Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

NUEVAS FORMAS DE COMBATIR EL CRIMEN EN INTERNET Y SUS RIESGOS

Javier Valls Prieto

Profesor Titular de Derecho Penal. Universidad de Granada

VALLS PRIETO, Javier. Nuevas formas de combatir el crimen en internet y sus riesgos. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2016, núm. 18-22, pp. 1-36. Disponible en internet:
http://criminet.ugr.es/recpc/18/recpc18-22.pdf
ISSN 1695-0194 [RECPC 18-22 (2016), 14 dic]

RESUMEN: En los últimos años el uso de bases de datos de gran escala por parte del sector público y privado ha aumentado considerablemente. Es una herramienta muy poderosa para predecir situaciones futuras que puedan afectar a la sociedad. En nuestro estudio nos interesa el uso de escáneres para la lucha contra el crimen que utilizan el Big Data para intentar garantizar la seguridad de la sociedad contra los riesgos de nuevas formas de criminalidad. En concreto el uso de Internet por grupos organizados de criminalidad para cometer crímenes está aumentando y muchas veces no hay otra forma efectiva de combatirla que explorando la red.
Por otro lado el uso de bases de datos de gran escala requiere la utilización de una gran cantidad de datos para intentar predecir dónde y cómo se va a desarrollar las nuevas formas de criminalidad o el crimen organizado. Más aun, la gestión de datos, con algoritmos tan potentes, puede revelar datos de los individuos o sobre su personalidad.
Esto implica que tenemos que evaluar y buscar un equilibrio entre los intereses de seguridad y la libertad para mantener el sistema de Derecho en un sistema democrático.

PALABRAS CLAVE: Seguridad, Intimidad, DDoS, Datos masivos, Vigilancia policial.

ABSTRACT: In the last years the use of large-scale databases has increased considerably in private and public sector. It is a powerful tool to predict future situations that may affect society. In our case the use of environmental scanners to fight crime is the project for using this technique of large-scale databases to try to guarantee the security of society against the risk of new, developing forms of criminal activities. In particular, the use of Internet by organized crime groups to commit their crimes is increasing and sometimes there is no other effective way to fight it than by exploring the Internet.
On the other hand, the use of large-scale databases involves utilizes a great amount of data to try to predict where and how organized crime or new forms of criminality will develop. Moreover, when these data are freely accessed to any other person voluntarily by the person concerned because of the use of algorithms, which are so powerful, the complete personality of an individual is revealed.
This means that we have to evaluate the interests of security of society and the privacy of the person, and we have to find the way to balance both in a democratic society.

KEYWORDS: Security, Privacy, DDoS, Massive data, Police surveillance.

Fecha de publicación: 14 diciembre 2016

SUMARIO: I. INTRODUCCIÓN. II. EJEMPLOS DE CIBERSEGURIDAD Y DELINCUENCIA INFORMÁTICA: 1. Actores. 2. Necesidad de víctimas. III. SISTEMÁTICA DEL ANÁLISIS DE DATOS PARA SEGURIDAD NACIONAL. IV. NORMATIVA EUROPEA PARA LA REGULACIÓN DE LA UTILIZACIÓN DEL BIG DATA EN INVESTIGACIONES POLICIALES: 1. Definición de datos. 2. Procesamiento de datos. 3. Transmisión de bases de datos. 4. Derechos de los interesados. 5. Seguridad de tratamiento/procesamiento. 6. Evaluación de riesgos a la Intimidad. Privacy Impact Assessment. 7. Sanciones. V. CUESTIONES ÉTICAS. VI. CONCLUSIÓN. BIBLIOGRAFÍA.

I. **INTRODUCCIÓN**

La gran revolución producida en los últimos años en minería de datos unida al abaratamiento de los sistemas de almacenaje de los mismos ha supuesto que en los últimos años la minería de datos sea una pieza clave en el desarrollo de la sociedad en el S. XXI. Si a esto añadimos que en la actualidad se crean datos de forma exponencial a como se hacía en el pasado y el sistema se alimenta por los ciudadanos mediante la web 2.0 o la utilización de dispositivos móviles nos encontramos con que el número de datos crece exponencialmente. e espera que la producción de datos para 2020 será de 40 zettabits (un zettabit es 10^{21}) lo que supone un incremento de 300 veces desde 2005[1] lo que convierte al análisis de datos en una fuente vital para el desarrollo de la sociedad en un futuro ya que nos va a permitir mejorar la utilización de recursos, mejorar el sistema de salud, sacar el máximo beneficio en la circulación de vehículos, etc. Estas nuevas técnicas en minería de datos, además del análisis, son de vital importancia en la detección de futuras amenazas criminales sobre todo en la delincuencia que se produce exclusivamente en Internet y, por ello, los cuerpos y fuerzas de seguridad del Estado necesita de estas herramientas para prevenir e investigar delitos. Ataques cibernéticos a instalaciones estratégicas de un Estado como puedan ser centrales eléctricas, suministro de agua, centrales nucleares, etc., información sobre reclutamiento de terroristas o de su formación, o toda la delincuencia que circula por la *Deep web*.

No existe una definición de *Big Data* propiamente dicha. Se empezó a utilizar en astronomía y genética en la década del 2000 y se ha ido extendiendo su uso al resto de la sociedad. Básicamente se refiere a las nuevas técnicas de procesamiento que han tenido que utilizar los ingenieros para poder usar unas cantidades de datos tan grandes que un solo ordenador no era capaz de hacer por sí sólo[2]. Para tener una idea de qué cantidad de datos estamos hablando sólo hay que pensar que compañías

[1] IBM http://www.ibmbigdatahub.com/sites/default/files/infographic_file/4-Vs-of-big-data.jpg?cm_mc_uid=17285312897914615394571&cm_mc_sid_50200000=1461832086 (visitado 29/09/2016)

[2] MAYER-SCHÖNBERG, V.; CUKIER, K., *Big Data. A revolution that will transform how we live*, John Murray, London, 2013, p. 6.

como Google o Facebook generan al día más datos que toda la información recogida en la biblioteca de Congreso de Estados Unidos[3]. Podríamos considerar el *Big Data* como ver y entender la relación entre piezas de información que por sí solas no nos dicen nada[4]. Esta modalidad de análisis de datos nos permite descubrir información relevante de datos que, en principio, no tienen conexión entre ellos. Estas técnicas de procesamiento se están utilizando en medicina, para regular el tráfico en las ciudades, para invertir en bolsa, para diseñar campañas publicitarias, etc. Y también está siendo utilizada por países y grupos de delincuentes para derrocar a países. Es por ello que su uso es una pieza clave de la defensa de un Estado en el S. XXI. Por poner un ejemplo de los riesgos y problemas a los que nos encontramos el viernes 21 de octubre de 2016, EE.UU. sufrió el mayor ciberataque de denegación de servicio de su historia[5].

De manera similar a la que la energía nuclear se utiliza para defender un país (y también para amenazarlo) este avance tecnológico implica unas ventajas y unos riesgos para la sociedad. Los datos que se utilizan son aportados por los usuarios tecnológicos, y muchos de ellos pueden ser considerados como datos personales[6], normalmente están abiertos al público por voluntad de sus usuarios y pueden ser procesados con diferentes fines, esto implica una seria amenaza para el derecho fundamental de la intimidad de las personas. Al igual que la energía nuclear implica una amenaza para la salud de los individuos y para el medio ambiente. Siguiendo con la analogía, de la misma forma que hemos controlado el uso civil y militar de la energía nuclear, con las técnicas de *Big Data* se tiene que limitar su uso. La discusión no está ya en si se debe utilizar o no (es claro que ninguna sociedad avanzada va a renunciar a su uso) sino como se va a regularizar su utilización.

La ciberseguridad ha ido tomando mayor importancia en la política de seguridad nacional, dado los riesgos que representa y los avances tan rápidos que se han desarrollado en el ámbito tecnológico. Esta evolución sigue y sigue hasta puntos inimaginables presentando nuevos retos, de los que la seguridad no se encuentra aparte[7].

El debate está abierto todavía.

[3] GENULIUS, S., *The data explosión in 2014 minute by minute*, http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/ (visitado 17/09/2015)

[4] MAYER-SCHÖNBERG, V.; CUKIER, K., *Big Data…*, cit., p. 19.

[5] Thielman, S., Johnson, C., "Mayor cyber attack disrupts internet service across Europe and USA" https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service (visitado 08/11/2016)

[6] La definición de dato personal es complicada pero si se toma la definición de la Directiva 46/95.

[7] CLOUGH, J., *Principles of cybercrime*, Cambridge University Press, Cambridge, 2012, p. 4 y ss.

II. EJEMPLOS DE CIBERSEGURIDAD Y DELINCUENCIA INFORMÁTICA

En 2015 el gobierno americano sufrió un ataque informático en que se tuvo acceso a los datos de millones de sus empleados. Por algunas personas, incluido el secretario de defensa, se ha considerado como un nuevo Pearl Harbor, en la medida en que se ha permitido a los adversarios lanzar ataques a infraestructuras críticas del Estado como son las redes de comunicaciones o sistemas militares críticos[8].

El 7 de abril del 2015 la cadena de televisión francesa TV5Monde, con un conjunto de 11 canales, fue atacada por ciberterroristas[9] controlando la emisión de la cadena y de sus redes sociales[10].

Regularmente Corea del Norte interfiere las comunicaciones del sistema de GPS en Corea del Sur que afectan al sistema de navegación aéreo[11] y marítimo. El sistema de GPS no sólo es utilizado en materia de geolocalización sino que es empleado, por ejemplo, en los mercados financieros para determinar el orden de compras de acciones. No sólo las infraestructuras finales encuentran las vulnerabilidades para posibles ataques sino que también, los intangibles en el proceso de funcionamiento se ven afectados.

Estos ataques son sólo algunos ejemplos de los problemas de seguridad que existen en la red y que afectan a infraestructuras críticas para el normal desarrollo de los Estados democráticos. A diferencia de los ataques físicos, los ataques informáticos no se perciben como una amenaza hasta que surgen. Muchos de estos ataques están relacionados con labores de espionaje más que con un daño inmediato a las infraestructuras pero, para los fines de estudio de este trabajo, es cierto que el *modus operandi* es el mismo.

Los ataques por parte de terroristas o grupos organizados de criminales tienen básicamente dos formas de realizar la acción: 1) controlando los ordenadores de una red o 2) bloqueando el sistema. Estas dos modalidades son utilizadas, para el objetivo de nuestra investigación, en tres modalidades de amenazas, ataques de denegación de servicio (DDoS), instalación de programas de espionaje y ataques online a infraestructuras críticas.

Estas tres formas de ataques tienen puntos en común. Simplificando mucho, las tres necesitan de la introducción de un programa (malware) en un ordenador que puede ser el destinatario final del ataque o puede ser un intermediario desde donde se inicia el ataque controlado por el llamado *botmaster*. No hay que olvidar que

[8] FARREL, H., *The hack on the U.S. government was not a "cyber Pearl Harbor" (but it was a very big deal)*, 2015. http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/06/15/the-hack-on-the-u-s-government-was-not-a-cyber-pearl-harbor-but-it-was-a-very-big-deal/ (visto 18/09/2915)

[9] Se cree que están relacionados con el terrorismo islámico.

[10] MEILHAN, P/ BOTHELO, G., *French TV network hit by 'powerful cyberattack'*, 2015. http://edition.cnn.com/2015/04/08/europe/french-tv-network-cyberattack/ (visto 17/09/2015)

[11] BBC, 2012, http://www.bbc.com/news/world-asia-17922021 (visto 24/09/2015)

ordenador hay que entenderlo en un sentido amplio. El último ataque a gran escala producido este año, al que ya nos hemos referido, se produjo mediante el denominado *Internet of things*, que son los ordenadores que rigen los aparatos con los que interactuamos, electrodomésticos, equipos domóticos, etc.

Aunque describir en detalle el *modus operandi* es una labor complicada por las diferencias que se producen dependiendo de las regiones, grupos involucrados y la tecnología que se utiliza, los cambios que se producen tan rápidamente, es posible identificar algunos puntos comunes entre todos ellos.

Como hemos señalado esta clase de ciber ataques tienen el control de ordenadores para producir el daño. La utilización de un *botnet* es básica en la activación del ataque. Por "*bootnets"* (concepto que se deriva de las palabras robot y network) debemos entender un ordenador controlado de forma remota y conectado a una red que ha sido infectado por un programa malicioso que puede activar los sistemas infectados en los denominados "bots", "robots" o "zombis".

En muchas ocasiones los legítimos usuarios de estos sistemas pueden no estar al tanto de la infección. Los zombis con el botnet instalados conectan con ordenadores controlados por los autores (conocidos como "command and control servers" o C&Cs) o a otros zombis con el fin de recibir las instrucciones, descargar programas adicionales y transmitir información en segundo plano de los sistemas infectados[12].

En el momento en que el ordenador está infectado por el botnet los hackers pueden controlarlo. El sistema clásico era mediante el uso del sistema de mensajería IRC pero recientemente se han detectado estructuras más complicadas, p.e. mediante los protocolos TCP, UDP y ICMP[13]. La primera generación de botnets estaba basada en servidores de control y mando (C&C) pero era relativamente sencillo evitar el ataque mediante la desconexión del C&C. La segunda generación utilizaba conexiones peer-to-peer, para evitar sistema de defensa, basados en redes descentralizadas. La tercera generación se caracteriza por una motivación económica y un diseño más sofisticado[14]

El software malicioso se distribuye de diferentes formas. Una clásica es mediante una web de donde la víctima se baja un archivo y, sin su conocimiento, se instala un archivo que pequeño tamaño[15]. Este archivo de pequeño tamaño, normalmente no mayor de cientos de KBs envía y recoge información del ordenador infectado (nuestro querido zombi). Este puede estar latente por largo tiempo hasta que el botmaster manda la orden de activación.

Esta situación se llega a producir por diferentes factores. Uno de ellos es que los

[12] UNODC, Comprehensive Study on Cybercrime, 2013, p. 32 y ss.

[13] INFOSEC Institute (2013) http://resources.infosecinstitute.com/botnets-and-cybercrime-introduction/ (visto 18/07/2015)

[14] SOOD A. K., ENBODY R. J. & BANSAL R., "Dissecting SpyEye. Understanding the design of third generation botners", *Computer network*, vol. 57, 2013, p. 440 y ss.

[15] Idem.

usuarios domésticos y pequeñas empresas no tienen presupuesto para instalar un sistema de protección lo suficientemente bueno para proteger sus ordenadores. Más aun, tampoco tienen ni el tiempo ni los conocimientos informáticos para tener sus ordenadores actualizados[16]. En estos puntos las compañías de seguridad pueden poner todo su esfuerzo pero existe otro punto, no técnico sino cultural que abre la brecha de seguridad, la lengua materna. La falta de conocimientos en China implica que la población no está capacitada para utilizar soluciones de seguridad tecnológicas que han sido desarrolladas en inglés. Como resultado de esto nos encontramos con que el 80% de los ordenadores conectados a Internet en este país están controlados por botnets[17]. Esto no significa ni mucho menos que la víctima tenga que encontrarse en el mismo país.

1. **Actores**

El prototipo de esta amenaza ha cambiado en la última década. La imagen idílica de un joven hacker detrás de un ataque que pone en peligro la seguridad de un estado no es hoy día la más acertada. Hoy día la escena de las ciberamenazas está más relacionada con el crimen organizado y unidades militares de ciberataques que con la idea romántica de David contra Goliat. Cerca del 80% de los ataques digitales son producidos por alguna forma de crimen organizado[18].

Para realizar ataque cibernéticos es necesario tener conocimientos informáticos, esto implica sociedad con un buen desarrollo en matemáticas, física y computación. El nivel educativo es bueno y tienen una tradición en el desarrollo de la matemática[19]. El desarrollo económico ha dejado de un factor clave para poder ser una amenaza que pongan en peligro a las infraestructuras críticas de un Estado.

Un punto a resaltar es, siguiendo a Kshetri, que no siempre se persigue un fin lucrativo sino que se persigue un motivo más idealista. En el caso de China muchos de los actores de estos ataques consideran sus acciones como un acto nacionalista contra los ataques desde Taiwan y USA con el fin de proteger el honor de la patria[20]. Algo parecido ocurre en los países poscomunistas. En estos caso los activistas consideran sus acciones más como una acción justa para dar algo a la sociedad y su idea es la de usar sus conocimientos para mejorar la sociedad. Los ciudadanos de estos países tiene un gran tradición en matemáticas, física y computación y las usas

[16] ERIKSEN-JENSEN, M., "Holding back the tidal wave of cybercrime," *Computer Fraud & Security*, vol. 03, 2013, p. 14–16.

[17] KSHETRI, N., "Cybercrime and cyber-security issues associated with China: some economic and institutional considerations", *Electronic Commerce Research*, vol. 13, 2013, p. 56 y ss.

[18] BAE SYSTEMS Detica, 2012, http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf (visitado 23/06/2015)

[19] KSHETRI, N., "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers", *Crime, Law and Social Change*, vol. 60, 2013, p. 60 y ss.

[20] KSHETRI, N., "Cybercrime and…", cit., p. 58

desde un punto de vista de honor para devolver a la sociedad los conocimientos que les han dado[21].

2. **Necesidad de víctimas**

El objetivo principal de los ciberataques son las infraestructuras esenciales para el Estado pero este en muchas ocasiones no se puede realizar sin la colaboración de víctimas intermedias que sirven como ejército para el ciberataque. Como este tipo de ataques se puede realizar desde cualquier parte hay que resaltar que cualquier tipo de fallo de seguridad puede tener serias consecuencias. Un típico error es no tomar las medidas necesarias para conseguir una seguridad real. Eriksen-Jensen comenta que los usuarios privados y pequeñas empresas no tienen tiempo ni dinero para mantener actualizados sus sistemas informáticos y consideran que sólo con tener actualizados los programas más importantes es suficiente[22]. Sin duda, en la realidad nos encontramos que una grieta en la seguridad permite a los hackers realizar un ataque.

Las víctimas finales de estos ciberataques son, por lo general, Estados y grandes empresas. Uno de los casos que hemos presentado de ataque a EE.UU. por parte, presumiblemente, de China se puede considerar como un ataque, entre otras cosas, porque, aunque es realizado por ciudadanos y no por militares, tienen el beneplácito de las autoridades ya sea con su consentimiento ya sea con su ayuda.

Ante este tipo de ataques no nos queda más que vigilar el medio en que se producen para poder evitarlos y esto implica la posibilidad de utilizar técnicas de "big data" para saber cuándo se va a producir, cómo se van a perpetrar, quién los va a realizar y qué objetivos se persiguen.

III. **SISTEMÁTICA DEL ANÁLISIS DE DATOS PARA SEGURIDAD NACIONAL**

La investigación en Internet no es algo nuevo. Sin embargo, como hemos señalado anteriormente, las nuevas técnicas de procesamiento y análisis de datos sí hacen que la revolución realizada en los servicios de inteligencia sea cuando menos fascinante. Y al mismo tiempo peligrosas. El espionaje masivo, tal y como se ha podido demostrar en el caso Snowden, permite tener controlada a cantidades ingentes de población y la reacción de la ciudadanía no se ha hecho esperar. Sin embargo, son unas herramientas vitales a las que ningún Estado va a renunciar ya que el riesgo por su no utilización es muy grande. La clave ahora mismo es cómo poder utilizarlo.

Desde el punto de vista militar la minería de datos se puede utilizar de dos for-

[21] KSHETRI, N., "Cybercrime in…", cit., p. 57 y ss.
[22] ERIKSEN-JENSEN, M., "Holding…", cit., p. 14.

mas estratégico y operacional. Básicamente, podríamos considerar el primero como unidireccional y el segundo bidireccional. En el primero una vez captados los datos podemos olvidar su origen, desde el punto de vista de protección de los mismos, mientras que en el segundo, tendríamos que mantener una trazabilidad de los mismos para conseguir pruebas de donde vienen los orígenes de las amenazas. Esto es un resumen de como es el procedimiento del tratamiento de datos que necesitaría una explicación más detallada pero para el objetivo de este trabajo nos sirve.

El sistema funciona en tres fases: adquisición de datos, procesamiento de los mismos y análisis. En la primera fase ya nos encontramos con problemas ético jurídicos para la realización de la misma. La pregunta es si se deben acceder a los datos cerrados (protegidos por algún tipo de seguridad) o sólo se deben acceder a los datos abiertos (open data). Aquí ya tenemos una gran diferencia de si se trata de una operación estratégica u operacional. En la primera no nos hará falta introducirnos en las fuentes cerradas ya que la generación de datos públicos hoy día nos da los datos suficientes para poder detectar los indicios de amenaza. En el segundo caso es cierto que nos podemos encontrar con mayores problemas. Por ejemplo, si consideramos que un Estado está realizando un ataque o ha realizado un ataque puede ser interesante el poder retrotraer la información obtenida al origen de la fuente para saber exactamente qué Estado es el que nos ataca. En estos casos la protección de la intimidad de las personas se haya en situación de alto riesgo y deberá de realizarse mediante la supervisión de una autoridad independiente que permita evitar los abusos en su utilización.

En la segunda fase nos encontramos con la necesidad de asegurar los datos mediante la toma de medidas de seguridad. Una doble muralla de seguridad con control restringido a un número pequeño de personas, así, como que el acceso quede registrado y que se active un aviso automático a los encargados de velar por el núcleo serían medidas imprescindibles. El procesamiento de datos se realizará internamente por un robot, lo que garantiza que la intimidad no se vea afectada, teniendo las personas encargadas acceso con el fin de poder solucionar errores que se detecten. El robot se puede programar de tal manera que el análisis de los datos vaya en una dirección, se extraigan las conclusiones sin poder volver a dar marcha atrás. Además se debe preparar un sistema de pseudoanonimización y trazabilidad de los datos. En los casos de tratarse de operaciones operacionales es preciso que se instale un sistema de trazabilidad fiable para poder mantener el acceso a los datos primogénitos.

En la tercera fase es preciso que un analista tome la decisión de si la alerta detectada es fiable o no. El procesamiento de datos automático es una gran ayuda pero, finalmente, la persona es la que debe tener la decisión de considerar la información obtenida y procesada como relevante o no.

En estas tres fases existen riesgos importantes para los Derecho fundamentales

de los ciudadanos, lo cual, como hemos podido comprobar con escándalos de investigaciones anteriores, implica un grave riesgo para el Estado de Derecho y para la confianza de los ciudadanos en sus sistema de defensa.

Con el tratamiento apropiado de los datos es factible, en un uso estratégico, el poder predecir cómo van a evolucionar las amenazas. Las agencias europeas de policía ya se encuentran desarrollando este tipo de herramientas como el proyecto del ePOOLICE. Este consiste en un escáner de detección de criminalidad organizada mediante el análisis de datos de tal manera que se puede predecir cuándo una amenaza va a dar el salto a la criminalidad organizada. Programas de calado parecido, desde el punto de vista operativo, son VIRTUOSO o CAPER. En estos casos no se trata de predecir sino de utilizarlo para resolver amenazas concretas y el procesamiento de datos, al ser bidireccional, es diferente.

Aunque los riesgos pueden parecer muy grandes para los ciudadanos el uso de esta tecnología no puede limitarse. El análisis masivo de datos ha llegado para quedarse y no puede ser una herramienta que se deje sólo en manos de los delincuentes. De la misma forma que admitimos el uso de armas de fuego por parte de los cuerpos y fuerzas de seguridad para combatir el uso por parte de los delincuentes o la utilización de otros avances industriales y tecnológicos, como pueden ser los vehículos a motor, con las técnicas de análisis de datos ocurre lo mismo. La cuestión no es si se pueden utilizar o no sino el cómo se van a utilizar. Cuál va a ser el correcto uso de las mismas para mantener el Estado de Derecho y la protección de los Derechos de los ciudadanos dentro de una democracia en el siglo XXI.

Para resolver esta cuestión vamos a analizar la normativa europea relativa a la utilización de bases de datos así como los principios éticos que deben regir su utilización.

IV. NORMATIVA EUROPEA PARA LA REGULACIÓN DE LA UTILIZACIÓN DEL BIG DATA EN INVESTIGACIONES POLICIALES

Como hemos señalado anteriormente una gran fuente de los datos proviene de la utilización de dispositivos móviles conectados a la red. Y los datos circulan por ella sin limitaciones ya que es un espacio, en principio, sin fronteras. Es por ello que desde una normativa exclusivamente nacional va a ser muy difícil dar una buena regulación al respecto. Además, en la Unión Europea se produce la necesidad de mover bases de datos en territorio comunitario para determinados servicios y negocios y, por ello, es necesario una armonización de la legislación para facilitar los mismos.

Al mismo tiempo el Convenio Europeo de Derecho Humanos recoge, en su artículo 8, el Derecho al respeto a la vida privada y familiar, de su domicilio y de su correspondencia, con la limitación de que el Estado, siempre que esté regulado por

la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional[23], la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derecho y las libertades de los demás. En este conflicto entre dos bienes necesarios en una democracia, intimidad y seguridad, el TEDH ha considerado que el artículo 8 (sobre la intimidad) es un derecho que tiene que estar equilibrado con seguridad pública, seguridad nacional y prevención de los desórdenes públicos o del crimen, siguiendo la redacción del artículo 8.2 del Convenio Europeo de Derecho Humanos. En este tercer punto el Tribunal considera que existen tres áreas donde está justificada la intrusión en la intimidad a) investigaciones policiales[24], b) control y vigilancia de reclusos[25] y c) y el control de extranjeros con antecedentes penales que quieren residir en un país diferente al suyo[26]. Así, se ha entendido por estado de emergencia cuando la vida de la nación se encuentra amenazada por una emergencia pública o por seguridad nacional. Así, puede ser invocado cuando se ve amenazada por un sistema altamente sofisticado de espionaje o por casos de terrorismo[27]. No existe una manga ancha a la hora de permitir que el Estado invada la vida privada de las personas, pero el margen de discrecionalidad que le da expresiones tan vagas como las que se utilizan siempre va a depender de la interpretación que se haga en los términos y circunstancias del caso supuesto, aunque el TEDH suele ser flexible[28].

Dentro de este contexto de utilización de datos y la protección del derecho a la intimidad, surge la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Este texto legal constituye la piedra angular sobre la que gravita la protección de datos en el espacio europeo[29]. Aunque el ámbito de actuación de esta norma no es la seguridad y actividades Estatales en áreas de seguridad (artículo 3.2), es la primera norma que determina los conceptos que nos van a servir en nuestra investi-

[23] VAN DER SLOOT, B., "How to asses privacy violations in the age of Big Data? Analysing the three different test developed by the ECtHR and adding for a fourth one", *Information & Communications Technology Law*, 2015. P. 6 http://dx.doi.org/10.1080/13600834.2015.1009714 (visitado 06/10/2016)

[24] Sentencias del TEDH *Keegan vs United Kingdon* de 18 de julio de 2006 y *Mancevskchi vs Modova* de 7 de octubre de 2007.

[25] Sentencias del TEDH *Nazarenko vs Ukraine* de 29 de abril de 2003 y *Lich vs Ukraine* de 29 de abril de 2003.

[26] Sentencias del TEDH *Boultif vs Switerlland* de 2 de agosto de 2001 y *Uner vs Netherlands* de 18 de octubre de 2006.

[27] Sentencias el TEDH *Leander vs Sweden* de 26 de marzo de 1987 y *Klass and others vs Germany* de 6 de septiembre de 1978.

[28] Van der Sloot, B., "How…", cit., p. 16.

[29] Esta protección se basa en Convención para la protección de personas en relación al proceso automático de datos personales, firmada el 28 de enero de 1981. Cfr. Cammillleri-Subrenat, A., Levallois-Barth, C., *Sensitive Data Protection in the European Union*, 2007, Bruylant, p. 15.

gación y que influyen en el uso de datos personales ya sea para fines comerciales o para cuestiones de seguridad.

Tiene como finalidad proteger los derechos fundamentales y las libertades de las personas físicas, y en particular su derecho a la intimidad con el respeto al procesamiento de datos (artículo 1) dentro de una Unión Europea que permite la libre circulación de datos.

Más tarde se creó la Decisión Marco 2008/977/JAI que limita su ámbito de aplicación a la cooperación judicial y policial en materia penal, recogida en los Tratados, y garantizando un nivel de seguridad pública mínimo (artículo 1). Para combatir la criminalidad en el territorio comunitario se consideró necesario la colaboración de los diferentes cuerpos y fuerzas de seguridad públicas y, entre las diferentes formas de ayuda, se determinó el intercambio de bases de datos con el fin de combatir de determinada delincuencia que actúa transfronterizamente, junto con el terrorismo internacional, estando limitado este intercambio de datos al ámbito de la seguridad[30].

Además del intercambio de datos nos encontramos con que los avances de la tecnología también son utilizados por la policía en su día a día. La investigación en Internet no es algo nuevo. Sin embargo, como hemos señalado anteriormente, las nuevas técnicas de procesamiento y análisis de datos sí hacen que la revolución realizada en los servicios de inteligencia sea cuando menos fascinante. Y al mismo tiempo peligrosas.

El espionaje masivo, tal y como se ha podido demostrar en el caso Snowden[31], la actuación del Government Communications Headquartes (GCHQ)[32] o recientemente los descubrimientos del Bundes Nachrichten Dienst (BND)[33], permite tener controlada a cantidades ingentes de población y la reacción de la ciudadanía no se ha hecho esperar. Sin embargo, son unas herramientas vitales a las que ningún Estado va a renunciar ya que el riesgo por su no utilización es muy grande. La clave ahora mismo es cómo poder utilizarlo y controlar su uso.

Desde el punto de vista de la seguridad, la minería de datos se puede utilizar de dos formas: estratégico y operacional. Básicamente, podríamos considerar el primero como unidireccional y el segundo bidireccional. En el primero una vez captados los datos podemos olvidar su origen, desde el punto de vista de protección de los mismos, mientras que en el segundo, tendríamos que mantener una trazabilidad de

[30] OERMANN, M., *Individualdatenschutz in europäischen Datenschutzrecht*, 2012, Centaurus, p. 81.

[31] GREENWALD, G., MACASKILL, E., POITRAS, L., "Edward Snowden: the whistleblower behind the NSA surveillance revelations", The Guardian, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (visitado 3/07/2013)

[32] WEAVER, M., "Security services spied on 20 high-profile people in questionable operations", https://www.theguardian.com/world/2016/jul/27/mi5-and-gchq-spied-on-20-high-profile-people-in-questionable-operations (visitado 29/07/2016)

[33] Süddeutsche Zeitung, "Datenschutzbeauftragte wirft BND systematische Gesetzesverstöße vor", http://www.sueddeutsche.de/politik/ueberwachung-datenschutzbeauftragte-wirft-bnd-systematische-gesetzesverstoesse-vor-1.3145616 (visitado 03/10/2016)

los mismos para conseguir pruebas de donde vienen los orígenes de las amenazas. Esto es un resumen de como es el procedimiento del tratamiento de datos que necesitaría una explicación más detallada pero para el objetivo de este trabajo nos sirve.

El sistema funciona en tres fases: adquisición de datos, procesamiento de los mismos y análisis. En la primera fase ya nos encontramos con problemas ético jurídicos para la realización de la misma. La pregunta es si se deben acceder a los datos cerrados (protegidos por algún tipo de seguridad) o sólo se deben acceder a los datos abiertos (open data). Aquí ya tenemos una gran diferencia de si se trata de una operación estratégica u operacional. En la primera no nos hará falta introducirnos en las fuentes cerradas ya que la generación de datos públicos hoy día nos da los datos suficientes para poder detectar los indicios de amenaza. En el segundo caso es cierto que nos podemos encontrar con mayores problemas. Por ejemplo, si consideramos que un Estado está realizando un ataque o ha realizado un ataque puede ser interesante el poder retrotraer la información obtenida al origen de la fuente para saber exactamente qué Estado es el que nos ataca. En estos casos la protección de la intimidad de las personas se haya en situación de alto riesgo y deberá de realizarse mediante la supervisión de una autoridad independiente que permita evitar los abusos en su utilización.

En la segunda fase nos encontramos con la necesidad de asegurar los datos mediante la toma de medidas de seguridad. Una doble muralla de seguridad con control restringido a un número pequeño de personas, así, como que el acceso quede registrado y que se active un aviso automático a los encargados de velar por el núcleo serían medidas imprescindibles. El procesamiento de datos se realizará internamente por un robot, lo que garantiza que la intimidad no se vea afectada, teniendo las personas encargadas acceso con el fin de poder solucionar errores que se detecten. El robot se puede programar de tal manera que el análisis de los datos vaya en una dirección, se extraigan las conclusiones sin poder volver a dar marcha atrás. Además se debe preparar un sistema de pseudoanonimización y trazabilidad de los datos. En los casos de tratarse de operaciones operacionales es preciso que se instale un sistema de trazabilidad fiable para poder mantener el acceso a los datos primogénitos.

En la tercera fase es preciso que un analista tome la decisión de si la alerta detectada es fiable o no. El procesamiento de datos automático es una gran ayuda pero, finalmente, la persona es la que debe tener la decisión de considerar la información obtenida y procesada como relevante o no.

En estas tres fases existen riesgos importantes para los Derecho fundamentales de los ciudadanos, lo cual, como hemos podido comprobar con escándalos de investigaciones anteriores, implica un grave riesgo para el Estado de Derecho y para la confianza de los ciudadanos en sus sistema de defensa.

Aunque los riesgos pueden parecer muy grandes para los ciudadanos no se puede evitar el uso de esta tecnología. El análisis masivo de datos es hoy día una herramienta imprescindible en las investigaciones policiales y no puede ser que su uso se deje sólo en manos de los delincuentes. De la misma forma que admitimos el uso de armas de fuego por parte de los cuerpos y fuerzas de seguridad para combatir el uso de las mismas por parte de los delincuentes o la utilización de otros avances industriales y tecnológicos, como pueden ser los vehículos a motor, debemos usar las técnicas de análisis de datos. La cuestión no es si se pueden utilizar o no sino cómo se van a utilizar, cuál va a ser el correcto uso del procesamiento masivo de datos para mantener el Estado de Derecho y la protección de los Derechos de los ciudadanos dentro de una democracia en el siglo XXI.

Tal y como se encentra conceptualizado el Big Data nos encontramos con que no existe una normativa *ad hoc* a los riesgos que plantea así que, como son bases de datos, se les va a poder aplicar es la normativa europea que hemos comentado. En nuestro caso nos vamos a centrar únicamente en la normativa relativa a las bases de datos policiales ya que nuestro objeto de estudio consiste en la utilización por parte de los cuerpos y fuerzas de seguridad de las técnicas predictivas del Big Data. Aun así, hay determinados problemas que no vienen resueltos por la Decisión Marco 2008/977/JAI y tendremos que recurrir a Directiva 95/46/CE para encontrar soluciones a los problemas que se nos van a plantear.

1. **Definición de datos**

Los conceptos básicos referidos a los datos vienen regulados en el artículo 2 de la Decisión Marco 2008/977/JHA[34], y son las mismas definiciones que en la Directiva 95/46/CE.

Siguiendo la normativa europea se entenderá por datos personales toda información sobre una persona física identificada o identificable («el interesado»). Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos que suministren alguna característica de su identidad física, fisiológica, psíquica, económica, cultural o social.

Además, dentro de los datos personales la normativa destaca a un grupo concreto que los denomina datos especialmente sensibles. Estos son categorías especiales de datos, que pueden revelar el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, de datos relativos a la salud o a la vida sexual[35], los cuales, solo se permitirá su utilización, por parte de

[34] Antes de esta normativa el intercambio de datos entre agencias e instituciones se realizaba, casi de forma alegal. Cfr. CAMMILLLERI-SUBRENAT, A., LEVALLOIS-BARTH, C., *Sensitive…*, cit., pp. 46 y ss.

[35] Esto es un listado mínimo que todos los Estados tienen que cumplir. En la legislación inglesa sobre

los cuerpos y fuerzas de seguridad, cuando sea estrictamente necesario y si el Derecho nacional establece garantías adecuadas (artículo 6). El TEDH no considera que el término necesidad se equivalente a indispensable, ni de equivalentes como admisible, razonable o deseable: tiene que ser "una necesidad social urgente"[36]. En este caso el uso de estos datos está menos limitado que cuando se trata de su uso para fines diferentes al de la seguridad y combate del crimen (artículo 8 de la Directiva 95/46/CE)[37]. Los dos requisitos que se exigen para esta utilización son: a) el procesamiento tiene que estar recogido en la ley y tiene que ser completamente necesario y b) los Estados Miembros deben proporcionar salvaguardas específicas y adecuadas como, por ejemplo, que se limite el acceso a los datos sólo a aquellas personas responsables legalmente de la terea por la que se solicitan[38].

Además, el TJCE ha considerado como datos personales las nóminas pagadas por una compañía[39], nombre y dirección[40] o la dirección IP de un ordenador[41]. En el caso *Rijkeboer* el Tribunal hace una distinción entre datos básicos y otro tipo de datos, los cuales tienen información o es receptor de información del sujeto que pueden revelar información sobre los datos básicos y aquellos en relación con el procesamiento de los datos básicos. Sólo los primeros pueden ser considerados como datos personales[42]. En la sentencia del caso *Huber* datos, como puedan ser nombre, nombre de soltera, fecha y lugar de nacimiento, nacionalidad, estado civil, sexo, registros de entrada y salida del país, situación de residencia, datos de pasaporte, registros bancarios así como domicilio y números identificativos de la administración son considerados como datos personales[43]. Luego la definición es más amplia que la puramente legal, llegando a ser grandísima cuando estamos tratando de supuestos como los señalados en el capítulo I de este trabajo, ya que, con las técnicas de Big Data, cualquier dato puede ser considerado como básico para identificar a la persona en el momento en el que se pone en correlación con otras bases de datos. No está de más señalar, después de los ejemplos tratados en la primera parte del trabajo que los metadata pueden ser considerados datos personales.

protección de datos se consideran datos sensibles, además, el salario de un empleado, los billetes de avión, las reservas de hoteles, los registros de bajas temporales de los empleados, los registros de los servicios sociales, información implicando a alguien en relación a un delitos de blanqueo de capitales (sic.) y la grabación por vídeo vigilancia de un empleado robando dinero del puesto de trabajo. Cfr. CAREY, P., TREACY, B., *Data Protection. A Practical Guide to UK and EU Law*, Oxford University Press, 2015, p. 103.

[36] VAN DER SLOOT, B., "How…", cit., p. 14. Sentencia del TUDH *Sunday Times vs United Kingdom* de 26 de abril de 1979.

[37] Qué es la misma definición que se utiliza en el sistema de información de Schengen.

[38] CAMMILLLERI-SUBRENAT, A., LEVALLOIS-BARTH, C., *Sensitive*…, cit., pp.50-51.

[39] Sentencias del TJCE unificadas C-465/00, C-138/01, C-139/01, *Österrreichischer Rundfunk and others*

[40] Sentencia del TJCE C-553/07, *Rijkeboer*

[41] Sentencia del TJCE C-461/10, *Bonnier and others*

[42] Sentencia del TJCE C-553/07, *Rijkeboer*

[43] Sentencia del TJCE C-524/06, *Huber*

Por tratamiento de datos se entiende cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Seguidamente se definen dos conceptos directamente relacionados con los Derechos subjetivos que tiene el ciudadano para proteger su intimidad. El concepto de bloqueo, el cual se ha de entender como la señalización de datos personales conservados con el objetivo de limitar su tratamiento en el futuro. Más adelante se refiere a un segundo concepto (apartado j) que es el de marcado, por el que los datos son conservados sin el objetivo de limitar su tratamiento futuro.

Y para finalizar, como últimas definiciones en conexión directa con los datos, se regula el concepto de fichero de datos personales o Fichero como todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica; y el concepto de procesamiento de disociación por el que se modifican los datos personales de tal forma que los detalles de las condiciones personales o materiales no puedan ya atribuirse a una persona física identificada o identificable, o sólo sea posible invirtiendo, tiempo, costes y trabajo desproporcionados.

Como podemos observar la definición de datos se ha quedado un poco obsoleta con el avance de la tecnología[44]. Es por ello que a partir de 2018 entra en vigor otra normativa comunitaria que, desde abril de 2016, sustituye a la Decisión Marco, la Directiva 2016/680 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

Esta norma regula el concepto de datos como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[45]. Como vemos, ya se

[44] OUBIÑA BARBOLA, S., "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", Colomer Hernández, I., Oubiña Barbolla, S., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, 2015, p. 72.

[45] Artículo 3 de la Directiva 2016/680.

hace mención expresa a determinados metadatos[46], como puede ser la localización o un identificador en línea, y, además, se han incluido los datos genéticos[47] y biométricos[48]. Estas dos últimas categorías vienen definidas más adelante como "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate", en primer caso, y como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos", el segundo. Además, se consideran datos relativos a la salud aquellos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

2. **Procesamiento de datos**

La Decisión Marco establece unos criterios para el correcto uso de los datos personales, que según su artículo 3, pueden ser recopilados por la autoridad competente con un fin determinado, explícito y legítimo en el marco de las funciones que posea y sólo podrán ser utilizados para el fin con el que se hayan recogido. El tratamiento de los datos deberá ser lícito y adecuado, pertinente y no excesivo con respecto a los fines para los que se recojan. Sigue el artículo 3, en su párrafo 2, con los requisitos que se tienen que cumplir para poder procesar los datos para otro fin. De esta forma se permite su posterior tratamiento si se cumplen tres requisitos: a) que no sea incompatible con los fines para los que se recogieron; b) las autoridades competentes se encuentren autorizadas a tratar los datos para ese nuevo fin y, c) que el tratamiento sea necesario y proporcionado[49]. Además, se podrá utilizar los datos para fines históricos, estadísticos o científicos siempre que estén disociados. Se ha criticado, y con razón, que el cambio de fin puede estar muy alejado de aquél para el que inicialmente fueron transmitidos[50]. Este es justo uno de los problemas

[46] En la STJUE de 8 de abril de 2014, casos C-293/12 *Digital Rights Ireland Ltd* y C-594/12 *Kärntner Landesregierung* se consideró que ya que se respetaba el contenido de las comunicaciones en los registros de telecomunicaciones la Decisión Marco respetaba los derechos fundamentales del artículo 7 de la CDHUE. Cfr. Oubiña Barbola, S., "Cambio…", cit., p. 115.

[47] Los datos genéticos son muy sensibles puesto que pueden tener una imagen total del AND. Cammillleri-Subrenat, A., Levallois-Barth, C., *Sensitive…*, cit., p. 49.

[48] Cfr. KIND, E.J., *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*¸ Springer, 2013, pp. 90 y ss. El autor considera que no está claro que se consideren los datos biométricos como datos personales según la definición de la Directiva 95/46/CE. Con la nueva regulación en el Reglamento 2016/679 y la Directiva 2016/680 se deben considerar como tales.

[49] Al ser regulaciones muy genéricas el Grupo de Trabajo del artículo 29 ha señalado que debe precisarse tanto el propósito, el uso legítimo y el fin por el que se recolectan los datos. Cfr. TREACY, B., BAPAT, A., "Purpose…", cit., p. 2-3.

[50] OUBIÑA BARBOLA, S., "Cambio…", cit., p. 87. Citando a RIJKEN, C., "Re-balancing Security and

que resuelve en gran medida la nueva Directiva 2016/680 con la obligación de tener el PIA.

En principio, esta regulación no impide la reutilización de datos que suele ser necesaria para la predicción mediante Big Data al utilizar varias bases de datos. Sin embargo, es posible una interpretación restrictiva de la norma, ya que no cumpliría en todos los casos con el primero de los requisitos obligatorios. En la nueva redacción de la Directiva se limita la reutilización para los casos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Además, se exigen dos condiciones: a) que el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin y b) que el tratamiento sea necesario y proporcionado para ese otro fin. En ambos casos el procesamiento se tiene que realizar de conformidad con el Derecho de la Unión o del Estado miembro. Con la nueva redacción del artículo 4 de la nueva Directiva se elimina la necesidad de que sea compatible con los fines para los que se recogieron pero, básicamente, está limitación viene de la necesidad de que se trate sólo para cuestiones penales, tal y como aparece regulado en el artículo 1.1. En principio se permite su utilización para otro uso, más aun cuando en la nueva Directiva se regula la necesidad de un PIA y de la protección de los datos por diseño, que veremos más adelante.

Galán Muñoz considera que es así pero entiende que puede ser incompatible con el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea[51]. Sin embargo, no somos de esta opinión. Aunque en la propuesta de Directiva no se regulaba expresamente la obligación de realizar un examen de riesgos y de medidas de seguridad, sí se exponen, en los artículos 19, 23, 24 y 27, las obligaciones del tratamiento de datos que, sin ser la redacción definitiva, ya indicaba por dónde tenía que ir el procesamiento automático de los mismos. Luego, podemos considerar que existen los controles necesarios para estar en consonancia con el Derecho a la intimidad recogido en el artículo 8 de la CDHUE. Más aún cuando se permite la reutilización fuera del ámbito de la Directiva siempre que esté sujeto el procesamiento a la redacción del Reglamento 2016/679, tal y como señala el artículo 9.1 de la Directiva 2016/680.

El procesamiento de los datos en materia penal se deberá realizar tomando una serie de salvaguardas. Regulado en los artículos 4, 5 y 6 de la Decisión Marco 2008/977/JHA se ponen una serie de obligaciones que se deben cumplir entre las

Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal Matters", *Common Market Law Review*, Oct. 2010, pp. 1455-1492.

[51] GALÁN MUÑOZ, A., "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: Hacia una nueva orientación de la política criminal de la Unión Europea", Colomer Hernández, I., Oubiña Barbolla, S., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, 2015, p. 56.

que está la rectificación, supresión y bloqueo; la limitación temporal del almacenamiento de los datos y cómo se van a tratar los datos esenciales.

El artículo 4 obliga a eliminar los datos que sean erróneos y cuando sea posible y necesario, se complementaran o actualizaran. Se exige que la información que se procese sobre los individuos sea real y va a servir para garantizar los derechos de los ciudadanos al asegurar que las decisiones que se tomen mediante el procesamiento de datos en materia criminal se basen en datos verídicos. Este principio en el correcto uso de datos personales va a permitir que el ciudadano pueda exigir borrar determinada información de las bases de datos policiales. Esta obligación se complementa con un principio básico en el tratamiento de datos personales como es la limitación temporal del uso de los datos. Los datos no se pueden utilizar de forma ilimitada.

Además, el derecho al olvido, que tienen los ciudadanos, se regula en sus dos facetas, borrado o bloqueo. El borrado o supresión se realizará en todos los casos en que el fin por el que fueron recabados se ha finalizado. El procesamiento con técnicas de Big Data, el hecho que haya datos erróneos no afecta a la predicción ya que en el tratamiento con el algoritmo consigue "eliminar" los datos erróneos y, además, como uno de sus requisitos es que estos se encuentren actualizados, garantizaría el cumplimiento de este requisito en beneficio de los ciudadanos. En el caso del bloqueo, en lugar de suprimirse la información de las bases de datos lo que se hace es mantener la información, siempre que haya razones justificadas para suponer que la supresión pueda perjudicar los intereses legítimos del interesado, siempre que el tratamiento se limite para los fines que impidieron su borrado.

La limitación de la utilización de los datos viene impuesto por el artículo 5 y se tendrá que hacer a priori, con posibilidad de extender el límite y revisando las predicciones por si hiciera falta su conservación, asegurando que se eliminarán en un determinado momento.

Por último, se exigirán medidas adicionales cuando se proceses los llamados datos especiales que, como hemos señalado con anterioridad, son los referentes al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, de datos relativos a la salud o a la vida sexual que consistirán en una estricta necesidad y que la regulación nacional establezca unas garantías suficientes. A diferencia de la Directiva 1995/46, donde se establece una prohibición clara de utilizar este tipo de datos, para regular más tarde la excepción a esta regla, en la Decisión Marco 2008/977 no se prohíbe la utilización de esta clase información pero sí se pone la obligación de realizar este procesamiento sólo en los casos de estricta necesidad. Este aspecto diferencial, que ha sido criticado[52] por la doctrina, se debe únicamente a la necesidad real de los cuerpos y fuerzas del Estado de identificar a los ciudadanos por rasgos físicos y a la existencia de este

[52] OUBIÑA BARBOLA, S., "Cambio…", cit., p. 85.

tipo de ficheros con anterioridad a la regulación, por ejemplo, el documento de identificación personal.

Estas medidas para el correcto uso de los datos se completan con la limitación al procesamiento automatizado que, como resultado del mismo, genere decisiones que produzcan efectos jurídicos adversos en el interesado o le afecten de manera significativa al evaluar determinados aspectos de su personalidad, siendo necesario que la normativa nacional lo regule con las garantías necesarias para los intereses legítimos del interesado.

3. **Transmisión de bases de datos**

Antecedentes en el intercambio de información policial hay bastantes. Desde 1970 se han puesto diferentes sistemas para el intercambio de información que ha ido evolucionando [53] hasta tener como núcleo central la Decisión Marco 2008/977/JHA. Esta norma es el centro de la transmisión de bases de datos en materia policial, dentro de la colaboración policial y judicial en el espacio de justicia y seguridad europeo. Es por ello que los siguientes artículos de la regulación se dedican a los controles que se deben tomar en la transmisión de dichos datos a otras autoridades.

De esta forma la autoridad competente se debe asegurar de que la información que se traslada no es errónea, controlando los datos que se van a enviar de antemano, que se añada información para el destinatario de los mismos para que pueda valorar el grado en que son exactos, completos, actualizados y fiables. En el caso en que los datos, que se hayan transmitido, sean erróneos u obtenidos de forma ilegal se deberá comunicar al destinatario dicha situación (Artículo 8).

Paralelamente, la autoridad competente está obligada a transmitir la información sobre los plazos de limitación en la utilización de los datos, para que sean destruidos una vez cumplido el plazo (Artículo 9).

Es obligatorio llevar un registro de la transmisión a efectos de comprobación de la licitud de su tratamiento, de autocontrol y de garantía de su integridad y seguridad que tendrán que estar a disposición de la autoridad de control competente (Artículo 10).

En el artículo 11 se regulan los supuestos en que la autoridad competente de los Estados miembros receptores de la información podrá destinar los datos recibidos a otro fin siempre que sean alguno de los siguientes: a) la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales distintas de aquellas para las que se transmitieron o pusieron a

[53] FIODORAVA, A., "La transmisión de información personal y datos personales en la Unión Europea para fines de investigación de delitos", Colomer Hernández, I., Oubiña Barbolla, S., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, 2015, p 126 y ss.

disposición; b) otros procedimientos judiciales y administrativos directamente relacionados con la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales; c) la prevención de amenazas inmediatas y graves a la seguridad pública o d) cualquier otro fin, solo con el previo consentimiento del Estado miembro transmisor o con el consentimiento del interesado, otorgados de acuerdo con el Derecho nacional. Las limitaciones que tienen de uso los datos se transmitirán a los receptores de la información debiendo tomar las medidas adecuadas para asegurarse su cumplimiento (Artículo 12).

La transferencia a terceros países o a organismos internacionales se permite sólo cuando se cumplan las siguientes condiciones: a) que sea necesario para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales; b) que la autoridad receptora del tercer Estado o el organismos internacional receptor sea competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales; c) que el Estado miembro que proporcionó los datos haya consentido la transferencia de acuerdo con su legislación nacional, con la excepción de ser una situación esencial para la prevención de una amenaza inmediata y grave a la seguridad del Estado miembro[54], tercer Estado o intereses esenciales de un Estado miembro y si el consentimiento no se puede obtener antes; y d) que el receptor garantice un nivel adecuado de protección en el tratamiento de datos previsto, con una primera excepción en que el Estado cedente tenga en su legislación regulado los supuestos de legítimos intereses específicos del interesado o legítimos intereses superiores, en especial los relativos al interés público, y una segunda excepción respecto a la confianza que tenga el Estado miembro sobre las garantías que ofrece el Estado receptor[55].

En los casos en que se trata de una trasmisión a particulares en los Estados Miembros se tendrán que cumplir con las siguientes condiciones: a) que la autoridad competente del Estado miembro del que se obtuvieron los datos haya consentido en que estos se trasmitan de acuerdo con su Derecho nacional; b) que los legítimos intereses específicos del interesado no impidan su trasmisión y c) que en determinados casos sea esencial que la autoridad competente trasmita los datos a particulares para el cumplimiento de funciones que tienen legalmente asignadas, para la prevención, la investigación, la detección, o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, para la prevención de amenazas

[54] Que obviamente se puede considerar delictiva pero que es antes de que se inicie todo la investigación policial o la actuación judicial y que, por la urgencia, no puede esperar al normal desarrollo de la solicitud de la autorización. En contra, GALÁN MUÑOZ, A., "La protección…", cit., p. 56.

[55] Aunque la redacción es bastante restrictiva en el uso, es cierto que posee excepciones múltiples y sobre todo poco claras, dejando el ámbito de aplicación muy abierto. Cfr. OUBIÑA BARBOLA, S., "Cambio…", cit., pp. 82-83.

inmediatas y graves a la seguridad o de los derechos de las personas. Justo en este punto de la transmisión de datos es dónde se ha producido el gran cataclismo en la colaboración con los Estados después del caso Schrems[56].

Maximiliam Schrems es un ciudadano austriaco que solicitó de Facebook Irlanda su derecho al acceso de sus datos en la red social teniendo en cuenta que los datos se trasladaban a EE.UU. después de las revelaciones de Snowden se sabía que se cedían a la NSA, la cual no respetaba las garantía necesarias para salvaguardar sus datos. Es por ello que solicita que Facebook le dé acceso a los datos que posee de él y al mismo tiempo solicita al comisario de protección de datos en Irlanda que ejerza sus funciones y prohíba a Facebook el traslado de los datos a EE.UU. para su procesamiento. Ante esa decisión interpone una demanda en *High Court* y este tribunal afirmo que el Derecho irlandés prohíbe la transmisión de datos a terceros países salvo en los casos en que el país interesado asegura un nivel de protección adecuado y que, aunque es cierto que las revelaciones de Snowden ponen de relieve importantes excesos, la Comisión Europea sigue considerando EE.UU. como un país de fiar. Aun así, el High Court presenta una cuestión prejudicial para saber si a) el comisario está vinculado lo estimado por la Comisión y b) si el comisario puede o debe realizar su propia investigación ante el cambio de paradigma suscitado por las revelaciones de Snowden. En la sentencia del TJUE de 6 de octubre de 2015 se dictaminó que la autoridad nacional tiene competencias para dictaminar si la transferencia a un tercer país cumple con las exigencias necesarias para respetar los derechos de los ciudadanos. Al mismo tiempo determina que los Estados miembros o la Comisión están capacitados para constatar el nivel de respeto a los Derecho fundamentales. En este caso cuando hay una Decisión de la Comisión, como es el listado de países en los que se autoriza la trasmisión de datos personales, es obligatoria para todas las instituciones de un Estado y mientras no haya sido declarada inválida por el Tribunal de Justicia los Estados miembros no adoptar medidas contrarias a esa decisión. Por tanto, las instituciones nacionales no pueden rectificar a la Comisión pero, al mismo, tiempo no pueden negarse a que los ciudadanos ejerzan sus derechos. El TJEU considera que las autoridades nacionales pueden controlar, en los casos más extremos contra la intimidad, de manera restrictiva a partir de un alto umbral de condiciones. Pero, por norma general, no tiene competencia para decidir en los casos que se refieran a las garantías de terceros países. Luego se mantiene el principio de que los Estados miembros y sus instituciones no pueden rectificar las decisiones de la Comisión. Sin embargo, lo que hace el TJCE es considerar que la normativa en la que se basa la decisión de la Comisión es inválida porque asume competencias que no le corresponde y, por tanto, dejando sin validez el acuerdo de transferencia de datos con la UE.

Como resultado final la Comisión negoció con mucha premura un nuevo Tratado

[56] STJEU C-362/14 *Maximiliams Schrems vs Data Protection Commissioner*¸

con EE.UU. que regulase el movimiento de bases de datos, el *Private Shield*, que está más acorde con las garantías de la regulación europea que el anterior, el *Safe Harbour*. También ha servido para desatascar la nueva normativa sobre bases de datos en la UE: el Reglamento 2016/679 y la Directiva 2016/680 que llevabas cuatro años de retraso respecto a lo proyectado.

4. **Derechos de los interesados**

Una vez regulado como se tiene que gestionar la utilización de las bases de datos la Decisión Marco, siguiendo el precedente de la Directiva 1995/46, establece cuales son los derechos que tienen los sujetos de los que se obtienen los datos.

Este punto es muy importante en la normativa actual sobre utilización de datos personales, Directiva 95/46 y la Decisión Marco 2008/977, y en la que entrará en vigor en 2018, Reglamento 2016/679 y Directiva 2016/680. La regulación genérica de la utilización de bases de datos personales (Directiva 95/46 y Reglamento 2016/679) concede más derechos que la específica en materia penal (Decisión Marco 2008/977 y Directiva 2016/679). Esta última tiene básicamente dos derechos: Derecho a la información y Derecho a oponerse.

El primero se encuentra recogido en los artículos 16 y 17 de la Decisión Marco 2008/977 y se puede desglosar en dos partes. Por un lado, el deber de ser informado en lo relativo a la recopilación o tratamiento de datos personales por sus autoridades competentes, conforme al Derecho nacional. En esta cuestión se echa en falta que el legislador regulara también el acceso al contenido de la información. En este punto creo que, sin ser obligatorio por parte de la Decisión Marco, sería necesario y muestra de un buen tratamiento de los datos que la autoridad competente informase al solicitante de los da de alguna de la información básica que se requiere en la Directiva 95/46, en el artículo 11, es decir: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información como, por ejemplo, las categorías de los datos de que se trate, la existencia de derechos de acceso y rectificación de los datos que la conciernen.

Estos derechos se completan con los recogidos en el artículo 17, el Derecho de acceso a los datos, que es la posibilidad que tiene el sujeto de tener información de que se ha transmitido o puesto a disposición datos que le conciernen, información sobre los destinatarios o categorías de destinatarios a los que se les han remetido los datos, comunicar que datos se están tratando o al menos la confirmación de que se han realizado todas las comprobaciones posibles, sin ningún tipo de restricciones y sin retrasos ni gastos excesivos. Este derecho tiene limitaciones debido a la necesidad de secreto principalmente en los casos de que exista la posibilidad de obstaculización de investigaciones o procedimientos jurídicos de carácter oficial, la posibilidad de obstaculización la prevención, detección, investigación y enjuicia-

miento de infracciones penales o la ejecución de sanciones penales; proteger la seguridad pública; la seguridad del Estado; para proteger al interesado[57] o los derechos y libertades de terceros. En caso de denegación del Derecho de acceso se ha de realizar una comunicación justificada con el interesado y recordarle sus derechos procesales de reclamación. Es lógico que el derecho de acceso esté más restringido en materia policial que en un uso no relacionado con las investigaciones no penales. Así, en el uso general de los datos, el Derecho a la información tiene un contenido más amplio, consistente en a) confirmación datos que pueden ser procesados, que la información que se está registrando tiene un fin determinado, cuál va a ser su contenido y a quién se les va a trasmitir. Esa información ha de ser en un lenguaje accesible e inteligible.

Las instituciones europeas han considerado que es imposible ejercitar ese derecho en esos términos cuando el procesamiento de datos se encuentra en medio de una investigación policial y, por tanto, podemos extender la misma consideración a los casos de seguridad nacional. Esta es la razón por la que este derecho a conocer y modificar se encuentra limitado. El interesado puede obtener la confirmación del controlador o de la autoridad supervisora nacional sólo cuando los datos relativos a él han sido transmitidos o puestos a disposición e informados a los receptores a los cuales se les ha revelado y comunicados los datos que están bajo procesamiento o puede recibir una confirmación del supervisor nacional de que se han tenido en cuenta todas las verificaciones oportunas[58]. Curiosamente, en el sistema general existen más limitaciones. De esta forma se añaden la defensa, el interés económico y financiero, y la función de control, de inspección o reglamentaria por la autoridad[59]. Probablemente sería más interesante tener una autoridad supervisora europea ya que se trata de un problema que supera el nivel de los Estados, como pueda ser en EE.UU.[60]

El segundo de los derechos es el de rectificación, supresión o bloqueo, que se podrá ejercer en los casos regulados en los artículos 4, 8 y 9. Los Estados miembros deberán establecer si podrá ejercer su derecho de forma directa o mediante la autoridad nacional de control competente. Si se negase la rectificación, supresión o bloqueo se deberá notificar al interesado de forma escrita junto con los derechos que le asiste para recurrir la decisión.

A diferencia de la Decisión Marco 2008/977, el ciudadano tiene un derecho a oponerse al tratamiento de sus datos, salvo que la legislación nacional diga otra

[57] Suena cuando menos irónico, cuando no parternalista, que la autoridad pública del tratamiento de datos no ofrezca la información por proteger la seguridad del ciudadano que la demanda.

[58] Sentencia del TJUE C-553/07, *Rijkeboer*

[59] Artículo 13 de la Directiva 95/46.

[60] MACSÍTHIGH, D., "App law within: rights and regulation in the smartphone age", *Int. J Law Info Tech*, vol. 21, 2013, p. 173 y ss.

cosa. En las investigaciones de carácter criminal, como es obvio no se puede dejar en manos del ciudadano con qué datos puede trabajar la policía[61].

En caso en que se hayan visto afectados sus derechos, el sujeto tendrá derecho a una indemnización por los daños y perjuicios como consecuencia del tratamiento ilícito de una acción incompatible con las disposiciones nacionales. Si el daño y perjuicio se produjese por la transmisión de los datos la autoridad abonará al tercer Estado la indemnización que este le haya pagado al sujeto.

5. **Seguridad de tratamiento/procesamiento**

Como hemos podido apreciar la Decisión Marco deja muchas puertas abiertas a la limitación de los derechos de los ciudadanos y, dado el precedente de los casos en los que ha habido un uso indiscriminado del análisis de datos masivos, es necesario que se asegure un buen uso de los datos. En su primer acercamiento la Decisión Marco, en su artículo 22, se exige a los Estados Miembros que se obligue a que se tomen las medidas técnicas y de organización para proteger los datos de su destrucción accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizado, en especial cuando el tratamiento o transferencia se haga dentro de una red o mediante acceso automatizado directo.

En el caso de tratamiento automatizado de datos se exige que cada Estado tome las siguientes medidas:

a) impedir el acceso de personas no autorizadas a las instalaciones utilizadas para el tratamiento de datos personales (control de acceso a las instalaciones);
b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o retirados sin autorización (control de los soportes de datos);
c) impedir que se introduzcan datos sin autorización en los ficheros y que puedan conocerse, modificarse o suprimirse sin autorización datos personales conservados (control de la conservación);
d) impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas mediante equipos de transmisión de datos (control de la utilización);
e) garantizar que las personas autorizadas para utilizar un sistema de tratamiento automatizado de datos solo puedan tener acceso a los datos para los que se les ha autorizado (control del acceso);
f) garantizar que sea posible verificar y comprobar a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse datos personales mediante equipos de transmisión de datos (control de las comunicaciones);

[61] Artículo 12 de la Directiva 95/46.

g) garantizar que pueda verificarse y comprobarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado de datos y en qué momento y por qué persona han sido introducidos (control de la introducción);
h) impedir que durante la transmisión de datos personales y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);
i) garantizar que los sistemas utilizados puedan repararse en caso de fallo del sistema (recuperación);
j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos conservados no se degraden por fallos de funcionamiento del sistema (integridad).

Los Estados miembros regularán que sólo pueda designarse como encargado de tratamiento a quien pueda garantizar el cumplimiento de las medias de técnicas y de organización para evitar la destrucción accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizado, en especial cuando el tratamiento o transferencia se haga dentro de una red o mediante acceso automatizado directo.

6. **Evaluación de riesgos a la Intimidad. Privacy Impact Assessment (PIA)**

Como todo avance tecnológico la utilización del Big Data lleva consigo, en sus primeras fases de desarrollo, una utilización responsable y ética, entendida no como algo bueno o malo, sino como guías y directrices que orienten un determinado campo[62] en el que el déficit en la protección legal de la persona no está correctamente realizado[63] o no es factible por la ponderación de intereses. Esto implica que, aparte de las medidas de seguridad descritas y la limitaciones que exige la normativa al tipo de datos, a la finalidad por la que se van a recolectar esos datos y a la duración limitada del procesamiento, se haga un tratamiento lo más limitado posible por la importancia de los Derechos Fundamentales que están en juego.

Para ello es necesario que se redacte un documento antes de la obtención de los datos en el que se reflejen de forma precisa y clara todos los aspectos expresados anteriormente y, además, especificar cuáles son los sistemas de seguridad que se van a imponer en el sistema (creación de registros de acceso, acceso mediante doble entrada, cortafuegos, sistema de pseudoanonimización, cursos de formación para el personal que va a tener acceso, etc.) Este documento, conocido por PIA se

[62] WRIGHT, D., FRIEDEWALD, M., "Integrating privacy and ethical impact assessments", *Science and Public Policy*, 40, 2013, p. 756.
[63] LÓPEZ JIMÉNEZ, D., "Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital", *Estudios Constitucionales*, 11, 2, 2013, p. 592.

tiene que revisar cada tiempo según va evolucionando el tratamiento de los datos. El PIA debe de tener una perspectiva amplía en la que se deben abordar los impactos en la intimidad y no limitarse únicamente a si es conforme a la ley[64]. Es necesario, por tanto, que cada organización tenga diseñado un PIA *ad hoc* para adecuar su comportamiento con los datos a sus necesidades y riesgos[65]. Los puntos básicos que debería cubrir, de forma general, serían 15[66]. Para empezar, el análisis de si es necesario un PIA o no, siempre que vaya a tener influencia en el diseño del proyecto al que se va a aplicar, que en nuestro objeto de estudio es imprescindible. Un segundo paso es determinar un equipo de trabajo para realizarlo. Aunque el responsable del PIA es el encargado del procesamiento de datos, la tarea de control no es fácil por lo que tiene que ser un equipo multidisciplinar entre personal técnico, jurídico, ético, de usuarios finales y de ciudadanos. Trazar un plan estratégico de impacto, con los temas, las personas que van a trabajar, reparto de tareas, un cronograma y la consulta a los expertos externos. También es necesaria una descripción del proyecto que se va a analizar, cómo se va a desarrollar con un cronograma de trabajo diseñado, así como analizar quienes son los posibles usuarios del proyecto. En relación directa sobre cómo se va a desarrollar el proyecto, es preciso determinar la forma en que se va a transmitir el flujo de información, que datos se va a solicitar, con qué fin, quién los va a recolectar, cómo se van a almacenar, con qué medidas se va a proteger y distribuir y como se va a procesar. El recurrir al consejo de los usuarios finales es básico para determinar de forma precisa cuales son las necesidades que tienen y cómo se va a utilizar en la práctica. En este punto es cuando será necesario un análisis legislativo sobre la adecuación del proyecto a la legislación vigente.

Creada la infraestructura se deben identificar los riesgos y posibles soluciones mano a mano con los usuarios y la magnitud del impacto en caso de que se produzcan. Después de formularán las recomendaciones, que deben estar redactadas en un informe que se debe hacer público para poder ser debatido con los interesados y se deben aplicar las recomendaciones sugeridas y aprobadas. En caso de que no se vayan a poner en marcha hay que explicar por qué no se ha hecho y justificar adecuadamente, la decisión.

Además es necesario que sea revisado y evaluado por personas externas, de tal manera que no quede controlados sólo por personal interno al proyecto. Lo cual puede implicar que haya que actualizar su contenido por sus comentarios o por los cambios que se puedan producir durante el proyecto. Finalmente, es necesario un plan de formación para aquellos que van a lidiar con el procesamiento de datos.

La introducción de los PIA en el día a día de la utilización de datos masivos se

[64] CLARKE, R., *Privacy Impact Assessment*, 2003, p. 2.

[65] RETZER, K., "Alinging corporate ethics compliance programs with data protection", *PDP* 13 6 (5), p. 2.

[66] WRIGHT, D., Friedewald, M., "Integrating…", cit., p. 760.

debe a las recomendaciones del Grupo de trabajo del artículo 29[67] y la obligación a las autoridades de crear estándares de actuación, como la oficina de protección de datos y se ha establecido como un elemento básico[68], al igual que los *compliance programs*[69] se han considerado documentos imprescindibles en la responsabilidad penal de las empresas.

Siguiendo esta influencia el Reglamento 2016/679 y la Directiva 2016/680 obligan en sus artículos 35 y 27, respectivamente, a que los Estados Miembros dispongan que el responsable de tratamiento realice una evaluación de impacto de las operaciones de tratamiento cuando la posibilidad de riesgo para la intimidad sea alta. El contenido de PIA en los supuestos de investigaciones policiales deberá ser el siguiente: una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas.

Sin embargo, en los casos de utilización de datos en el ámbito no penal los requisitos impuestos por el Reglamento son mucho más extensos. Además de los ya mencionados se exige uno más que es la evaluación de necesidad y proporcionalidad de las operaciones de tratamiento. Además, se establece la obligación sobre el encargado del procesamiento de tener que requerir asesoramiento por parte de la autoridad de protección de datos, de usuarios y de externos como se planteaba en los puntos de desarrollo del PIA. A esto hay que añadir la publicación de listas de los tratamientos y procedimientos que requieran una evaluación de impacto. Y en el caso de tratamiento de datos a gran escala (Big Data) se requerirá como extra que se evalué el impacto en la intimidad cuando se utilicen sistemática y exhaustiva aspectos personales, se procesen datos especiales o relativos a condenas o sanciones penales o la observación sistemática de una gran zona de acceso.

Este punto es el que tratábamos en el primer capítulo que era una necesidad en el procesamiento de datos masivos ya que es la única forma de crear una confianza con el ciudadano para que se puedan utilizar sus datos. El Derecho a la intimidad con el Big Data se ve en un serio riesgo y, desde luego, no se puede considerar que va a existir como anteriormente.

Es por ello que el legislador comunitario ha optado por este sistema de autocontrol y de objetivación de la responsabilidad en caso de mal uso de las técnicas de tratamiento de datos.

[67] WRIGHT, D., "Making Privacy Impact Assessment More Effective", *The Information Society*, 29, 2013, p. 307.

[68] Que se lleva utilizando desde los 90 en los países anglosajones. WRIGHT, D., FRIEDEWALD, M., "Integrating…", cit., p.756.

[69] RETZER, K., "Alinging…", cit., p. 3.

7. **Sanciones**

Lo que no ha cambiado con la creación de la Directiva 2016/680[70] es el tema de las sanciones. Tanto en esta norma como en la Decisión Marco[71] se utiliza un clásico recurso en el Derecho sancionador comunitario que es "Estados miembros establecerán las normas en materia de sanciones aplicables a las infracciones de las disposiciones adoptadas con arreglo a la presente Directiva y tomarán todas las medidas necesarias para garantizar su cumplimiento. Las sanciones establecidas serán efectivas, proporcionadas y disuasorias". Sobre la naturaleza de estas sanciones siempre suele a ver dudas[72]. Hoy día las sanciones se encuentran en Ley Orgánica de Protección de Datos y se trata de sanciones pecuniarias y, en los casos, en que sea una entidad pública la infractora se sancionará dentro de las posibilidades que ofrece el sistema disciplinario de las Administraciones públicas, luego se trata de sanciones de carácter administrativo. Sin embargo, esta redacción no elimina la posibilidad de sanciones penales como ha ocurrido en otros ámbitos donde el Derecho Europeo ha intervenido como puede ser el fraude de subvenciones de la Unión Europea, el Derecho la pornografía infantil, el terrorismo, etc. Sólo en el caso del medio ambiente se ha establecido expresamente la necesidad de sanciones penales.

Sin embargo, el Reglamento 2016/679 si dice expresamente en su exposición de motivos que es necesario poner sanciones penales[73], aunque no en su articulado, que se encuentra redactado de la siguiente forma: Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias. Ahora el legislador no menciona expresamente la naturaleza jurídica de las sanciones que se deben aplicar. Lo único que deja claro es que deben ser diferentes a las administrativas. Esto puede tener una justificación de derecho comparado ya que en otros ordenamientos existe otra modalidad de sanciones, como es el caso alemán donde existen las *Ordnungswidrigkeiten*¸ a medio camino entre las sanciones administrativas y las sanciones penales, como es también el caso en Italia, y que por eso deje la posibilidad abierta, pero entonces no tendría mucho sentido que en la exposición de motivos se hablase claramente de penales.

Con respecto a nuestro objeto de estudio tenemos la libertad de decidir qué tipo de sanción se impondría, pero tenemos argumentos para decantarnos por las san-

[70] Artículo 57 de la Directiva 2016/680

[71] Artículo 24 de la Decisión Marco 208/977/JAI

[72] Por ejemplo, en el Reino Unido se cantiga como delito los casos más grave que afecte a la intimidad de las personas. Cfr. CAREY, P., TREACY, B., *Data*…, cit., p.248-259.

[73] Puntos 149 y 152 de la exposición de motivos.

ciones penales si consideramos que los datos que se utilizan están menos restringidos de los del Reglamento, que se ofrecen menos derechos a los ciudadanos con respecto a sus datos y se pueden poner muchas más limitaciones al ejercicio de los derechos de acceso, información y borrado y rectificación de los ciudadanos.

En la normativa sobre investigaciones policiales hemos visto como se argumenta que se necesitan datos para una correcta investigación policial en base al criterio de la seguridad. Además, hemos visto como las técnicas de Big Data, mal utilizadas, pueden tener un gran impacto en la intimidad de las personas y, sin embargo, en el equilibrio entre intimidad y seguridad se permite decantarse por esta última, básicamente, porque se concede una confianza en los cuerpos y fuerzas de seguridad del Estado. Por tanto, dado que el daño causado en caso de mala utilización es mucho más grave que cuando se trata del sector privado, al que sí se le podría imponer una pena, dado que los datos que se pueden utilizar son más sensibles que los que se permite al sector privado y dado a que los Derechos de los ciudadanos tienen limitaciones para poder ejercitarse, debemos considerar que las sanciones deben de ser como mínimo iguales a las del sector privado, si no superiores ya que el daño puede tener un alcance mayor.

V. **CUESTIONES ÉTICAS**

El tema de la utilización del Big Data todavía es muy novedoso y aunque se está intentando regular es de extremada complejidad. De hecho se estaba esperando la reforma de la legislación europea desde el 2012, año en el que se anunció la salida del nuevo reglamento sobre la utilización de bases de datos, y por los cambios acontecidos se ha retrasado hasta abril de este año en el que se ha dado luz verde al Reglamento 2016/679 y la Directiva 2016/680. La dificultad legislativa es grande y es por ello que la regulación ha tenido que normativizar, lo que tendría que ser un comportamiento ético, lo que es el código de buenas prácticas, que es la única salvaguarda decente que nos queda. El que los cuerpos y fuerzas de seguridad del Estado puedan utilizar estas técnicas depende únicamente de su buen uso y de las mismas las sanciones que se pueden imponer por su mal uso.

El uso de esta tecnología sólo se puede justificar cuando el objetivo perseguido sea la prevención o combate de graves amenazas a la seguridad y cuando la amenaza implique un alto riesgo para el Estado o las instituciones democráticas que no pueda ser combatida por otros medios, así como delimitar temporalmente el uso y almacenamiento de los datos y la selección de los mismos.

Otro de los problemas es como gestionar los datos y en particular los datos personales. Los datos tienen que procesarse de forma anónima. En cualquier caso si los datos son utilizados en una operación los datos tienen que permanecer anonimizados para permitir la posibilidad de devolución a su dueño. En 2013 el Tribunal de

apelación del Reino Unido, en su sentencia R (Catt) contra la asociación de jefes de policía y otros, afirmaba que hay un ánimo legítimo en el almacenaje y retención de información en las bases de datos de la policía cuando el fin es la protección del orden y del crimen y el mantenimiento de los derecho y libertades de los demás[74] permitiendo su uso con el fin de proteger los derechos de los demás ciudadanos.

Un tema importante es el de los datos de menores. Por norma general se deberían evitar utilizar información concerniente a menores de edad, Dado que los sistemas de procesamiento recogen mucha información para detectar futuras amenazas del Estado podríamos considerar que eliminar los datos de los menores no va a influir en la detección de las mismas. Por ello es posible que los sistemas de detección puedan trabajar sin esos datos. Los menores deben tener un alto nivel de protección de su intimidad porque se encuentran en una edad especial en donde su personalidad no está del todo formada y, en su caso, la protección de su intimidad es muy importante para su futuro.

Otra cuestión ética de gran relevancia es el de las fuentes de donde se puede extraer la información. Básicamente Internet tiene dos tipos de fuentes abiertas y cerradas. Dado que estás pueden romper las expectativas de valoración del Estado es mejor reducirlas sólo a las fuentes abiertas, aquellas a las que se puede acceder libremente, sin necesidad de romper ningún código. En las fuentes abiertas la gente da información voluntariamente en los medios sociales como pueden ser foros, blogs, redes sociales y otro tipo de páginas interactivas o aplicaciones[75] permitiendo que otras personas tengan acceso a la misma. La opinión del Grupo de trabajo sobre datos abiertos no dice nada de su uso por parte del sector público en cuestiones de seguridad. Sí lo hace en conexión con el sector privado y recomiendan su anonimización en su utilización y en los casos en que no sea posible, se recomienda a las oficinas de protección de datos que se tome un acuerdo de compatibilidad para su uso posterior[76]. En cualquier caso la nueva normativa permite el uso de los datos que el titular ceda de forma abierta.

De especial interés es si el Estado pude utilizar todos los datos que posee de los ciudadanos o no[77]. Podemos considerar estos datos como una fuente abierta de datos pero no hay que olvidar que el consentimiento de la persona limita el fin por el que se pueden usar.

En cualquier caso la clave para el correcto uso de los datos se tiene que basar en el PIA que clarifique su utilización. Este documento, que deben de conocer los que

[74] OSWALL, M., "Joining the dots – intelligence and proportionality", *Privacy and Data Protection*, vol. 13, 2013, p. 6.

[75] WHITCROFT, O., "Social media – challenges in control of information", *Privacy and Data Protection*, vol. 13, 2013, p. 7

[76] TREACY, B., BAPAT, A., "Purpose limitation – clarity at last?", *Privacy and Data Protection*, vol. 13, p. 11.

[77] MCDONAGH, M., "E-Government in Australia: the Challenge to privacy of Personal Information", *Int. J Law Info Tech* 10, 2002, p. 342.

van a trabajar con esos datos, es un conjunto de medidas y directrices que va a determinar las zonas críticas para la privacidad y que determina protocolos de actuación ética en su tratamiento. En esta evaluación hay que determinar cuál va a ser su finalidad legítima, es decir, que el propósito por el cual se utiliza es legítimo, en nuestro caso evitar la amenaza concreta que se esté intentando evitar. En estos casos viene justificado por la Decisión Marco de 2008, y su futura sucesora la Directiva 2016/680 y el artículo 8 de la Convención Europea de Derechos Humanos.

Además, es necesario especificar la necesidad de la utilización de estas técnicas y de los robots. Esto significa que no puede existir otra forma de poder hacer frente a estas amenazas. Como hemos señalado con anterioridad las amenazas de las que estamos hablando se realizan en gran parte por Internet. Al encontrarse en un espacio prácticamente ageográfico y sin fronteras, e indudablemente fuera de del alcance del Estado, es indudable que la necesidad de conseguir la información necesaria que se encuentra en la red es, estratégicamente, vital para prevenir dichas soluciones. Ya no sólo para evitar las situaciones de riesgo, también es necesario para combatir las amenazas reales que se puedan dar. Sin embargo hay que señalar que al igual que hay instituciones que promueven su utilización[78] también hay detractores que consideran que no aportan nada a la prevención ya que prefieren a los analistas humanos a la utilización de máquinas[79]. Este argumento no está falto de razón. Y es por ello que las decisiones finales no son tomadas por máquinas sino por humanos. Los robots sólo detectan indicios que deben ser validados por personas.

Por otro lado, es cierto que la sociedad no es favorable a la utilización de sus datos por parte del Estado de forma general. Sin embargo, es cierto que la sociedad al mismo tiempo encarga la protección de sus vidas y la seguridad a este. En esa dualidad debemos entender que bajo el correcto uso de los mismos y la finalidad se puede permitir su uso.

Vista la necesidad también es oportuno preservar el principio de proporcionalidad en su uso. Dado que en los casos de utilización estratégica el sistema no tiene ningún interés en las personas sino en las amenazas podemos considerar que el respeto a los Derechos fundamentales, por un lado, y la detección de amenazas a la seguridad, por otro, es proporcional. En los caso de su utilización operacional puede ser más discutido. La proporcionalidad en este caso viene dada por asegurar el buen uso de los datos y su utilización limitada en el tiempo. Sólo podrá conside-

[78] Véase EUROPOL, *The Internet organized crime threat assessment (IOCTA)*, 29 September 2014, p. 81 y ss., https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta (visto 27/09/2015)

[79] REES, M., La loi sur le renseignement sera préjudiciable à nos équilibres psychiques, sociaux et démocratiques, Lettre ouverte au Conseil constitutionnel, *Next Inpact*, 20 enero 2015, http://www.nextinpact.com/news/95859-la-loi-sur-renseignement-sera-prejudiciable-a-nos-equilibres-psychiques-sociaux-et-democratiques.htm (visto 27/09/2015)

rarse proporcional cuando se limite su uso a las necesidades concretas del caso que se quiere combatir y se utilicen sólo los datos necesarios para el caso específico. La información para los supuestos de uso estratégico se basa principalmente en el procesamiento de hechos y situaciones que en algunas situaciones están en conexión con el nombre de la persona (que al mismo tiempo puede estar en conexión con otras personas. Como en principio en este tipo de operaciones no es necesario utilizar datos personales y en los casos en los que se incluyan va a ser por accidente ya que no es el objeto de las operaciones. Es por ello que se tienen que tomar algunas medidas de seguridad para evitar un impacto mayor en estas situaciones. Así, que se respete la ley de cada Estado, que las personas que tengan acceso a los datos personales tengan un sistema de autentificación y de control de acceso así como un registro del motivo del acceso.

Especial mención necesitan los metadatos asociados a los archivos. Son piezas de información adherida a fotografías, mensajes en las redes sociales, comentarios en blogs, etc. Estos metadatos pueden consistir en información como la geolocalización, la hora, el tiempo de software utilizado, etc. que permiten un rastreo de la información. Estos metadatos pueden ser considerados, por sí mismos, como datos que pueden ser procesados sin ser considerados como personales pero que, sin embargo, pueden conducirnos a la identificación de un individuo. El procesamiento posterior de estos datos puede concernir a cualquier persona que publique un artículo o una opinión en una red social y esto produce una interferencia en la intimidad de las personas aunque sea de forma indirecta. Este tipo se situaciones son las que, aun no siendo queridas por el análisis de datos, necesitan de una especial protección y por las que una limitación de las personas a las que tiene acceso al sistema, el almacenar los metadatos en un lugar diferente al del resto de datos, poner diferentes niveles de seguridad, asegurar que la trazabilidad de los datos sólo la puede realizar determinado personal autorizado y sólo para determinados propósitos. Es preciso que se realice un registro de las entradas en el sistema y que esté controlado por una unidad independiente de los cuerpos y fuerzas de seguridad.

Si se respetan estas medidas y dado que la finalidad por la que se utilizan estas técnicas de investigación están justificadas se puede entender que el impacto en la intimidad de los ciudadanos es lo suficiente limitado para que el equilibrio entre seguridad y el Derecho a la intimidad sea el correcto.

Estas medidas recogidas en la evaluación deben ponerse en funcionamiento antes de la entrada en funcionamiento de esta tecnología y a ser posible antes de que la normativa sea aprobada o de que se adopte la autorización de procesamiento de los datos.

Desde el punto de vista ético, la utilización de robots para la toma de decisiones automáticas (como pueda ser matar) ha generado mucha controversia[80] en la pri-

[80] http://www.stopkillerrobots.org/2015/04/humancontrol/ (visitado 15/09/2015)

mavera de este año. Eminentes figuras como Jody Willians[81], premio nobel de la paz, o expertos en inteligencia artificial[82]. La toma de decisiones automática en cuestiones de prevención del crimen tiene problemas parecidos y es por ello que los robots tampoco deberían tomar decisiones sin el control de un humano en este campo. Como las investigaciones para evitar el crimen pueden afectar a los sujetos de forma indirecta es preferible que la detección de amenazas e investigaciones dependan finalmente de la decisión de un humano ya que los falsos positivos en la detección están entorno al 25%.

VI. **CONCLUSIÓN**

La utilización de Internet como sistema de comunicación o espacio en que se comenten delitos es una realidad hoy día. Es por ello que no se puede renunciar a las posibilidades que otorga para prevenir los posibles crímenes que se puedan producir. Los avances en procesamiento de datos a gran escala ofrecen a los Estados una herramienta muy importante para la defensa contra las posibles amenazas que hemos podido ir analizando en el presente trabajo. Sin embargo, no es menos cierto, que plantea grandes incógnitas sobre su uso por parte de los ciudadanos y el respeto a sus derechos, en particular los relativos a la intimidad y la libertad de pensamiento.

En cualquier caso, el uso del Big Data tiene sus limitaciones técnicas. Este modelo de procesamiento es buena para las correlaciones no causales que normalmente no se pueden utilizar como prueba en un proceso[83]. Es por ello que dentro de los dos usos que hemos comentado, estratégico y operacional, sólo se debería utilizarse en el primero de ellos.

Es incuestionable que el Estado tiene que utilizar este tipo de herramientas en la lucha contra la delincuencia. No es admisible dejar en manos de los criminales unas herramientas tan poderosas sin que se puedan utilizar para contrarrestar en los casos de seguridad nacional. El único problema es cómo se va a controlar su utilización. Está claro que su uso por parte del Estado no puede estar legitimado cuando no hay un equilibrio entre la afectación a los Derechos Humanos y la protección que se quiere dar a los mismos ante los posibles ataques que se vayan a producir. En cualquier caso es indudable que la justificación de una restricción de la intimidad para proteger un bien mayor, la seguridad, es una delgada línea que, hoy día, podríamos considerar más ancha ante la realidad del desarrollo de las actuales técnicas de procesamiento de datos que hemos comentado anteriormente. Es por ello que los sistemas jurídicos tienen que cambiar para regular su uso conforme a

[81] WILLIAMS, J., "Borderless battlefield: the CIA, the US Military and the drones", *International Journal of Intelligent Ethic*, vol. 2, 2011, pág. 25 y ss.
[82] http://futureoflife.org/AI/open_letter_autonomous_weapons (visitado 13/09/2015)
[83] MAYER-SCHÖNBERG, V.; CUKIER, K., *Big Data*..., cit., p. 171 y ss.

los principios y reglas del Estado de Derecho. Este es un reto que se ha de afrontar desde una regulación supranacional y que la Unión Europea tiene que liderar.

La normativa europea tiene las garantías suficientes para garantizar el correcto uso de este tipo de robots por parte de los cuerpos y fuerzas de seguridad del Estado para conseguir buenos resultados en la lucha contra las amenazas tecnológicas y posibles ataques a infraestructuras estratégicas de un país. La figura de un supervisor independiente es básica en el control de este tipo de investigaciones para asegurar que los derechos de los ciudadanos están adecuadamente protegidos. Pero aun así, quedan más problemas por resolver.

Como la adquisición de datos se realiza en un espacio sin fronteras y por ello que sea necesario pensar en términos de normativa internacional referente al tratamiento de datos, sistemas internacionales de protección derechos humanos y, probablemente, de una jurisdicción internacional para resolver los problemas que este tipo de lucha contra el crimen va a presentar.

La gran novedad en la nueva regulación es la obligación de realizar el PIA. Esta valoración de riesgos se tiene que centrar en los datos en sí, el procesamiento de los mismos y en el análisis, tomando las medidas adecuadas para su correcto uso. Así, en la primera fase del mismo, la recolección de datos, hay que determinar y especificar, con el fin de limitar las acciones de los operarios del sistema, si se van a recolectar datos de fuentes abiertas o si se va a entrar en las zonas protegidas para la obtención de datos. Justamente, con la determinación de estos puntos, es cuando se podrá dar autorización, por parte de la autoridad competente para el procesamiento y análisis de los datos. Así mismo habrá que especificar los sistemas de pseudoanonimización de los mismos, sistemas de protección de los datos y los sistemas de seguridad en los casos en los que se vayan a transferir a terceras partes o a otros lugares para su utilización. Dentro de la segunda fase habrá de determinar un registro de entrada al sistema para controlar que sólo tengan acceso al mismo las personas autorizadas. Dentro de las medidas de seguridad sería interesante poner un acceso con doble contraseña de tal manera que sirva de protección en el caso de que se acceda al primer nivel de seguridad. Así mismo, es necesario un sistema de alerta por acceso a las personas encargadas de su protección. En esta segunda fase en la que el robot empieza a realizar el análisis de datos es preciso este se realice en la medida de los posible sin utilizar datos sensibles como puedan ser nombre, raza, sexo, religión, ideología política, datos relativos a la orientación sexual o datos genéticos. Y si es preciso utilizarlos que se haga de forma automática por el robot pero que no se rebele la información en el resultado final. En la tercera y última fase hay que evitar que las decisiones finales sean tomadas directamente por un robot. En esta última fase los analistas son los que tienen que tomar la decisión final a la hora de determinar si se trata de una amenaza y cuál será la respuesta que se dé a la misma.

BIBLIOGRAFÍA

BAE SYSTEMS Detica, 2012 http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf

BBC, 2012, http://www.bbc.com/news/world-asia-17922021

CAREY, P., TREACY, B., *Data Protection. A Practical Guide to UK and EU Law*, 2015, Oxford University Press

CLARKE, R., *Privacy Impact Assessment*, 2003

CLOUGH, J., *Principles of cybercrime*, Cambridge University Press, Cambridge, 2012

ERIKSEN-JENSEN, M., "Holding back the tidal wave of cybercrime," *Computer Fraud & Security*, vol. 03, 2013

EUROPOL, *The Internet organized crime threat assessment (IOCTA)*, 29 September 2014

FARREL, H., The hack on the U.S. government was not a "cyber Pearl Harbor" (but it was a very big deal), 2015. http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/06/15/the-hack-on-the-u-s-government-was-not-a-cyber-pearl-harbor-but-it-was-a-very-big-deal/

FIODORAVA, A., "La transmisión de información personal y datos personales en la Unión Europea para fines de investigación de delitos", Colomer Hernández, I., Oubiña Barbolla, S., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, 2015

GALÁN MUÑOZ, A., "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: Hacia una nueva orientación de la política criminal de la Unión Europea", Colomer Hernández, I., Oubiña Barbolla, S., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, 2015, Aranzadi

GENULIUS, S., The data explosión in 2014 minute by minute, http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/

GREENWALD, G., MACASKILL, E., POITRAS, L., "Edward Snowden: the whistleblower behind the NSA surveillance revelations", The Guardian, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

IBM http://www.ibmbigdatahub.com/sites/default/files/infographic_file/4-Vs-of-big-data.jpg?cm_mc_uid=17285312897914615394571&cm_mc_sid_50200000=1461832086

INFOSEC Institute (2013) http://resources.infosecinstitute.com/botnets-and-cybercrime-introduction/

KIND, E.J., *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*¸ Springer, 2013

KSHETRI, N., "Cybercrime and cyber-security issues associated with China: some economic and institutional considerations", *Electronic Commerce Research*, vol. 13, 2013

KSHETRI, N., "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers", *Crime, Law and Social Change*, vol. 60, 2013

LÓPEZ JIMÉNEZ, D., "Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital", *Estudios Constitucionales*, 11, 2, 2013

MACSÍTHIGH, D., "App law within: rights and regulation in the smartphone age", *Int. J Law Info Tech*, vol. 21, 2013

MAYER-SCHÖNBERG, V.; CUKIER, K., *Big Data. A revolution that will transform how we live*, John Murray, London, 2013

MCDONAGH, M., "E-Government in Australia: the Challenge to privacy of Personal Infor-

mation", *Int. J Law Info Tech* 10, 2002
MEILHAN, P/ BOTHELO, G., French TV network hit by 'powerful cyberattack', 2015. http://edition.cnn.com/2015/04/08/europe/french-tv-network-cyberattack/
OERMANN, M., *Individualdatenschutz in europäischen Datenschutzrecht*, 2012, Centaurus
OSWALL, M., "Joining the dots – intelligence and proportionality", *Privacy and Data Protection*, vol. 13, 2013
OUBIÑA BARBOLA, S., "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", Colomer Hernández, I., Oubiña Barbolla, S., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, 2015
REES, M., La loi sur le renseignement sera préjudiciable à nos équilibres psychiques, sociaux et démocratiques, Lettre ouverte au Conseil constitutionnel, *Next Inpact*, 20 enero 2015
RETZER, K., "Alinging corporate ethics compliance programs with data protection", *PDP* 13 6 (5)
SOOD A. K., ENBODY R. J. & BANSAL R., "Dissecting SpyEye. Understanding the design of third generation botners", *Computer network*, vol. 57, 2013
SÜDDEUTSCHE ZEITUNG, "Datenschutzbeauftragte wirft BND systematische Gesetzesverstöße vor", http://www.sueddeutsche.de/politik/ueberwachung-datenschutzbeauftragte-wirft-bnd-systematische-gesetzesverstoesse-vor-1.3145616
THIELMAN, S., JOHNSON, C., "Mayor cyber attack disrupts internet service across Europe and USA" https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service
TREACY, B., BAPAT, A., "Purpose limitation – clarity at last?", *Privacy and Data Protection*, vol. 13
UNODC, Comprehensive Study on Cybercrime, 2013
VAN DER SLOOT, B., "How to asses privacy violations in the age of Big Data? Analysing the three different test developed by the ECtHR and adding for a fourth one", Information & Communications Technology Law, 2015. P. 6 http://dx.doi.org/10.1080/13600834.2015.1009714
WEAVER, M., "Security services spied on 20 high-profile people in questionable operations", https://www.theguardian.com/world/2016/jul/27/mi5-and-gchq-spied-on-20-high-profile-people-in-questionable-operations
WHITCROFT, O., "Social media – challenges in control of information", *Privacy and Data Protection*, vol. 13, 2013
WILLIAMS, J., "Borderless battlefield: the CIA, the US Military and the drones", *International Journal of Intelligent Ethic*, vol. 2, 2011
WRIGHT, D., "Making Privacy Impact Assessment More Effective", *The Information Society*, 29, 2013
WRIGHT, D., FRIEDEWALD, M., "Integrating privacy and ethical impact assessments", *Science and Public Policy*, 40, 2013