito se utilizan por primera vez como herramienta propia de la prevención situacional del delito. Tenían la finalidad de conocer las tendencias delictivas que aparecían en un determinado lugar, lo que permitía llevar a cabo medidas para prevenir esos delitos. En España se usó por primera vez en las olimpiadas de Barcelona en 1992 y posteriormente en el marco del programa "Policía 2000" de la Dirección General de Policía (Alonso, 2002).

Desde entonces hasta ahora, estas herramientas han evolucionado notablemente, de tal forma que hoy en día el SIG permite la digitalización de los datos geográficos, su integración en la base de datos, y su posterior análisis que culmina con la plasmación cartográfica de los resultados en forma de mapa, tabla o gráfico. En el ámbito policial, este sistema tiene dos vertientes, la espacial, que se refiere a mapas y representaciones cartográficas, y la temática, que consiste en tablas con información alfanumérica. Además, el SIG cuenta con puntos calientes (*hot spots*) que nos muestran los lugares donde se concentra mayoritariamente los delitos. Esto se representa en el mapa a través de diferentes colores donde el rojo es el ítem más elevado, lo que se traduce en que el número de delitos en ese punto concreto es superior a la media general de la ciudad que se esté analizando (Stangeland y Garrido, 2004).

La gran ventaja que tiene este sistema es la demostración visual que ofrece de los datos con una perspectiva más o menos amplia en función de la zona que se quiera conocer. Pero no es la única. Hay otra serie de ventajas, como el desarrollo de mapas, para poder saber la localización y los autores de los hechos relacionados con el mobiliario urbano y todos los servicios públicos, mejorar la seguridad vial, realizar controles de alcoholemia teniendo en cuenta las zonas con mayor afluencia de gente en relación con el ocio

nocturno, realizar mapas con puntos calientes donde se consuma bebidas alcohólicas en la vía pública, etc (Medina, 2013).

2. El sistema de seguimiento integral en caso de violencia de género: El Sistema VioGen

Las TIC no se usan por parte de las fuerzas policiales únicamente para la investigación de personas presuntamente sospechosas con la finalidad de obtener pruebas que puedan inculparlas durante la fase de plenario o juicio oral en un proceso penal, sino que también se han aprovechado sus ventajas para proteger a las víctimas. En este sentido, una de las principales novedades que ha supuesto el desarrollo tecnológico en el sistema de justicia penal español ha sido el Sistema VioGen (González y Garrido, 2015).

Se trata de una aplicación informática que permite realizar consultas a la base de datos de víctimas de violencia de género con el objeto de permitir su seguimiento integral y facilitar el trabajo que tienen encomendado los diferentes especialistas policiales en su prevención y protección.

Es en el año 2004 cuando el Ministerio del Interior elabora una aplicación a la que solo podían acceder los Cuerpos y Fuerzas de Seguridad del Estado y otras instituciones autorizadas (Instituciones Penitenciarias o Servicios sociales, entre otras), con el objetivo de realizar acciones de seguimiento y coordinación en materia de violencia de género. Pero no es hasta 2007 bajo la Instrucción 10/2007 de 10 de julio, cuando se aprueba el Protocolo para la valoración policial de la mujer de riesgo de violencia contra la mujer en España. El protocolo se basa en una serie de actuaciones policiales encaminadas a determinar si existe riesgo y la intensidad de este para tomar las medidas que sean oportunas para proteger de forma inmediata la vida, la integridad y los derechos de las víctimas tanto directas como indirectas.

El sistema VioGen persigue los siguientes objetivos:

- Unir y coordinar todas las instituciones públicas que tienen competencias en materia de violencia de género para dar una respuesta eficaz, facilitando toda la información que tenga cada una de ellas.
- Efectuar valoraciones por parte de las Fuerzas y Cuerpos de Seguridad del Estado sobre el riesgo existente.
- Llevar a cabo unas u otras medidas de protección, según el nivel de riesgo estimado.
- Facilitar la valoración del riesgo de que haya nuevos actos violentos.
- Recopilar toda la información de interés de cara a la elaboración de un plan de seguridad personalizado para la víctima.
- Facilitar la labor preventiva cuando haya algún hecho que ponga en peligro a la víctima.

Para valorar correctamente el riesgo que tienen las víctimas de violencia de género se deben tener en cuenta los factores de riesgo y de protección en función al tipo concreto de delincuencia, por lo que debemos atenernos a la información que se tenga de cada caso concreto y alejarnos de la concepción de que hay unos parámetros comunes a cualquier

tipo de violencia[1]. Cuando una mujer víctima de violencia de género llega a las disposiciones policiales, se le aplica en primer lugar el formulario de Valoración Policial del Riesgo (VPR)[2]. Dicho formulario está compuesto por 39 indicadores, de mayor a menor riesgo, que se agrupan en cuatro categorías: historia de violencia, que se refiere a la gravedad del hecho que se denuncia y el historial violento de la pareja; factores relacionados con el agresor, dividiéndose a su vez en la relación de pareja (celos, control, acoso), las características antisociales y violentas, e indicadores psicopatológicos; factores relacionados con la vulnerabilidad de la víctima y la calidad de la relación; y la percepción subjetiva de la víctima sobre su propio riesgo y el de los familiares más cercanos y sobre la relación. Estos datos son posteriormente dados de alta en una base de datos electrónica, cuando el caso sea nuevo, o actualizados si coinciden agresor y/o víctima. Gracias a este protocolo se otorga una valoración inicial del riesgo, aunque se puede posteriormente corregir o modificar el resultado que otorga automáticamente este

[1] Cuando hablamos de factores de riesgo nos estamos refiriendo a determinadas conductas o características por parte de la víctima, del agresor o incluso del contexto, que fomentan la posibilidad de que se produzca un acto violento (Kroop, 2008). Podemos distinguir entre dos tipos de factores de riesgo: Los factores de riesgo estáticos son los que pertenecen al pasado y no pueden ser modificados, como la infancia o adolescencia de alguna de las partes, los hijos, etc. En cambio, los factores de riesgo dinámicos pueden modificarse a lo largo del tiempo (tipo de relación que se tenga con una pareja, situaciones puntuales como una separación, un juicio, etc.) y esa fluctuación, tanto para mejor como para peor, va a estar relacionada directamente con la mayor o menos probabilidad de que se cometa el hecho violento. Esta diferenciación se realiza porque, aunque los dos condicionan el comportamiento futuro del agresor, los factores de riesgo dinámicos pueden ser corregidos con tratamientos o terapias adecuadas, mientras que los estáticos pueden ser buenos indicadores en tanto en cuanto permiten hacer una valoración estable en el tiempo, pero no se pueden modificar. Por lo tanto, para una valoración adecuada es necesario tener en cuenta ambos factores de riesgo. En cuanto a los factores de protección, se afirma que hay determinadas características que tienen un efecto protector, por lo que la inhibición de la conducta violenta, según Garrido (2005), va a depender del número y la intensidad de los factores de protección. Sin embargo, debemos tener en cuenta que esta afirmación no es absoluta, es decir, que haya factores de riesgo no implica obligatoriamente que llegue a explosionar el hecho violento, y viceversa, que no haya factor de riesgo no lleva implícito que esa persona nunca vaya a cometerlo. La relación entre ambos factores va a depender de cada caso concreto, ya que cada uno influye de una manera diferente en cada caso.

[2] Los instrumentos para valorar el riesgo de violencia contra la mujer en España son los siguientes:

- Escala de Predicción del Riesgo de Violencia Grave contra la pareja –Revisada (EPV-R): Se trata de veinte elementos agrupados en cinco grupos que se ponderan en función de su capacidad discriminativa para poder predecir la violencia grave donde existen tres niveles: bajo, moderado o alto.
- Protocolo de Valoración del Riesgo de Violencia contra la mujer por parte de su pareja o expareja (RVD-BCN): Valora el riesgo a corto plazo y está compuesta de dieciséis factores donde de incorporan algunos como la vulnerabilidad y la percepción del riesgo que tiene la mujer.
- Protocolo de Valoración Policial del Riesgo de Reincidencia en Violencia de Género (VPR y VPER): Este es el sistema VioGen en el cual se valora el riesgo a través de formularios de Valoración Policial del Riesgo y Valoración Policial de la Evolución del Riesgo (VPR y VPER).

El primero de ellos ofrece una valoración inicial del riesgo, ya que se clasifican los casos y se les asignan determinadas medidas de carácter urgente. Posteriormente los agentes usan el segundo formulario para la monitorización y el seguimiento del caso. Este formulario guarda una gran similitud con el Protocolo multiescala de valoración del riesgo Riscanvi. Este protocolo permite pronosticar el riesgo que tiene el sujeto de cometer conductas violentas en un futuro. Concretamente pronostica el riesgo de cometer violencia institucional, quebrantamiento de condena, violencia hacia él mismo o la reincidencia en relación al mismo hecho que ya ha cometido (Andrés-Pueyo, 2013).

protocolo. Además, se cuenta con un sistema informático online y multiagencia, es decir, se pueden conectar miles de usuarios de manera simultánea y de diferentes entornos, ya sea policial judicial, social o penitenciario, para hacer una correcta valoración inicial del riesgo.

Una vez respondido el cuestionario, el caso se va a calificar en uno de los cinco niveles de riesgo, estos son, extremo, alto, medio, bajo o no apreciado. En función del nivel de riesgo que se estime, los agentes llevarán a cabo las medidas de protección que estimen oportunas[3]. Posteriormente los agentes usan el segundo formulario, la Valoración policial de la evaluación del riesgo (VPER) para la monitorización y el seguimiento del caso (López Ossorio, González Alvarez y Andrés Pueyo, 2016). Este formulario se suele cumplimentar una vez finalizado el juicio en el que se resuelve la solicitud sobre la orden de protección o la solicitud de cualquier otra medida cautelar. Este protocolo permite pronosticar el riesgo que tiene el agresor de cometer conductas violentas en un futuro. Concretamente pronostica el riesgo de cometer violencia institucional, quebrantamiento de condena, violencia hacia él mismo o la reincidencia en relación al mismo hecho que ya ha cometido. Esta reevaluación posterior permite realizar valoraciones periódicas y así modificar y reajustar la protección que la víctima necesita en ese momento posterior. Está compuesto por 43 indicadores, tanto de factores de riesgo (34 indicadores) como de protección (9 indicadores), estáticos y dinámicos, y realiza un pronóstico autónomo mixto, es decir, tiene en cuenta ambos factores para poder evaluar la probabilidad de reincidencia e ir monitorizando los cambios que se van produciendo a lo largo del tiempo para poder actuar cuando sea necesario. Todos estos ítems se agrupan en 5 dimensiones de las cuales cuatro de ellas son las mismas que en el cuestionario anterior (historia de violencia, factores relacionados con el agresor, factores relacionados con la vulnerabilidad de la víctima, y la percepción de la víctima sobre su situación) y una nueva

[3] Si el *riesgo es no apreciado*, se le facilita a la víctima la misma información que a cualquier otro ciudadano. En este sentido se le aportan contactos telefónicos como oficinas de atención a víctimas de delito o servicios sociales. También se incluyen ciertos conocimientos sobre materia de autoprotección a nivel general. Sin embargo, también se le insta a la víctima a que aprenda qué circunstancias son las más probables a sufrir riesgo en su caso concreto y que aprenda a cómo poder contrarrestarlas o evadirlas. Si el *riesgo es bajo*, en cuanto a información se refiere, se le facilitan ciertos contactos con Fuerzas y Cuerpos de Seguridad de atención permanente, es decir, las 24h al día. También se le informa sobre el servicio de tele asistencia móvil o los servicios sociales más próximos a su lugar de residencia. En cuanto al ámbito operativo, se le facilita a la víctima ciertas llamadas periódicas o visitas presenciales por las FFCCS, bien con vehículos discretos, bien con los oficiales, según esta determine. Además, también se le informará sobre posibles resoluciones judiciales de ámbito civil, como custodia de hijos o separación de bienes, que puedan provocar un aumento en el riesgo de ser víctima. Si el *riesgo es medio*, a partir de este nivel, ya no se opta por ninguna medida de carácter informativo, sino que todas son en formato operativo. En estos casos, lo más frecuente es tener una entrevista con la víctima, efectuar un traslado a un centro de acogida, si procede, llevar a cabo un control periódico en ciertos momentos del día y lugares, como su lugar de residencia, trabajo o centro escolar de los hijos/as o el acompañamiento de la víctima a procedimientos judiciales, cuando se estime un riesgo en su integridad. Si el *riesgo es alto*, se va a hacer especial hincapié a la víctima de la urgente necesidad de ser trasladada a un centro de acogida, siempre que no se haya identificado el paradero previamente del agresor. Se le otorga el mismo control descrito en el caso anterior, pero con mayor frecuencia, además de contactar con personas de su entorno para facilitar información y una mejor protección. Por último, si el *riesgo es extremo*, las medidas consisten en la vigilancia continua de la víctima y de los menores cuando entrañe un riesgo o amenaza inminente, control de cada movimiento que haga el agresor, etc. También se encargan de la vigilancia frecuente o aleatoria de la víctima y los menores, intentar que la víctima se traslade a otro domicilio o a un centro de acogida de manera provisional hasta que se detenga al autor, control telemático al agresor, etc.

que son las que monitorizan el riesgo y van modificando las medidas de protección a lo largo del tiempo[4].

Como aspecto relevante, el VioGén también se encarga de dar una serie de pautas para la protección de la persona en el ámbito virtual, es decir, a través de las TIC. En este sentido, hace recomendaciones tales como:

- Restringir el acceso del perfil o perfiles de la víctima a algunas personas.
- Utilizar perfiles cuyo nombre identificativo no sea el nombre real.
- Rechazar cualquier solicitud de amistad que pueda estar relacionado con el entorno del agresor.
- Evitar a toda costa la difusión de información relativa al ámbito personal, como ubicaciones en tiempo real o contenido multimedia como fotografías o vídeos.

3. La e-justicia: El proceso de transformación digital en la Administración de Justicia

El proceso de transformación digital de la Administración de justicia se traduce a través de distintas líneas de acción enmarcadas en las iniciativas legislativas en materia de administración electrónica que apoyan y regulan el proceso de modernización de la administración de justicia española. Las tecnologías a las que nos referimos tienen una aplicación muy diversa que podemos clasificar según el grado de complejidad y el nivel de interacción que tenga con los diferentes operadores jurídicos. En cuanto a su uso, éstas se pueden clasificar en:

- El tratamiento de la información: Es el uso más importante que se le otorga a las nuevas tecnologías y la base sobre la que se sustentan los demás. Se basa en transmitir información procedente de la Administración de Justicia. El tratamiento de la información aumenta la trasparencia, lo que aleja la corrupción judicial, agiliza la transmisión de información entre los operadores jurídicos y entre los ciudadanos. Todo ello conlleva un aumento de la calidad de la justicia.
- La gestión de los expedientes judiciales: Esto conlleva una mejora en la eficacia de la administración basándose en la modernización de las oficinas judiciales. Un ejemplo de ello es la propuesta en España de eliminar totalmente el formato papel en los procesos judiciales.
- La relación entre la Administración y los operadores jurídicos: Lo que facilita y mejora las relaciones entre las diferentes oficinas u operadores y los ciudadanos, aumentando así la eficacia de la Administración. A través de la digitalización de

[4] Esta valoración del riesgo a lo largo del tiempo se puede realizar a través de una evolución positiva de los casos o una evolución negativa, dependiendo de si se han registrados nuevas incidencias o no las ha habido. En el caso de que se haya producido una incidencia, se estudia el hecho para saber los motivos y las características de la misma. Si fuera necesario, tras la evaluación, se puede adoptar otro nivel de riesgo superior al que el agresor tenía previamente y, por consiguiente, nuevas y más restrictivas medidas de protección. En el caso de que no se haya producido ninguna incidencia, se va reduciendo el nivel de riesgo progresivamente hasta que llegue al nivel de Riesgo No Apreciado. Cuando se llegue a este nivel, se le comunica a la autoridad judicial competente y el Sistema VioGén pasa a estar inactivo para el agresor, en el caso de que no tenga este sistema como medida cautelar de protección, ya que dado el caso será el juez quien decida cuando pasa a estar inactivo.

determinados formularios o escritos judiciales, el usuario puede descargar estos documentos para firmarlos y enviarlos por correo electrónico a su abogado, o remitirlo directamente a las oficinas judiciales en los casos que sea pertinente.

La modernización tecnológica de la administración de la justicia comienza en España en 1997 con el Libro Blanco de la justicia. Fue la primera vez que se valoró la necesidad de una reforma judicial. Pero no fue hasta 2002 cuando se configuró el Pacto de Estado para la Reforma de la Justicia. En 2007 se aprueba el Plan de modernización de la Justicia con el fin de perfeccionar la administración en cuanto a innovación tecnológica, a través del Real Decreto 84/2007, de 26 de enero, sobre la implantación en la Administración de Justicia del sistema informático de telecomunicaciones LexNet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos. Este plan está coordinado por la Comisión de Modernización e Informática que se ocupa de analizar y verificar los programas y las aplicaciones informáticas a nivel nacional y autonómico, mejorar los sistemas informáticos de gestión procesal e introducir las mejoras que sean necesarias en cada ocasión.

El 5 de julio de 2011 se aprueba la Ley 18/2011, que regula actualmente el uso de las tecnologías de la información y la comunicación en la Administración de Justicia. Junto al Real Decreto 396/2013, de 7 de junio, son el pilar jurídico de los nuevos sistemas de gestión procesal que han de permitir el desarrollo de la e-Justicia en España. Los principales objetivos son aprovechar el uso de las tecnologías para agilizar todas las actuaciones judiciales con el objetivo de llegar a obtener procesos sin dilaciones indebidas, y generalizar ese uso para todos los profesionales de la justicia. También otorga a los ciudadanos el derecho de comunicarse de manera electrónica con la Administración, aunque eso ya estaba establecido en la Ley 11/2007 de 22 de junio, a través de la cual ya se planteaba la necesidad de crear un sistema que permitiera, tanto a los ciudadanos como a los profesionales, acceder a los servicios de justicia a través de internet, creando sedes judiciales electrónicas o páginas webs en las que se pudiera realizar diferentes actos procesales.

Es oportuno aludir asimismo al llamado Punto Neutro Judicial (PNJ). Se puede definir como una red que conecta diferentes administraciones y órganos dentro de ellas para ofrecer a los órganos judiciales los datos que necesiten a la hora de hacer cualquier tramitación judicial. Esta red otorga acceso directo a las bases de datos del Consejo General del Poder judicial, de la Administración General del Estado y de otras instituciones para así facilitar los trámites y evitar dilaciones indebidas, al igual que también se permite la conexión entre estos órganos y entidades financieras externas, registros, etc. Los objetivos que tiene esta aplicación son otorgar ayuda a los órganos judiciales en cuanto a asuntos de gestión se refiere, proporcionar ayuda al juez, automatizar la gestión de los órganos para favorecer su rapidez y facilitar la compatibilidad y organizar los diferentes sistemas informáticos que tiene la Administración de Justicia. Se inició en 1995 con la petición de la Agencia Tributaria a la Administración de justicia para que se pudiera acceder automáticamente a los datos judiciales, pero este acuerdo se fue ampliando cada vez a más organismos. De hecho, actualmente el PNJ sirve de conexión entre, por ejemplo, el CGPJ y DGT, el Catastro, Instituciones Penitenciarias, Seguridad Social, SEPE, entre otros.

Otra de las medidas que forman parte de la transformación digital de la administración de justicia es la videoconferencia, de tal modo que determinadas actuaciones previas al juicio oral se pueden realizar a través de esta modalidad para que la persona no tenga que desplazarse a las dependencias judiciales si no fuera necesario. Además, en la Carta de

Derechos del Ciudadano que se aprobó en 2002 se establecía que la comparecencia de los sujetos ante los órganos judiciales debía ser lo menos gravosa posible. No es necesario que esté presente el letrado de la administración, ya que en este tipo de actuaciones no se levanta acta y su función se quedaría supeditada a identificar al interviniente y ver que se están cumpliendo todos los requisitos formales. Algunos ejemplos de las actuaciones que se pueden realizar mediante videoconferencia son las declaraciones testificales o pruebas periciales, interrogatorios de parte, etc.

Sin embargo, los cambios que han producido las nuevas tecnologías en el sistema judicial no quedan reducidas a las actuaciones previas al juicio oral, sino que también han permitido que en determinadas circunstancias el acto oral se pueda realizar de manera telemática. Bien es cierto que antes de la pandemia que estamos viviendo, este tipo de juicios no tenían casi presencia en nuestro país, pero el desarrollo de las nuevas tecnologías ha hecho que la justicia no se pare por completo durante este año y medio, sino que se ha amoldado a la situación pandémica y, como muchos autores afirman, el juicio telemático ha llegado para quedarse. El Ministerio de Justicia ha creado una aplicación llamada "Cisco Meeting" para que se realicen tanto actuaciones previas como el propio acto judicial, afirmando que este cumple con todas las garantías de seguridad y confidencialidad necesarias para realizar estas actuaciones, ya que cada sala virtual cuenta con dos claves, la de moderador y la del invitado, además de un enlace que solo tendrán ambos. Según la guía que ha elaborado el Ministerio de Justicia, este sistema de videoconferencia es óptimo para actuaciones internas entre los propios órganos judiciales, entre los operadores jurídicos y para el propio ciudadano. Esta nueva manera de llevar a cabo los juicios permite agilizar su celebración, ya que como sabemos, el sistema judicial español se caracteriza por la sobrecarga de trabajo que tiene. También se evita que los diferentes profesionales tengan que desplazarse de un lugar a otro, por lo que la espera entre juicio y juicio, y el coste que este supone también son menores. Y una de las mayores ventajas que tiene es que se minimiza la revictimización y la victimización secundaria de la víctima, sobretodo en los juicios de carácter penal donde la víctima tiene que ir a declarar al juzgado en presencia física de diferentes operadores jurídicos y del acusado.

4. La implantación de las nuevas tecnologías en el ámbito penitenciario

El control telemático es la tecnología que utiliza la Administración Penitenciaria, para realizar el seguimiento a distancia de aquellas personas acusadas o condenadas por un hecho delictivo (Arenas, 2018). Actualmente hay diferentes dispositivos para llevar a cabo este seguimiento, aunque en España generalmente se usan dos: los dispositivos que permiten saber si una persona está o no en el lugar que se le ha determinado y los que controlan los movimientos sin necesidad de que la persona tenga que estar en un lugar en concreto. Según el tipo que se utilice, se estará ejerciendo un mayor o menor control sobre el sujeto y sobre su libertad de circulación y autonomía.

Cuando hablamos del primer modelo, nos estamos refiriendo a la monitorización estática o de primera generación. Este tipo nos permite saber la presencia o no de una persona en el lugar que se le ha indicado previamente. Se hace a través de un teléfono fijo en el domicilio del sujeto o de pulsera adherida a la muñeca o al tobillo. Si el dispositivo tiene una especie de "walkie-talkie" con un emisor y un receptor de llamadas de voz estaríamos hablando de un sistema de verificación por voz. Este sistema se basa en llamadas aleatorias al domicilio del sujeto. Este tiene que contestar todas las veces que se produce

la llamada, de lo contrario consta como una ausencia y automáticamente se envía una alerta al centro de control. Antes de conectar el teléfono en su domicilio, al sujeto se le hacen diferentes pruebas fonéticas para verificar la voz de la persona y determinarlas como propias, de tal modo que, cuando se le llame y conteste, el sistema sea capaz de analizar la voz y saber si la identidad es la correcta o no. Es decir, la verificación se realiza a través de patrones vocales. En algunas ocasiones, en lugar de realizar la comprobación a través de llamadas aleatorias, se avisa al sujeto de que tiene que estar en el domicilio en determinadas horas concretas y se le llama por teléfono entonces para verificar si realmente se encuentra allí. Otra modalidad es el sistema de verificación con vídeo y respiración. Se trata de una mezcla del sistema de radiofrecuencia con un novedoso sistema de reconocimiento vocal y facial. Se coloca una cámara en el domicilio del sujeto y cuando tiene que verificar su ausencia o presencia, se coloca delante de la cámara y la imagen se transmite al centro de control que se compara con la foto del expediente para saber si es la misma persona. En los casos de personas condenadas por un delito relacionado con la bebida, además del control de la imagen se suele colocar una especie de boquilla para que sople y el sistema determina si ha estado bebiendo durante el tiempo que no ha tenido seguimiento o si por el contrario sigue cumpliendo las normas.

Si en cambio, el mecanismo emisor-receptor se hace a través de mensajes que llegan a una base conectada a un servidor de datos que controla a la persona, independientemente del lugar en el que se encuentre, estaríamos hablando de una monitorización por radiofrecuencia con dispositivo portátil. Se trata del mismo mecanismo que los casos anteriores. Es decir, en el domicilio hay un sistema fijo desde el cual, en el caso que fuera necesario, se podrán recibir llamadas desde el centro de control. Sin embargo, a diferencia de los casos anteriores, lo que transmite las señales es una pulsera que se coloca el sujeto en la muñeca o en el tobillo, que monitoriza sus pasos en base a la distancia que haya entre el dispositivo fijo y la pulsera (este radio de frecuencia se impondrá en función de las necesidades laborales o familiares), y cuando ambos están dentro de la frecuencia permitida se reconocen y de esa manera se puede saber cuándo este sale de la zona permitida.

Por otro lado, tenemos la monitorización móvil o activa, los sistemas GPS. Este sistema GPS ha ido sustituyendo a los tradicionales sistemas de radiofrecuencia. Como diferencias a destacar, en este caso el sujeto (emisor) sigue llevando una pulsera o una tobillera, pero la señal en vez de a un dispositivo fijo se manda a un teléfono móvil que actúa como receptor. Las señales se van emitiendo, y como el sistema está conectado a diferentes satélites, se puede ver la ubicación exacta del sujeto cada dos minutos, por lo que su control es mucho mayor, reduciéndose solo a las zonas donde no hay vía satélite, aunque incluso ahí el GPS guarda toda la información en su sistema. Además, estos dispositivos son cada vez más pequeños y tienen una autonomía mayor, ya que la batería dura casi 24 horas. Gracias a estos dispositivos el sujeto tiene una libertad de circulación mucho mayor, puede circular por cualquier lado menos por aquellas zonas en las que el juez le haya prohibido ir. El sujeto suele recibir algunas pautas del centro de control y debe ajustar su comportamiento para cumplir en todo momento lo que se le indique. Por ejemplo, puede ser avisado de la batería baja de la pulsera, lo que implica que en los próximos días tiene que ir al centro de control para cambiársela, de la batería baja del rastreador, de la tobillera desaparecida, que implica que la persona está en una zona fuera del rango que cubre la señal y se desconoce la ubicación, de que el transmisor abierto cse ha roto o se lo ha quitado sin permiso, de la pérdida de cobertura o de la entrada a una de las zonas que tiene prohibidas.

Dentro de este tipo de monitorización existe una variante, la móvil bilateral. Aquí el sujeto sigue teniendo una pulsera para controlar sus movimientos, pero el sistema controla también a otro sujeto para poder saber la proximidad o no del individuo respecto de otra persona u otro lugar al que no se pueda acercar. Es decir, ambos tienen un sistema de control, de tal forma que si están unidos se reconocen, se detectan y salta la incidencia al centro de control. Sin embargo, el sistema que tiene la víctima solo queda registrada cuando esté cerca del sujeto con el fin de que la policía pueda saber exactamente dónde está, y el sistema de control del victimario está rastreado siempre. Esto se usa para evitar que el agresor se aproxime a la víctima y para asegurarse en vez de controlar solo sus movimientos, se controlan los movimientos de ambos (Bermudo, 2019).

España hace su primera referencia al control electrónico en el Reglamento Penitenciario de 1996 cuando se introduce la monitorización electrónica como modo de ejecución del tercer grado. De este modo, en el art. 86.4 RP se establece una nueva forma de cumplir la pena privativa de libertad en régimen abierto a aquellos internos clasificados en tercer grado que podrán cumplir el tiempo mínimo establecido (ocho horas) en el domicilio con control telemático en lugar de en los centros penitenciarios. Pero la implantación del control electrónico o telemático se hace efectiva en nuestro país a partir de la Instrucción 12/2006 de la Secretaría General de Instituciones Penitenciarias, por la que se permite a los penados en tercer grado cumplir parte de la condena que le resta en sus domicilios.

En cuanto a la violencia de género, no será hasta el año 2003 cuando se introduzca la posibilidad de aplicar la monitorización para los casos de órdenes de alejamiento, a través de la ley 27/2003, de 31 de julio, reguladora de la orden de protección de las víctimas de la violencia doméstica. Se introduce definitivamente como medida cautelar penal de alejamiento en el art. 63.4 de la ley orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género. Sin embargo, no será hasta el año 2009 cuando se apruebe el protocolo de Sistemas de Seguimiento por Medios Telemáticos de las Medidas de Alejamiento en Materia de Violencia de Género y se pondrán en marcha los primeros dispositivos de control telemático a alguien imputado por un delito de violencia de género. Esta medida se pone en marcha una vez que el Juez ha visto los informes de la policía a través del sistema VioGén determinando el riesgo existente para la víctima, de los servicios sociales e instituciones penitenciarias.

El control telemático como pena se introduce a través de la localización permanente (art. 37 CP) y de la pena de alejamiento a las víctimas de violencia de género (art. 48 CP).

Finalmente, a través de la reforma del Código penal propiciada por la LO 5/2010, de 22 de junio, se incorpora una medida no privativa de libertad y postpenitenciaria, la libertad vigilada. Se trata de una medida basada en tener localizado continuamente al sujeto a través de los nuevos medios electrónicos. Esta medida, que empezó aplicándose solo en condenados por delitos contra la libertad sexual y terrorismo, ha ido expandiendo su ámbito de aplicación, de tal forma que, tras la reforma del código penal de 2015, se puede aplicar también en los delitos de lesiones, contra la vida, contra los malos tratos domésticos y en los casos de violencia de género.

5. Discusión

No hay duda de que las nuevas tecnologías han llegado para quedarse en nuestras vidas. El reto consiste en saber implementar de una forma coherente y eficaz estas aplicaciones y sus ventajas al sistema de justicia penal.

Los datos y el análisis de los datos ya están desempeñando un papel muy importante en la vigilancia predictiva (identificación de personas, lugares y momentos de un mayor riesgo delictivo), así como en el establecimiento de sentencias basadas en el riesgo. Sin embargo, desde Europa nos advierten de que el uso de la inteligencia artificial en el trabajo policial requiere de garantías sólidas de cara a prevenir la discriminación y garantizar el derecho a la privacidad. En la Resolución del Parlamento europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016/(INI)). En dicha resolución se manifiesta la necesidad de que el uso de las aplicaciones basadas en inteligencia artificial se clasifique como de alto riesgo cuando tengan potencial para afectar significativamente la vida de las personas. De esta forma, se señala que los sistemas de inteligencia artificial deben diseñarse de tal forma que protejan y beneficien a todos los miembros de la sociedad, tomando decisiones explicables y transparentes, aspirando a que no se produzcan efectos perjudiciales y respetando siempre los derechos y libertades fundamentales de los individuos. En concreto, se pide que los algoritmos usados en estos sistemas sean explicables, transparentes, trazables y comprobables, a los efectos de asegurar que los resultados generados por dichos algoritmos sean inteligibles para cualquier usuario. Asimismo, se indica que sólo debe permitirse la adquisición por parte de las autoridades policiales de herramientas y sistemas cuyos algoritmos sean auditables y, a tal efecto, se recomienda el uso de software de código abierto siempre que sea posible.

Hemos podido comprobar, que el uso de las tecnologías en la administración de justicia trae consigo numerosos beneficios, tales como el ahorro de tiempo y de trabajo, así como una mayor transparencia y eficacia. Todos los cambios que se están llevando a cabo en los últimos años van encaminados a lograr una Justicia en Red o una Justicia sin papel, caracterizada como ya hemos visto en la digitalización de la información que tradicionalmente ha estado en formato físico y así poder acceder a ella desde cualquier lugar, en la creación del expediente judicial digital, donde se aglutina toda la información judicial de una persona y a la que gracias a la digitalización se va a poder abastecer de éste otros organismos como el Ministerio, CC.AAs, la Fiscalía o la misma judicatura y a la automatización de las gestiones que permite una mayor rapidez y también seguridad gracias a la firma electrónica y el impulso de la videoconferencia y la grabación de los juicios para la agilización de los procesos. Sin duda, la mayor complejidad es la derivada de la transferencia de competencias en materia de administración de justicia a las Comunidades Autónomas que las tienen transferidas, lo que ha dado origen a que actualmente tengamos distinto sistemas informáticos que dan soporte a la gestión procesal. Llegar a esta situación no ha sido casual, sino derivada de varios factores entre los que podemos señalar como de gran importancia: el impacto en el proceso de gestión procesal, así como su repercusión en los distintos ordenes de administración de justicia: Civil, Penal, Administrativo, etc.

Por último, la transformación digital en el ámbito penitenciario no solo se está produciendo de puertas para fuera, el debate actual se centra en la necesidad de implantar en las prisiones españolas el uso de la videoconferencia y el uso de Internet para los internos. Actualmente el acceso a internet a través de los ordenadores del centro es bastante limitado, aunque la Instrucción 2/2007 regula las comunicaciones por videoconferencia tanto para las actuaciones judiciales, como para las consultas médicas y las comunicaciones. Estas últimas se pueden llevar a cabo cuando el interno lo solicite y cuando no haya tenido ningún tipo de comunicación con la familia en los último cuatro meses. Se hace a través de los servicios sociales que se ponen el contacto con la familia

y con el centro penitenciario más próximo a ésta para poder realizarla desde allí. Tiene una duración máxima de 15 minutos y solo se podrá realizar cada cuatro meses. A causa de la pandemia por covid, esta medida ha ido proliferando, con la intención de que no se rompan los vínculos familiares ni haya una ruptura con la sociedad que genere una actitud desmotivada del interno ante la reinserción.

Referencias bibliográficas

Alonso, A. (2002). Desarrollo de la brigada de investigación tecnológica (B.I.T.) del cuerpo nacional de policía en el marco del programa "Policía 2000". En J.A. Ortega Carrillo (coord.), *Educando en la sociedad digital: ética mediática y cultura de paz*, vol. 1, págs. 551-554

Andrés-Pueyo, A. (2013). Valoració del risc i gestió de la reincidència: la utilitat del RisCanvi en la reinserció. En J. Cid, M. Ferrer & A. Ibáñez (Coords.), *De l'execució de penes a la reinserció*. Barcelona: UAB. págs. 67-70

Arenas, L. (2018). Los medios de control telemáticos en el sistema penal español. Valencia: Tirant lo Blanch

Barona Vilar, S. (2019). Cuarta revolución industrial (4.0) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino de la robotización de la justicia. *Revista jurídica digital UANDES*, 3/1

Bermudo Castellano, J.M. (2019). Medios telemáticos en la Administración penitenciaria española. Revista de Estudios penitenciarios. 40 años de Ley orgánica general penitenciaria, págs. 87-101

Casanova, R. (2016). *La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos*. Diario LA LEY. Disponible en : https://diariolaley.laleynext.es/content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAAAEAMtMSbF1CTEAAiMjS0MLc7Wy1KLizPw827DM9NS8klS1xKTi_JzSktTQokzbkKLSVAB0FgTHMQAAAA==WKE. Ultima consulta el 18 de octubre de 2021

Cerezo, A. I., López, J. y Patel, A. (2007). "International cooperation to fight transnational cybercrime", en Preenel, Bart; Gritzalis, Stefanos; Kokolakis, Spyros; Tryfonas, Theo (eds), *Digital Forensic and Incident Analysis*, Ed. IEEE Computer Society, USA, 2007, págs. 13-27.

Chapman, B. (2016). Research on the Impact of Technology pn Policing Strategy in the 21st Century. Final Report. Disponible en https://www.ojp.gov/pdffiles1/nij/grants/251140.pdf. Ultima consulta el 25 de enero de 2022.

Flores, Emilio Javier; Asanza, María Isabel; Berrones, Marcelo, "Ciberdelincuencia un mal que afecta a la sociedad actual", en *Contribuciones a las Ciencias Sociales*, septiembre 2014, págs. 1-14.

Garrido, V. (2005): *¿Qué es la psicología criminológica?*. Madrid: Editorial Biblioteca Nueva.

Gimeno, V. (2011). *La intervención de las comunicaciones telefónicas y electrónicas*. El Notario del siglo XXI. Disponible en: https://www.elnotario.es/index.php/hemeroteca/revista-39/697-la-intervencion-de-las-comunicaciones-telefonicas-y-electronicas-0-2863723191305737. Ultima consulta el 18 de octubre de 2021.

González, J.L. y Garrido, M.J. (2015). Satisfacción de las víctimas de violencia de género con la actuación policial en España. Valoración del Sistema VioGen, *Anuario de Psicología Jurídica*, vol. 25, págs. 29-38

Kroop R. (2008): "*Intimate partner violence risk assessment and management". Violence an Victims*, págs. 202-220.

López-Barajas, I., (2017). *Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos*. UOC, Barcelona.

López Ossorio, J.J., González Alvarez, J.L y Andrés Pueyo, A. (2016). Eficacia predictiva de la valoración policial del riesgo de la violencia de género. *Psychosocial Intervention*, vol. 25, n. 1, págs. 1-7

Loredo, J. A. y Ramírez, A. (2013). "Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo", en *Celerinet*, págs. 44-51.

Medina, J.E. (2013). Prevención de la conducción influenciada por medio de los mapas del crimen. Un análisis desde la aplicación de las teorías criminológicas ambientales a la seguridad vial. Tesis defendida en la Universidad Miguel Hernández de Elche.

Miró, F. (2011). "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", en *Revista Electrónica de Ciencia Penal y Criminología*, Nº 13, 2011, págs. 1-55.

Pérez, M., (2016). *El registro remoto de equipos informáticos como diligencia de investigación en el proceso penal.* Universitat de les Illes Balears. Mallorca.

Picotti, L. (2000): "*Fundamento y límites de la responsabilidad penal de los proveedores de acceso y servicio a internet". Revista de derecho y proceso penal*. págs. 211-232.

Roca, J. L. (2014). *Cibercrimen y ciberterrorismo: ¿exageración mediática o realidad?* Proyecto Fin de Grado, España/Madrid: Universidad Politécnica de Madrid.

Stangeland, P. y Garrido de los Santos, M.J. (2004). El mapa del crimen: Herramientas geográficas para policías y criminólogos. Tirant lo Blanch, Valencia.

Velasco Núñez, Eloy (2016): "*Delitos tecnológicos: definición, investigación y prueba en el proceso penal: actualizado tras la reforma del Código Penal y de la Ley de Enjuiciamiento criminal de 2015".* Valencia: Tirant lo Blanch.