SECCIÓN III – PROCESO PENAL

SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

RELACIÓN GENERAL

Lorena BACHMAIER WINTER*

Lista de abreviaturas

Art./art.	Artículo
CEDH	Convenio Europeo de Derechos Humanos
CoE	Consejo de Europa
CPP	Código procesal penal
FISA	*Foreign Intelligence Surveillance Act*
ILP	*Intelligence led policy*
NSA	*National Security Agency*
para.	Parágrafo
SJP	Sistema de justicia penal
TEDH	Tribunal Europeo de Derechos Humanos
TI	Tecnología de información
TIC	Tecnologías de información y comunicación
TOC	Transnational organized crime/criminalidad organizada transnacional
UE	Unión Europea
UN	United Nations/Naciones Unidas
UNODC	United Nations Office on Drugs and Crime/Oficina de las Naciones Unidas contra la Droga y el Delito

I. Contenido y objetivos del informe general

El presente rapport general ha sido preparado para el XIX Congreso Internacional de Derecho Penal que se celebrará en Rio de Janeiro del 31 de agosto al 6 de septiembre de 2014, en el marco de la AIDP (*Association Internationale de Droit Pénal/International Association of Penal Law*). El tema de este congreso mundial gira en torno a la utilización y el impacto de las TIC en los sistemas de derecho y justicia penal, con la finalidad de entender mejor y de hacer frente a los desafíos que la sociedad de la información representa para la justicia penal. Lo cual es de extrema importancia, si se tiene en cuenta que el camino hacia la sociedad de la información parece irreversible y afecta a virtualmente todos los aspectos de la vida social[1]. La Sección III se centra en las transformaciones que el desarrollo de las TIC han producido en la investigación y en el proceso criminales, y tiene por objeto proporcionar una perspectiva global de cómo el uso de TIC ciertamente abre las puertas a nuevas soluciones y posibilidades en el modo de investigar, perseguir y juzgar los delitos; pero también lleva consigo no pocos riesgos para la tutela de los derechos humanos, especialmente el derecho a la privacidad y el derecho a la protección de datos. Este rapport general está basado en completos y excelentes informes nacionales, que dan respuesta al cuestionario preparado en su día por el fallecido Prof. Nijboer. Estos informes nacionales, que se han recibido entre enero y agosto de 2013, provienen de 15 países: Argentina, Austria, Bélgica, Brasil, China, Colombia, Croacia, España[2], Estados Unidos, Finlandia, Holanda, Italia, Japón, Suecia y Turquía[3].

Además, el informe general ha tenido en cuenta los excelentes informes especiales en materia de protección de datos en la UE, las iniciativas de la UE sobre TIC, las TIC y el derecho de defensa, el impacto de los medios de comunicación en los sistemas de justicia penal (SJP), y el rapport especial sobre Finlandia. En nombre de la AIDP y en el mío propio, quisiera agradecer sinceramente a todos los rapporteurs sus magníficas aportaciones. Junto a

* Catedrática (acred.) de Derecho Procesal, Universidad Complutense, Madrid, España (l.bachmaier@der.ucm.es).

[1] Así se hacía ya notar, en 1993, en el *White Paper on Growth, competitiveness and employment. The challenges and ways forward into the 21st Century*, también conocido como el Plan Delors, COM (93) 700, de 5 diciembre 1993.

[2] No hay informe nacional de España en el CD adjunto. Este informe debería haber sido escrito por mí misma pero, por problemas de tiempo, he preferido concentrarme en el informe general, en lugar de escribir un texto separado sobre la situación de las TIC y el proceso penal en España. No obstante, el marco jurídico español y su práctica son valoradas en este rapport general.

[3] Los autores de los informes nacionales son: Javier de Luca y otros (Argentina), Farsam Salimi (Austria), Daniel De Wolf (Bélgica), Fauzi H. Choukr y Coriolano Almeira (Brasil), Song Yinghui y otros (China), (Colombia), Elizabeta Ivicevic (Croacia), Stephen Thaman (Estados Unidos), Helena Vihriälä (Finlandia), Tijs Kooijmans y Paul Mevis (Holanda), Giulio Illuminati (Italia), Tatsuhiko Inatani (Japón), Nils Rekke (Suecia), y Serap Keskin Kiziroglu y otros (Turquía)

esos rapports nacionales y especiales, la preparación de este informe general ha requerido estudiar los más relevantes documentos e informes de Naciones Unidas, convenios y recomendaciones del Consejo de Europa (CoE), y otros convenios internacionales[4]. El UNODC *Comprehensive Study on Cybercrime*[5], publicado a principios de 2013, ha sido especialmente útil e ilustrativo para reunir información y prácticas relativas a países de los que no había rapports nacionales. Y, naturalmente, se ha consultado la literatura jurídica de mayor importancia, con especial atención a los estudios publicados en lengua inglesa.

A pesar del esfuerzo realizado para lograr una cobertura global del tema de las TIC en el ámbito de la justicia penal, obviamente el informe contiene lagunas, puesto que no se ha podido disponer de rapports de todas las secciones nacionales de la AIDP, y porque es imposible tratar todos los países y todos los problemas que surgen en cada ordenamiento jurídico. No obstante, el hecho de que este informe no aborde todas las áreas a nivel global no ha de considerarse una deficiencia. En primer lugar, porque la finalidad de este rapport general es proporcionar un estudio comparativo que presente y analice los asuntos clave que surgen en países que pertenecen a diferentes culturas jurídicas y que poseen diversas circunstancias sociales y económicas. Y en segundo lugar, porque el propósito es subrayar problemas, detectar tendencias y tomar conciencia de los desafíos y de las transformaciones que se están produciendo en los procesos penales como consecuencia del incremento de los delitos cibernéticos y en general del uso de las TIC. De ahí que, para ello, una panorámica general que abarque varios países de particular relevancia resulta sin duda suficiente.

Como indica acertadamente uno de los informes nacionales[6], hablar de las TIC en el sistema de justicia penal equivale a hablar del sistema de justicia penal prácticamente en su totalidad, pues el uso e impacto de las TIC se hallan presentes, de algún modo, en cada acto y en cada fase de la prevención, investigación, instrucción, acusación y juicio penales. De hecho, las TIC no solo son relevantes en relación con el ciberdelito, sino que han adquirido progresiva importancia en el contexto de virtualmente todos los tipos de delito. Como se hace notar en el *UNODC Comprehensive Study on Cybercrime*, "la presencia creciente de la prueba electrónica en todos los tipos delictivos probablemente revolucionará las técnicas y actuaciones policiales". Más aún, J. Nijboer, en el Anexo al cuestionario que preparó para esta sección, escribía acertadamente que "casi todos los aspectos de la sociedad están influidos por TI e TIC"; y que "tanto el ámbito de lo privado como de lo público resultan afectados de tal manera que cada vez resulta más difícil distinguir entre ambos (…)". Así, el uso y la influencia de TIC en los sistemas de justicia penal es un tema que ha de ser estudiado por la doctrina jurídica a un nivel global, porque: 1) son esenciales para todos los procedimientos criminales; 2) evolucionan más rápidamente que las respuestas jurídicas que el legislador es capaz de proporcionar; 3) tienen un profundo impacto en la esfera de los derechos humanos.

No obstante, ha de hacerse notar que esta sección de la AIDP —y por tanto este informe general— se refiere a las TIC y el proceso penal. Podría parecer superfluo recordar esto, pero es esencial tener presente que nuestra principal atención se centra en el impacto de las TIC en los SJP, y no en el área de la seguridad y el espionaje. La línea divisoria entre ellos, sin embargo, no es del todo clara, y de hecho con frecuencia resulta bastante nebulosa[7]. Por esa razón, es necesario estudiar el trasvase de la información obtenida por razones de seguridad al proceso penal —y en otras cuestiones, la admisibilidad de esa información como prueba en el juicio. En todo caso, nuestro objetivo no es evaluar las políticas que algunos países han adoptado en materia de seguridad, el creciente papel del llamado *ciberimperialismo*, los diversos aspectos del desarrollo del *Estado vigilante*, o los

[4] Convenio de Budapest sobre la Ciberdelincuencia, del Consejo de Europa (23 noviembre 2001); Directiva de la UE 2000/31/CE sobre comercio electrónico; Decisión Marco de la UE 2005/222/JHA relativa a los ataques contra los sistemas de información; Directiva de la UE 2006/24/CE sobre conservación de datos; *The Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information* (2001); *The Arab Convention on Combating Information Technology Offences* (2010); *The Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2010); el documento sobre Establishment of Harmonized Policies for the ICT Market in the ACP Countries Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts,* elaborado por la *International Telecommunications Union* (ITU), la *Caribbean Telecommunications Union* (CTU) y la *Caribbean Community*; y el proyecto de *African Union Convention on the Establishment of a Legal Framework Conducive to Cyber security in Africa* (2012).

[5] Ese estudio se encuentra disponible en: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[6] Vid. el informe de Holanda, punto 1: "Introduction". En el mismo sentido, M. Simonato, en el rapport especial *Defence rights and the use of information technology in criminal procedure*, p.1. Este informe hace referencia a casi todos los apartados incluidos en este rapport general, pues la cuestión de los derechos de defensa es relevante en cada una de las fases del proceso y en relación con el uso de cada medida que implica la utilización de TIC; como señala el autor, las TIC, en general, han reforzado la posición de la acusación y, por tanto, la utilización de TIC constituye un reto adicional para la posición de la defensa a la luz del principio de igualdad de armas.

[7] Sobre este punto, en relación con la situación de Estados Unidos antes y después de los atentados del 11-S, vid. J. Vervaele, "Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal", en *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito,* Madrid, 2012, pp. 29-85, p. 39 ss.

límites éticos, de las conductas de algunas de las agencias de inteligencia en el mundo. En otras palabras, este rapport no trata de las actividades de la *National Security Agency* (NSA) en los Estados Unidos, de ciertas filtraciones o de la masiva intromisión en la privacidad de las de los ciudadanos llevada a cabo por algunos gobiernos mediante la utilización de sofisticadas tecnologías, justificando tal intromisión en amenazas a la seguridad nacional o internacional. Lo anterior no significa que esos métodos de obtener información no sean relevantes para nuestro estudio. Lo que deseo subrayar es que no se pretende aquí evaluar, analizar o criticar las actuaciones de los servicios de inteligencia en general, y cómo ejercen su poder (o abusan de él); el acento se pone en la investigación, persecución y enjuiciamiento a través del proceso penal. Así, por ejemplo, más que analizar los mecanismos que los gobiernos utilizan para escuchas —los cuales obviamente serán descritos y mencionados— nos interesa sobre todo examinar cómo la información obtenida de esa manera puede pasar al proceso penal, y explorar vías para impedir que tal información sea usada de manera incontrolada e ilegal para imponer sanciones penales a los ciudadanos.

Este informe general sigue la estructura del cuestionario enviado en su día a las secciones nacionales, que contenía 25 cuestiones divididas en cinco apartados:

(1) Cuestiones generales y definiciones.

(2) Elaboración de posiciones de información (*building information positions)* cuyo objetivo es determinar el uso que la policía y las fuerzas de seguridad hacen de las TIC para orden obtener información en un entorno de prevención o proactivo.

(3) La función y utilización de TIC en la investigación penal, que es quizás la parte central de este estudio —de ahí que haya terminado por ser también la parte más extensa en el borrador de propuesta de resolución.

(4) La función de las TIC y la prueba en el proceso penal. En este apartado, el cuestionario se refería a las diferentes fases probatorias: obtención, almacenamiento, conservación, presentación, admisión y evaluación de pruebas.

(5) El uso de las TIC en el juicio.

Hay leves yuxtaposiciones entre los apartados 3, 4 y 5. Por ello, decidí analizar en el apartado 3 las cuestiones relativas a obtención, conservación y almacenamiento o custodia de la prueba electrónica. La presentación y práctica de la prueba, así como el empleo de las TIC en el juicio se aborda en el apartado 5. El apartado 4 se centra en la admisibilidad y evaluación de la prueba. El cuestionario no incluía cuestiones relativas a la utilización de TIC en la fase posterior al juicio, de ahí que este tema no se trate en este rapport, a pesar de su indudable importancia práctica en la ejecución de sentencias y control de su cumplimiento.

Antes de entrar de lleno en el desarrollo del rapport, conviene anticipar algunas conclusiones preliminares que pueden inferirse del mismo:

1) Hace falta un marco jurídico efectivo que regule las medidas de investigación que implican el uso de las TIC, intentando encontrar un equilibrio adecuado entre los poderes de investigación y el respeto de los derechos humanos, especialmente el derecho a la privacidad. Muchas de las diligencias de investigación relacionadas con las TIC se llevan a cabo sobre la base de normas generales de entrada y registro domiciliario, lo cual no resulta apropiado y genera problemas prácticos.
2) Las TIC son ampliamente utilizadas en la elaboración de posiciones de información (building up information positions), así como para la instrucción penal. Sin embargo, muchos países no regulan las facultades que tienen las fuerzas de seguridad y policía en la fase de previa al comienzo del proceso penal, bien sea como prevención o de mantenimiento de la seguridad. Además, el trasvase de datos desde el área de la prevención al proceso penal debería estar regulada de alguna forma, y deberían ponerse en marcha mecanismos y controles que sirvan para evitar que esa información fluya de manera ilegal de una esfera a la otra.
3) Sería necesario elaborar normas y protocolos bien definidos en materia de almacenamiento y de garantías para la integridad de la prueba digital y electrónica. El imputado ha de tener en todo caso la oportunidad de comprobar la integridad de la prueba informática o digital.
4) El acceso a las bases de datos habría de estar sujeto a controles más estrictos, no solamente en la fase de investigación sino también en la de prevención. Sería preciso establecer instrumentos de control precisos que permitan determinar qué bases de datos se han utilizado, con qué finalidad y por quién.
5) Todo ciudadano cuya privacidad se haya visto violada debería ser informado de ello.

1. Cuestiones generales

Este apartado tiene por objeto proporcionar una visión general de las definiciones, términos e instituciones involucradas en el uso de TIC en los sistemas de justicia penal. Ciertamente, para el derecho penal sustantivo es importante aclarar qué se entiende por ciberdelito y cuáles son sus elementos, pero esa tarea es igualmente relevante para el proceso penal y, en general, para el sistema de justicia penal. En principio unificar conceptos y llegar a un acuerdo sobre ciertas definiciones, sin duda facilitaría el análisis comparativo y una comprensión común de esta realidad —por ejemplo, qué puede considerarse comunicación electrónica o datos personales

almacenados. Sin embargo desde otra perspectiva no resulta del todo claro si fijar definiciones sobre TIC y proceso penal es incluso conveniente, porque, como señala el rapport belga, algunas definiciones podrían tener un efecto negativo debido al rápido desarrollo de las tecnologías[8]. Conviene no perder de vista que lo que de verdad es esencial para analizar el impacto de las TIC en el sistema de justicia penal es conocer qué instrumentos se utilizan, qué función desempeñan en cada una de las fases del proceso penal al, y —esto es de vital importancia— en qué medida y bajo qué condiciones pueden admitirse como prueba los datos obtenidos o almacenados mediante TIC.

1. (1) ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del proceso penal (incluida la investigación y práctica forense)? ¿Cómo están reflejadas estas definiciones conceptuales en la doctrina científica, la legislación, las decisiones judiciales, y las prácticas pertinentes en el contexto del proceso penal?

Ninguno de los países estudiados define con precisión el significado de "sociedad de la información", ni proporciona tampoco definiciones concretas de las herramientas, técnicas, mecanismos o medidas de investigación relativas a las TIC dentro del proceso penal. En general, conceptos como redes electrónicas, sistemas informáticos, datos relativos al tráfico (*traffic-data*), o datos relativos al contenido (*content-data*), instrumentos forenses y periciales, etc., se toman del lenguaje general relativo a las TIC, de convenios internacionales o de la legislación penal sustantiva en materia de ciberdelito. Dentro de la UE, las definiciones de comunicaciones electrónicas, datos informáticos, redes cibernéticas, datos de tráfico, datos de contenido, proveedor de servicios, etc., se encuentran en las correspondientes directivas de la UE[9], y se toman también de convenios internacionales como el Convenio de Budapest sobre Ciberdelincuencia de 2001. La Directiva de la UE de 2002 sobre intimidad y comunicaciones electrónicas[10] define en su artículo 2 algunos conceptos importantes en materia de TIC. Aunque la Directiva hace notar expresamente que tales definiciones se incluyen a los efectos de la aplicación de la propia Directiva, bien pueden ser empleados también en el ámbito del proceso penal. Este es el texto del art. 2 de dicha Directiva:

Salvo disposición en contrario, serán de aplicación a efectos de la presente Directiva las definiciones que figuran en la Directiva 95/46/CE y en la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco).

Además, a efectos de la presente Directiva se entenderá por:

a) «usuario»: una persona física que utiliza con fines privados o comerciales un servicio de comunicaciones electrónicas disponible para el público, sin que necesariamente se haya abonado a dicho servicio;

b) «datos de tráfico»: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

c) «datos de localización»: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

d) «comunicación»: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;

---

[8] Rapport de Bélgica, cuestión B (1).

[9] Por ejemplo, la Directiva 2006/24/CE sobre conservación de datos, en su artículo 2.2, incluye definiciones para los siguientes conceptos:
a) «datos»: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario;
b) «usuario»: toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso publico, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio;
c) «servicio telefónico»: las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia);
d) «identificador de usuario»: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a Internet o a un servicio de comunicaciones por Internet, o de su registro en uno de dichos servicios;
e) «identificador de celda»: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil;
f) «llamada telefónica infructuosa»: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red.

[10] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 julio 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, DOUE L 201, p.37.

e) «llamada»: una conexión establecida por medio de un servicio telefónico disponible para el público que permita la comunicación bidireccional en tiempo real;

f) «consentimiento» de un usuario o abonado: el consentimiento del interesado, con arreglo a la definición de la Directiva 95/46/CE;

g) «servicio con valor añadido»: todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de trafico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación;

h) «correo electrónico»: todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que este acceda al mismo.

Es razonable pensar que las definiciones anteriores se utilizan también en el ámbito del derecho penal sustantivo de los países de la UE, pero no tenemos constancia de ello.

De modo excepcional, los códigos de procedimiento criminal de algunos países incluyen algunas definiciones parciales o definen algunos conceptos, incluidas aquellas normas que se refieren a, por ejemplo, los siguientes conceptos: sistemas informáticos (Bélgica), sistema de información (Turquía), procesamiento de datos informáticos (Austria, *Automationsunterstützte Datenverarbeitung*) o prueba electrónica y documento electrónico (Croacia[11], Colombia, si bien este último dentro del proceso civil). Bélgica también adopta una definición muy general y "neutral", que comprende el uso de cualquier clase de TIC: "todo sistema que permita el almacenamiento, proceso o transmisión de datos". Normalmente, la prueba electrónica se define como un material, elemento o información que existe en forma electrónica digital[12]. No obstante, una encuesta realizada en dieciséis países europeos revelaba que ninguno de ellos tenía una definición real de prueba digital[13].

Los Estados Unidos promulgaron muy pronto una legislación especial en materia de comunicaciones electrónicas, en concreto la *Electronic Communications Privacy Act* (ECPA) de 1986, que modificaba las normas preexistentes sobre escuchas telefónicas, el llamado Título III de la *Omnibus Crime Control and the Safe Streets Act* de 1968. Por ejemplo, se incluyeron definiciones de "comunicación electrónica" e "interceptación" en el ordenamiento jurídico norteamericano. Según el informe nacional USA, la comunicación electrónica incluye "cualquier transmisión de signos, señales, escritos, imágenes, sonidos, datos o datos de inteligencia de toda clase, que sean transmitidos, en todo o en parte, por cable, radio, o por sistemas electromagnéticos, foto-electrónicos o foto-ópticos". Por su parte, la interceptación comprende "la interceptación que se produce al mismo tiempo que la transmisión de comunicaciones"; pero no, en cambio, el acceso a correos electrónicos almacenados que han sido enviados a un proveedor de servicios pero que aún no han sido leídos, o la grabación de un mensaje instantáneo. Las definiciones anteriores, aunque pueden clarificar el ámbito de aplicación de la ley, han causado problemas de interpretación, por ejemplo, en relación con la interceptación de correos electrónicos: técnicamente, un correo electrónico solo puede "interceptarse", en su calidad de comunicación, durante los segundos o milésimas de segundo antes de que el correo remitido haya sido almacenado en una ubicación temporal. Esto planteaba la cuestión de si la "interceptación" de correos electrónicos debería ser autorizada solamente de acuerdo con las normas que regulan el acceso a datos almacenados (*search of data*), o si más bien aquellos datos de correo guardados podían considerarse "en transmisión" hasta que fueran recuperados por el destinatario, en cuyo caso habrían de aplicarse las normas sobre "interceptación de comunicaciones". Como veremos, problemas análogos surgen en otros ordenamientos jurídicos, especialmente porque los conceptos tradicionales creados para la comunicación o para los registros no se han adaptado adecuadamente a la nueva realidad de las TIC y al uso masivo de comunicaciones electrónicas.

En general, el proceso penal contiene por regla sólo normas dispersas sobre diferentes aspectos de las TIC. En particular cuando se regulan específicamente las TIC, es en relación a ciertas medidas investigativas que implican el uso de las TIC, señalando cuáles son los requisitos para su uso con fines de investigación penal. Deberíamos preguntarnos si las definiciones de conceptos relacionados con TIC son en el contexto del proceso criminal tan necesarias como en el derecho penal sustantivo[14]. Y quizás no lo sean. Pero sin duda, debido al papel creciente desempeñado por las TIC y los nuevos datos que pueden obtenerse mediante las mismas —por ejemplo, aparatos de geo-localización, buscadores de internet, reconocimiento automático de matrículas, chips

[11] Art. 202, para. 32 CPC: "evidencia electrónica (digital) se refiere a datos que fueron obtenidos como evidencia en forma electrónica (digital)". Sin embargo, el Código establece también que la evidencia electrónica no es un tipo de evidencia, sino un "medio mediante el que se conserva la evidencia" (art. 331 CPC). Vid. el rapport de Croacia, p.2.

[12] UNODC *Comprehensive Study on Cybercrime*, p. 157.

[13] Vid. F. Insa (2007), The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study, Journal of Digital Forensic Practice, 1:4, 285-289, cit. también por M. Simonato, p. 11.

[14] Vid. Recomendación del Comité de Ministros del Consejo de Europa No. R (89) 9 *on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes*; y la Convención sobre Ciberdelincuencia del Consejo de Europa, de 23 noviembre 2001.

añadidos a mercancías, tecnología de imágenes térmicas, cámaras de vigilancia, y toda clase de software—la investigación de los delitos claramente ha experimentado una transformación radical. Ello plantea nuevos desafíos a las normas existentes que regulan las medidas de investigación tradicionales y las reglas sobre prueba sin contemplar las particularidades de la prueba electrónica.

Una cierta armonización del significado, ámbito y requisitos de las medidas de investigación relativas a las TIC sería altamente deseable. Lo mismo puede decirse de términos como: datos de suscriptor, meta-datos o datos externos, datos de contenido y datos de tráfico; y sería muy útil ponerse de acuerdo acerca de cuáles de esos datos deben considerarse como "datos en tránsito" y datos almacenados o "en reposo" (*data at rest*)[15], pues la definición de tales conceptos determinará en muchos casos cuál es la medida investigativa adecuada y cuál es la normativa aplicable. Esto resulta especialmente necesario para los estudios comparatísticos, así como para la cooperación internacional en materia de criminalidad —sin duda, el uso de los mismos términos para los mismos actos de investigación relativos a TIC, y un acuerdo sobre el significado de la prueba electrónica, facilitarían la cooperación internacional y la admisibilidad de las pruebas obtenidas en el extranjero.

Si se subraya aquí la importancia de las definiciones y de la armonización en las investigaciones criminales transnacionales, es porque el empleo de las TIC ha ejercido como factor multiplicador de la criminalidad transnacional y, por tanto, reclama una rápida ejecución de las solicitudes de cooperación judicial. Además, el propio funcionamiento de los sistemas de almacenamiento en la "nube", generan que aunque un delito se cometa en el territorio de un solo Estado, los datos de comunicaciones electrónicas necesarios para su esclarecimiento podrían estar guardados en servidores situados en el extranjero,[16] planteando así nuevos retos para la obtención de pruebas en el extranjero, con implicaciones en materia de poderes extraterritoriales y para el respeto de la soberanía. Finalmente, para comprender correctamente la relación entre las TIC y el proceso penal es esencial señalar que su utilización e importancia se extiende mucho más allá del contexto del ciberdelito o de los procesos e investigaciones relacionados con la informática.

1. (2) ¿Existen instituciones específicas y /o grupos de trabajo o equipos operativos involucrados en la aplicación de las TIC en el sistema de justicia penal?

La expansión del uso de sofisticadas TIC en la comisión de delitos representa un continuo desafío para las autoridades policiales y judiciales involucradas en la lucha contra la delincuencia, las cuales necesitan mantenerse al día en todas las innovaciones tecnológicas, no sólo para detectar nuevas formas delictivas, sino también para estar en condiciones de obtener las pruebas necesarias para la acusación. Dentro del entorno del Consejo de Europa, la Recomendación No. R (95) 13[17] ya hacía hincapié en que "debería contemplarse el establecimiento de unidades especializadas para la investigación de delitos que, para ser combatidos, requieren una especial pericia en tecnología de la información".

Las respuestas que los cuestionarios dan a esta pregunta tienden a subrayar, por una parte, las instituciones que son responsables, en general, de la informatización del proceso, la automatización del sistema de justicia y el equipamiento técnico de los tribunales, funciones que normalmente caen bajo la competencia del Ministerio de Justicia (por ejemplo, en Austria, Bélgica, Brasil, Croacia, España, Turquía); y por otra parte, aluden a las unidades especializadas, dentro de las fuerzas policiales o de seguridad, que se ocupan del ciberdelito, de las herramientas de investigación y análisis informáticos (*computer forensics*) y de las actuaciones de vigilancia en o a través de internet.

Según los rapports, todos los países poseen unidades especiales para perseguir el ciberdelito y sistemas informáticos para combatir la criminalidad. Estas *cyber-forces* que son unidades con una alta especialización tecnológica, se ubican frecuentemente en las estructuras de la policía, en las unidades de inteligencia policiales (así por ejemplo Argentina, China, o España, donde la Guardia Civil cuenta con el Grupo para Delitos Telemáticos y la Policía Nacional con la Brigada de Investigación Tecnológica) y también en el ámbito de la fiscalía (entre otros, Finlandia, Holanda y Suecia tienen una fiscalía especializada). Los servicios de inteligencia también tienen unidades de esa clase, aunque no todos los informes proporcionan información al respecto, ya que el cuestionario solamente hacía referencia a los órganos dentro del sistema de justicia penal y no en el sistema de seguridad del Estado. Esto parece indicativo de que la frontera entre la inteligencia y la investigación criminal, en la práctica, no es nítida en muchos ordenamientos.

---

[15] En este sentido se manifiesta también U. Sieber, "Mastering complexity in the global cyberspace: the harmonization of computer related criminal law" en M. Delmas-Marty, M. Pieth y U. Sieber (eds.), *Harmonising Criminal Law*, Paris, 2008.

[16] Vid. el Discussion Paper del CoE *Law Enforcement Challenges in Trans-border Acquisition of Electronic Evidence from Cloud Computing Providers* (2010), disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf.

[17] Recomendación del Comité de Ministros No. R (95) 13, *Concerning problems of criminal procedural law connected with the information technology*, adoptada el 11 septiembre 1995.

Un alto número de países tienen varias unidades especializadas: una en cada una de las instituciones involucradas en el sistema de justicia penal. A veces hay también otra unidad centralizada que coordina las diferentes unidades o cuerpos policiales (por ejemplo, Bélgica, España, Holanda, Japón, Turquía o Estados Unidos). El rapport de Estados Unidos informa que en ese país existen fuerzas específicas (*task forces*), al menos para las fuerzas policiales, relacionadas con la implementación de las TIC en el sistema de justicia criminal: el *Internet Crime Complaint Center*, que es un centro de coordinación para la investigación de delitos en internet; la *Cyber Initiative and Resource Fusion Unit*, que analiza las tendencias en materia de delitos en internet, y filtra también falsas pistas antes de que la información sobre ciberdelitos llegue a la fiscalía (es interesante el apoyo que esta unidad recibe de diversas compañías privadas, como Microsoft o eBay, por ejemplo); el *U.S. Computer Emergency Readiness Team*, que no lleva a cabo investigaciones, pero da apoyo, coordina y ejecuta proyectos de investigación; y finalmente *Infragard*, que es parte del Departamento de Seguridad Interior (*Department of Home Security*), y en el que entes públicos y privados comparten información, promoviendo el diálogo entre la comunidad de TIC y las autoridades policiales y de seguridad.

De esa manera, en el plano de la investigación penal, todos los países estudiados parecen haber respondido a las necesidades derivadas del delito informático mediante la creación de unidades especializadas. No es sorprendente que las unidades especiales para la investigación de ciberdelitos sean también las encargadas de proporcionar apoyo a otros unidades en el uso de las TIC y en la evaluación forense de la prueba electrónica en algunos países (p. ej., Austria, Croacia, España). Si tales unidades están adecuadamente equipadas y tienen suficientes recursos humanos y técnicos, es una cuestión que no es abordada en el presente estudio. El informe de UNODC muestra que el nivel de especialización es muy diverso, y que en muchos países en vías de desarrollo el grado de entrenamiento y capacitación de las unidades especializadas en TIC y ciberdelito necesita mejorarse mucho[18]. En Estados Unidos, si se atiende al desarrollo del marco legal, así como a la bibliografía y a la información publicada en los medios de comunicación, parece evidente, que hay una experiencia amplia en el uso de las TIC, no sólo en el ámbito de la investigación criminal, sino también en lo relativo a la seguridad nacional y prevención del terrorismo.

Las respuestas que se dan en este estudio difieren de otros estudios que abarcan también países africanos, en los cuales se indica que esos países muestran en general una carencia de unidades suficientemente especializadas, y que algunos países sólo tienen algunas personas expertas dentro de los departamentos de policía[19].

La Unión Europea[20], desde hace mucho, ha contemplado el desarrollo y utilización de las TIC en el ámbito penal como una prioridad, y así lo pone de manifiesto, por ejemplo, el Sistema de Información de Schengen (SIS), una base de datos creada para los procedimientos penales. Los datos personales —que pueden incluir nombres, características físicas, lugar de nacimiento, nacionalidad, si la persona es o no peligrosa, etc., — pueden utilizarse solamente para la finalidad de las alertas que se fijaron cuando los datos se introdujeron. Este sistema de información se complementa con la red SIENA (*Secure Information Exchange Network Application*), empleada sobre todo por los Estados miembros de la UE para intercambiar información bajo la Decisión Marco 2006/960/JHA, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[21]. Las agencias creadas en la UE para la cooperación penal policial y judicial son, respectivamente, Europol y Eurojust. Europol es el organismo policial europeo centrado principalmente en el intercambio de información y en el análisis de inteligencia en relación con delitos graves transfronterizos. Proporciona apoyo analítico a las autoridades de los Estados miembros y les asiste en sus investigaciones penales. Como indica de Busser en su rapport especial, "el *Europol Information System* (EIS) es, junto con el sistema de *Analysis Work Files* y SIENA, el instrumento más importante cuando se trata de intercambio de información por Europol"[22]. Eurojust es la institución de la UE para la cooperación judicial y para el apoyo a las investigaciones penales transfronterizas de los Estados miembros; posee un sistema de gestión de casos específico, que funciona dentro de la red segura de la Comisión s-TESTA. A nivel de la UE, vale la pena mencionar también la *European Judicial Network*[23], que se ocupa de las comunicaciones seguras de las autoridades judiciales; el portal europeo *e-justice*, donde se encuentran documentos digitalizados relevantes para

[18] UNODC *Comprehensive Study on Cybercrime*, pp. 152-156.
[19] UNODC *Comprehensive Study on Cybercrime*, pp. 152-153.
[20] En relación con el uso de las TIC y de los mecanismos de protección de datos a nivel de UE, me remito a los completos y pormenorizados rapports especiales de E. De Busser y D. Brodowski, *European Initiatives Concerning the Use of IT in Criminal Procedure and Data Protection*, que responden al entero cuestionario en el nivel supranacional de la Unión Europea. De ahí que las referencias al uso de TIC en la UE se reduzcan a un mínimo en este informe general.
[21] DOUE L. 386, 29 diciembre 2006.
[22] Para ulteriores detalles sobre el funcionamiento de estos instrumentos y redes, vid. el rapport de E. De Busser, p. 12, y la bibliografía allí citada.
[23] Decisión del Consejo 2008/976/JHA, de 16 diciembre 2008, sobre la Red Judicial Europea, O.J.L. 348 of 23 diciembre 2008, p. 130.

la justicia penal (como por ejemplo, legislación, autoridades competentes, etc.)[24]; y el ECRIS (*European Criminal Records System*), un sistema descentralizado que provee de una estructura de comunicación para peticiones de antecedentes y archivos penales mediante formularios estandarizados[25].

Establecer centros especiales para la investigación y la formación y capacitación en el uso de las TIC resulta, según revelan los informes, de gran utilidad. El rapport belga menciona el Centro de Excelencia sobre Ciberdelincuencia, para la formación, educación e investigación en el sector público, centro en el cual trabajan juntos las compañías privadas de TIC, con la policía, la fiscalía y la judicatura.

Finalmente, parece también que se ha logrado un cierto grado de especialización tanto a nivel policial como de investigación y desarrollo tecnológico, que se refleja en la detección e instrucción de delitos, mientras que, según revelan los informes, tal especialización en el ámbito judicial la especialización aún es muy desigual y en muchas ocasiones deja aún mucho que desear[26].

1. (*3) ¿Existen entidades o empresas privadas/comerciales que prestan servicios relacionados con las TIC en el ámbito del sistema de justicia penal?*

Entre los servicios que los proveedores de TIC ofrecen al sistema de justicia penal podemos distinguir entre, por una parte, el equipamiento técnico e informático (*hardware* y *software*) para la gestión del trabajo administrativo y procesal de los tribunales; y, por otra parte, aquellos servicios relativos consistentes en la elaboración de informes periciales o en la obtención y análisis de datos, proporcionados en diferentes fases del procedimiento en relación con la compilación, manipulación y evaluación de la prueba electrónica.

Por lo que concierne al primer aspecto, la mayoría de los países no tiene reglas específicas sobre el equipamiento informático y gestión informatizada de la administración de justicia, pero se aplican las normas generales de gestión de la administración pública. Habitualmente existe un organismo público que se encarga de la automatización de la gestión y de los procedimientos, y ese organismo contrata con las empresas privadas mediante concurso público (por ejemplo, Bélgica, España, Italia).

Por lo que se refiere a la segunda forma de cooperación entre empresas de TIC y la justicia penal en las diversas fases del proceso, de acuerdo con los rapports, esas relaciones de cooperación son de alcance muy diverso. En algunos países no hay normas legales sobre la contratación de empresas privadas para proporcionar servicios o análisis periciales (*forensics*) a la policía, la fiscalía o las autoridades judiciales (Argentina, Brasil, Colombia, Finlandia); lo cual significa que la contratación de tales servicios no está prevista legalmente, pero tampoco está prohibida. España se remite fundamentalmente a las pericias elaboradas por las unidades públicas forenses especializadas, que son a menudo parte de la estructura policial, pero las partes del proceso penal pueden también contratar expertos privados. En Austria, las compañías privadas actúan solamente como peritos o expertos en el proceso. En Bélgica, el perito judicial es designado por el juez en uso de sus facultades discrecionales, y puede ser una persona individual o una empresa. En algunos otros países, a pesar de la falta de regulación, hay acuerdos de cooperación concretos entre empresas privadas y los actores del SJP (Holanda, Japón). El informe de Croacia explica que hay empresas que proveen de *computer forensics*, colaboran en la recuperación de datos, y proveen asesoramiento en materia de seguridad de las TI. Muchas grandes empresas de consultoría tienen un departamento de *forensics* que da servicios especializados de TIC en materia de prueba electrónica, sobre todo a petición de la defensa.

La UE funciona sobre la base de sus propios expertos y proveedores de servicios y, de ordinario, evita la contratación con proveedores de servicios privados, si bien puede haber interacción con estos últimos en la realización de informes periciales relativos a la integridad y fiabilidad de la prueba electrónica.

En suma, parece que, por lo que concierne a la elaboración de informes periciales o *ICT forensics*, son dos los modelos más comunes de cooperación que existen entre las empresas privadas de TIC y los sistemas de justicia penal: uno se apoya en gran medida en empresas privadas para la investigación penal relacionada con las TIC, contratando expertos de empresas privadas o bien peritos individuales; y otro se nutre principalmente de los expertos integrados en organismos públicos, involucrando en menor medida a individuos o empresas privadas.

Por lo que se refiere a otras formas de cooperación, la Directiva de la UE sobre conservación de datos[27] establece que las compañías privadas de telecomunicaciones y los proveedores de internet están obligados a cooperar en la conservación de datos y en la vigilancia de las comunicaciones, con arreglo a los requisitos legales sobre protección de datos y derecho a la intimidad.

[24] Vid. mas detalles en el rapport de D. Brodowski, pp. 7-8.
[25] Vid. E. De Busser, p. 17.
[26] Esta apreciación es también confirmada por el UNODC *Comprehensive Study on Cybercrime*, pp. 172-177.
[27] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 marzo 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DOUE L. 105, de 13.4.2006, p. 54.

Todos los países analizados tienen normas que imponen a las compañías privadas que proveen servicios TIC el deber de cooperar en la investigación criminal, con diferentes obligaciones relativas a los datos que han de almacenar. Además de la cooperación formal, hay otros grados y vías de cooperación informal, que pueden ser muy efectivos para la prevención e investigación de delitos, pero que implican serios riesgos para la seguridad jurídica, el Estado de derecho y la tutela del derecho fundamental de los ciudadanos a su intimidad.

Todos los rapports nacionales afirman que los proveedores de servicios de internet y las compañías de telecomunicación están obligados a cooperar proporcionando datos que sean necesarios para fines de investigación o probatorios. Como se verá más adelante —esta es cuestión que se examina en el apartado (3)(3) de este informe general— en la mayoría de los casos los proveedores de servicios tienen la obligación de entregar datos solamente en cumplimiento de un requerimiento formal, normalmente proveniente de una autoridad judicial. Aunque en la práctica se dan relaciones de cooperación informal, la obligación de las empresas de suministrar datos sólo nace de requerimientos conformes con las garantías del debido proceso. Esto se aplica a todos los Estados miembros de la UE, pues el art. 4 de la Directiva de 2006 sobre conservación de datos expresamente indica cuáles son los requisitos formales que han de cumplirse para que los proveedores de servicios estén obligados a entregar los datos que se les reclaman[28].

La cooperación con entidades o empresas privadas está sujeta a diversos límites jurídicos, financieros y prácticos. En general, son aplicables las normas sobre contratación pública, aunque no siempre sucede así, como por ejemplo en la designación de expertos. En los informes nacionales no aparecen detalladas las obligaciones o las limitaciones en la designación de peritos privados, si bien parece deducirse que normalmente los expertos tienen el deber legal de cooperar cuando son requeridos para ello por una autoridad judicial. En el ejercicio de sus funciones además quedan obligados a la confidencialidad. En cuanto a los servicios suministrados por proveedores de servicios, parece que su obligación de cooperación está sujeta a previa orden judicial y que, a falta de la misma, la cooperación de las empresas se encuentra limitada por las normas sobre protección de datos. Algunos rapports hacen notar que hay también acuerdos de cooperación para compartir información general sobre delitos relacionados con TIC, avances tecnológicos, tipos de registros y búsquedas, instrumentos y herramientas eficaces, desarrollo de investigación sobre software, etc. Como ya se señaló antes en la sección (1)(2), en varios países existen institutos o asociaciones donde se reúnen expertos del mundo de las telecomunicaciones e intercambian conocimientos, discuten medidas prácticas, y comparten información sobre cuestiones técnicas —así como sobre riesgos y amenazas— con académicos y con las fuerzas policiales y de seguridad (p. ej., Bélgica y Estados Unidos). Dichas experiencias parecen haber producido resultados positivos para todas las partes involucradas[29].

2. Información e inteligencia: elaboración de posiciones de información (*information positions*) con fines preventivos y de seguridad

La elaboración de "posiciones de información" es parte de la denominada actuación basada en informaciones de inteligencia (*intelligence-led-policing*, ILP). *Intelligence-led-policing* es un término que no tiene una traducción exacta en castellano. Hace referencia a un proceso de organización y análisis de información que permite a las fuerzas de policía y seguridad de un estado tomar decisiones y diseñar estrategias para definir sus actuaciones, tanto preventivas como represivas, en cuestiones que afectan a la seguridad de un estado, y en particular en relación con delitos graves, como por ejemplo terrorismo o fenómenos de criminalidad transnacional organizada (TOC)[30]. La información se recoge y se analiza con el objetivo precisamente de establece una estrategia policial en material penal (*management or criminal policy*), una táctica, un plan de acción o un concreto operativo (misiones, controles, investigaciones). En el ámbito de la UE, el Programa de la Haya de 2005[31] ya advierte de la necesidad de reforzar el enfoque pro-activo de las autoridades de policía, con el fin de elaborar un concepto estratégico de política criminal que pueda hacer frente a las amenazas de la delincuencia grave de manera más efectiva.

---

[28] "Artículo 4: Acceso a los datos.— Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva sola- mente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. Cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos."

[29] En el mismo sentido, también el UNODC *Comprehensive Study on Cybercrime*, p. 151.

[30] Vid. UNODC *Handbook on the Crime Prevention Guidelines: Making them Work*, 2010, accesible en http://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/10-52410_Guidelines_eBook.pdf; y art. 28 de la *UN Convention against Transnational Organized Crime*, firmado en Palermo en 2000.

[31] *Communication from the Commission to the Council and the European Parliament de 10 de mayo de 2005 – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice* COM(2005) 184 final, O.J.C 236 of 24.9.2005.

El término *information position* tampoco tiene una acepción equivalente en español, por lo que he optado por o utilizar el término en inglés o bien traducirlo literalmente. Soy consciente de que la traducción literal resulta en un concepto que no es utilizado en el ámbito de la investigación policial o penal. En otras palabras, poco o nada dice la expresión "posición de información" a los hispano-parlantes. No obstante, he optado por utilizar el concepto "posición de información" aquí, primero porque no encuentro otro más adecuado que lo defina de manera equivalente; en segundo lugar para evitar confusiones y en tercer lugar, porque considero que es el término que, por ser el más descriptivo, tenderá a imponerse en un futuro. Pero ello requiere, empezar por explicar en qué consiste una "posición de información" (*information position*) hace referencia al "resultado de localizar, compilar, conectar y procesar una masiva cantidad de datos, que se encuentran almacenados para fines específicos en diversas bases de datos"[32] y que también se conoce como "Big data". La elaboración de una "posición de información", puede considerarse equivalente al concepto de "inteligencia" o información de inteligencia, si bien el concepto de inteligencia tiene diversos sentidos. Uno de esos significados, según las *Analytical Guidelines of Europol* de 2000 es: "información procesada", el producto del ciclo de inteligencia que implica la obtención, selección y evaluación de información[33]. Una definición similar la encontramos en las *Law Enforcement Analytical Standards* elaboradas por el Departamento de Justicia de los Estados Unidos[34], si bien en este documento se distingue entre "inteligencia" e "inteligencia táctica". Conforme a estas definiciones no resulta fácil entre "elaboración de posiciones de información" y "actividad de inteligencia", pues ambas aluden a la recolección, procesamiento y análisis de datos. No obstante, el concepto de "inteligencia" tradicionalmente suele asociarse a los servicios secretos y a la seguridad exterior, lo cual puede explicar que en el ámbito europeo se haya optado en muchos países por utilizar la expresión de "elaborar posiciones de información", para evitar confusiones. Con ello se diferencia claramente entre las actividades de inteligencia llevadas a cabo en el marco de la seguridad nacional, las cuales pueden utilizar medidas más intrusivas y normalmente están sometidas a controles menos rígidos, y por otro lado, la información recabada por unidades policiales para mejorar la actuación preventiva en la lucha contra delincuencia grave, es decir hacer frente a la amenaza sin necesidad de que esa actuación esté conectada directamente a un delito ya cometido. En este último ámbito no suele permitirse el uso de medidas coercitivas, como por ejemplo, intervención de comunicaciones. Así se exige también en la Resolución "Medidas Procesales Especiales y Respeto de los Derechos Humanos", adoptada en el XVIII Congreso Internacional de la AIDP, celebrado en Estambul en septiembre de 2009, se dice: "*The collection of digital information for law enforcement purposes should be regulated by criminal procedure.*"[35].

Estas diferencias conceptuales no siempre están debidamente precisadas ni a nivel legal ni tampoco en la literatura científica. Por ello es explicable que muchos informes nacionales hayan respondido a las cuestiones referentes a "elaboración de posiciones de información", incluyendo también la actividad de las unidades de inteligencia o servicios secretos dedicados a la seguridad nacional.

Los cambios conceptuales en el derecho penal sustantivo han originado también cambios en la esfera procesal. El proceso penal, que tradicionalmente estaba concebido como un cauce de respuesta ante el delito ya cometido, pasa a superar esta esfera reactiva para convertirse en un mecanismo pro-activo en la lucha contra la delincuencia. Ello tiene como consecuencia que tienda a difuminarse la línea divisoria entre la actividad de las unidades de inteligencia y las actuaciones de los órganos de investigación penal[36]. En la medida en que la separación entre prevención y represión del delito va desdibujándose, o al menos ya no puede diferenciarse de manera nítida, en la esfera pro-activa se comienzan a utilizar técnicas de obtención y análisis de información, con el fin de identificar no solo nuevas tendencias y riesgos en general, sino también la estructura y características de grupos de criminales, así como sus objetivos y posibles actos preparatorios de delitos. A ello se añade el hecho

[32] Vid. E. De Busser, p. 8.

[33] Vid. G.Rauchs y D.J. Koenig, "Europol", en *International Police Cooperation. A World Perspective* ed. por D.J. Koenig y D. K. Das), Maryland 2001, pp. 43 ss.

[34] Intelligence: Information + Evaluation. The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities. Intelligence is information analysed to determine its meaning and relevance. Information is compiled, analysed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. Tactical Intelligence: Information regarding a specific criminal event of immediate use by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety. Disponible en: http://www.ialeia.org/files/docs/law%20enforcement%20analytic%20standards.pdf

[35] Punto 14 de la Resolución, que continúa diciendo: "En los casos en que la información afecte al derecho de privacidad, esa obtención habrá de ser autorizada por decisión judicial. Para ordenar la entrega de esos datos a los proveedores de servicios de telecomunicaciones, se exigirá una justificación más específica que la general de que tales datos son relevantes para la investigación". Vid. *XVIIIth International Congress of Penal Law* (Istanbul, Turkey, septiembre 2009), Istanbul 2009, p. 172.

[36] Vid. las muy ilustrativas conclusiones de J. Vervaele, "Special procedural measures and the protection of human rights", General Report for the *XVIIIth International Congress of Penal Law,* Istanbul 2009, pp. 138 ss., en el cual no sólo se destacan los cambios producidos en las actuaciones de inteligencia y de la investigación penal, sino que además ofrece una interesante visión de esas transformaciones desde una perspectiva comparatista. Al respecto vid. también L. Bachmaier, Información de Inteligencia y proceso penal, in Terrorismo, proceso penal y derechos fundamentales, pp. 56 ss., y la bibliografía allí citada.

de que diversos delitos también entran dentro de la consideración de amenazas a la seguridad nacional, por lo que las unidades de los servicios secretos ven ampliado su como de actuación, más allá de las funciones que tradicionalmente tenían encomendadas. El principio, consolidado desde hace tiempo, de la separación entre funciones de inteligencia y funciones de persecución penal (*Trennungsgebot*), empieza a ser cuestionado y sustituido por un modelo basado en la cooperación, conforme al cual las unidades policiales elaborarán inteligencia y las unidades de inteligencia actuarán en la lucha contra actividades delictivas[37]. La lucha contra formas complejas de criminalidad organizada transnacional ha llevado a tener que analizar una cantidad de datos masiva, que requiere emplear software especial para el rastreo y obtención de esos datos, pero sin poder prescindir de su selección y análisis por personal cualificado para poder sacar conclusiones acerca de objetivos y riesgos relevantes tanto para la seguridad nacional como para el sistema penal.

2. (1) ¿Qué técnicas relacionadas con las TIC se utilizan para elaborar posiciones de información (information positions) por las fuerzas policiales y de seguridad?

Antes de analizar las respuestas a esta pregunta, ha de señalarse que en la mayoría de los informes no se diferencia entre información obtenida con fines de diseñar una estrategia policial penal y, por otro lado, la información relativa a amenazas contra la seguridad nacional. Como ya se ha señalado antes, hasta cierto punto esto no es sorprendente, pues en muchos ordenamientos jurídicos el concepto de "elaboración de posiciones de información" sigue siendo desconocido, y solo recientemente la actuación de la policía y otras fuerzas de seguridad en la esfera preventiva (o realizando indagaciones exploratorias, como se lee en el informe holandés) ha atraído la atención de la doctrina judicial. Si bien es cada día más relevante la actuación pro-activa de la policía, dirigida a identificar riesgos más que a recabar vestigios de un delito cometido, los códigos procesales tradicionalmente no han prestado atención a estas actuaciones, considerándolas algo ajeno al proceso penal.

Por otro lado, no es inusual que en las leyes que regulan las funciones y actuaciones de las fuerzas policiales no se contengan normas específicas sobre las medidas a adoptar con el fin de identificar riesgos y diseñar conceptos estratégicos de prevención. En la medida en que la protección de la privacidad y otros derechos fundamentales se contempla desde la esfera de las medidas de investigación penal y en referencia a un proceso penal, y no desde la perspectiva de las actividades de inteligencia y prevención, los requisitos para realizar esas intromisiones en la esfera de derechos humanos no aparecen debidamente regulados.

De los informes nacionales parece deducirse que la mayoría de los estados utilizan todo tipo de TIC con fines preventivos, de planificación estratégica y de seguridad nacional: observación e interceptación de comunicaciones, rastreo de datos financieros, instrumentos de geo-localización, reconocimiento automático de matrículas de vehículos, aparatos de escuchas, cámaras de vigilancia tanto visibles como ocultas, rastreo de datos informáticos, software para *data-matching*, tecnología de exposición térmica, receptores o *beepers* y otros instrumentos de seguimiento y vigilancia. El informe de China se refiere con carácter general a "otros instrumentos de vigilancia secreta", mientras que el informe USA enumera de manera muy detallada las diversas técnicas e instrumentos que se utilizan en ese país para llevar a cabo una amplia vigilancia de las comunicaciones y movimientos, así como para facilitar el acceso a diferentes bases de datos. También menciona los drones, que se utilizan con frecuencia para controlar los movimientos en la frontera norteamericana, y con ello diseñar estrategias y operativos en ese ámbito. La utilización de drones ha generado una amplia polémica, llevando al Congreso de los Estados Unidos a adoptar una ley en febrero de 2013, en la que se prohíbe su uso, sin previa autorización judicial, con el fin de vigilar a individuos concretos o propiedades concretas.

Parece que en el ámbito de las actividades de inteligencia —no queda claro si en un sentido amplio o en un sentido estricto— los estados recurren a todo tipo de medios tecnológicos, y que su utilización más o menos intensa depende de los recursos económicos disponibles así como de la valoración del riesgo existente. La manera en que se utilizan en la práctica estos instrumentos es en gran parte desconocida, y en todo caso esa cuestión queda fuera del ámbito de este informe general. En cuanto a las condiciones y los requisitos para hacer uso de todas esas técnicas de TIC, no podemos ofrecer una respuesta clara, pues la mayoría de los informes nacionales, al responder al cuestionario, no diferencian entre servicios de inteligencia que operan en el ámbito de la seguridad nacional y unidades de inteligencia policiales que recaban información con el fin de elaborar políticas y estrategias preventivas y/o de seguridad, esto es, para la elaboración de posiciones de información.

El ordenamiento jurídico de los USA cuenta con una amplia regulación acerca de las actuaciones de vigilancia que puede llevar a cabo el estado con fines de seguridad nacional; pero, al igual que ocurre en la mayoría de los países, no queda bien delimitado si los datos obtenidos como consecuencia de la actividad de los servicios de inteligencia pueden ser utilizados como prueba dentro de un proceso penal por delitos. El FBI (*Federal Bureau of Investigation*) y la CIA (*Central Intelligence Agency*) llevan desde los años 40 colaborando en operaciones de inteligencia interior. La *Foreign Intelligence Surveillance Act* (FISA) de 1978, aunque reformada en varias ocasiones desde entonces, regula la vigilancia de agentes extranjeros, ciudadanos extranjeros y amenazas

[37] Para Alemania vid., por ejemplo, A. Abbühl, *Der Aufgabenwandel des Bundeskriminalamtes*, Stuttgart 2010, pp. 353 ss.

extranjeras[38], estableciendo diversos requisitos y diferente nivel de garantías, dependiendo de si la persona vigilada es un ciudadano norteamericano o no, aplicando en este último caso un nivel de garantías inferior.

En este contexto, merece la pena mencionar el informe belga, pues es uno de los pocos en el cual se traza una clara distinción entre las actividades de los servicios secretos de inteligencia y las actuaciones que llevan a cabo otras unidades policiales o de seguridad, con el fin de elaborar posiciones de información. Este informe señala que en el ámbito policial preventivo y de elaboración de posiciones de información, pueden utilizarse tres tipos de técnicas relacionadas con las TIC: acceso a bases de datos, sistemas de vigilancia, y estadísticas. Nos centramos ahora en este último punto, la vigilancia de sistemas y las estadísticas, pues el acceso a bases de datos y el procesamiento de los datos, es objeto de una pregunta específica, y por tanto se aborda separadamente más adelante.

Dentro de la finalidad de elaborar posiciones de información, el ordenamiento belga permite dos tipos de sistemas de vigilancia electrónica: la video vigilancia en espacios públicos y la utilización de imágenes obtenidas mediante satélites. La video vigilancia mediante cámaras fijas en espacios públicos debe estar debidamente señalizada en cada uno de esos lugares y no puede estar dirigida a grabar imágenes de carácter íntimo. Si esas imágenes tuvieran interés desde la perspectiva penal, la policía deberá ponerlo en conocimiento de las autoridades judiciales. Por lo que se refiere a las cámaras móviles, pueden utilizarse para eventos especiales y para el tiempo que duren esos eventos, con el fin de detectar posibles alteraciones del orden público o riesgos concretos para la seguridad, siempre que la autoridad municipal gubernativa correspondiente preste autorización.

La utilización de las denominadas "cámaras inteligentes" (*intelligent cameras*) sigue siendo objeto de controversia: no existe una regulación concreta sobre los requisitos y condiciones para su utilización, por lo que en la práctica se aplican las normas relativas a la vídeo vigilancia. Esto puede llegar a infringir el derecho a la privacidad, pues mediante esas cámaras pueden obtenerse datos sometidos a especial protección, como datos de carácter político, religioso, étnico o sexual de la persona sometida a esa medida de vigilancia, ya que la "cámara inteligente" capta todos los movimientos de una persona o un vehículo.

Por último, el informe belga hace referencia al procesamiento de datos estadísticos como una de las técnicas para elaborar posiciones de información, si bien se destaca que esta herramienta de análisis ha de ser mejorada, pues la falta de datos estadísticos precisos en relación con la actividad criminal no siempre permite realizar análisis plenamente exactos.

De lo anterior puede concluirse que es necesario clarificar cuáles son las actuaciones que pueden llevar a cabo las autoridades policiales y de seguridad con el fin de elaborar posiciones de información. Debido a que la utilización de las TIC permite acceder y procesar una ingente cantidad de datos, los riesgos que ello implica para el derecho a la privacidad de los ciudadanos son evidentes. De ahí que sea preciso regular estas actuaciones de manera precisa. Ello no resulta sencillo, puesto que requiere definir previamente qué se entiende por funciones de "seguridad y de prevención", así como el concepto de "medida de investigación penal" en un sentido estricto. En la medida en que los dos ámbitos —el preventivo y el represivo— no están nítidamente separados, resulta complicado también delimitar los poderes de actuaciones de las fuerzas policiales y de seguridad en la elaboración de posiciones de información.

2. (2) ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y/o privadas (por ejemplo, el Registro de pasajeros o datos financieros como los SWIFT) tienen acceso las fuerzas policiales y de seguridad?

Algunos informes responden a esta cuestión señalando que la policía puede accede a todo tipo de bases de datos, si existe una previa autorización judicial (así, por ejemplo, Brasil o Colombia). De ahí que no resulte fácil saber qué bases de datos son accesibles directamente por las fuerzas policiales en esos países. Otros países indican que las autoridades policiales pueden accede a todo tipo de bases de datos públicas, pero, si se ven afectados datos personales, entonces se requiere autorización judicial (Italia, Holanda). En Holanda, además, las fotografías de personas, son, conforme a la normativa sobre protección de datos, datos sensibles, ya que pueden permitir identificar los orígenes étnicos o las creencias religiosas de ese individuo. Por ello, para accede a esas fotografías se requiere previa autorización judicial.

Parece que todos los países permiten que las fuerzas policiales y de seguridad accedan a las bases de datos de acceso abierto (*open-source*) y, además, a bases de datos de huellas digitales, registros de documentos de identidad, registros de matriculación de vehículos, la información sobre los huéspedes registrados en los hoteles, información de aduanas, registro de licencias de armas, archivos policiales, y los sistemas de intercambio de información como Europol e Interpol. Estas bases de datos pueden consultarse, de ordinario, sin previo control

[38] Vid. el informe USA, p. 22: "for the purposes of the application of the Foreign Intelligence Surveillance Act a foreign power includes not only a foreign government or an entity under the control of a foreign government, or a foreign-based political organisation, but also a group engaged in international terrorism or activities in preparation therefor, and an entity not substantially composed of US citizens or residents that is engaged in the proliferation of weapons of mass destruction".

judicial. Ahora bien el acceso puede estar sometido a diversos controles, como una previa autorización interna, la introducción de un código de acceso, o incluso código que solo permiten acceder a información limitada, dependiendo de los objetivos de la búsqueda y las funciones que desempeña quien accede a la base de datos. Dentro de la UE, las autoridades policiales también pueden tener acceso al Sistema de Información de Visados (VIS, *Visa Information System*), en el cual se contienen datos biográficos, y biométricos de las personas que han solicitado un visado para el espacio Schengen. Para poder accede a esta base de datos, la autoridad correspondiente ha de has constar que esa consulta es necesaria para prevenir, detector o investigar un delito de terrorismo u otro delito de naturaleza grave[39]. Bajo condiciones semejantes las autoridades policiales en de los estados miembros de la UE y Europol, pueden acceder a la base de datos EURODAC, que contiene los datos de aquellas personas que han formulado una petición de asilo en alguno de los estados miembro de la UE. El Supervisor Europeo de Protección de Datos (EDPS) expresó su preocupación por el acceso libre por parte de unidades policiales a estas bases de datos. Como consecuencia de estas acciones del EDPS en 2013, estos accesos se verifican por una autoridad independiente en cada uno de los estados miembro[40]. El Sistema de Información Aduanera de la UE (*Customs Information System*, CIS) cuenta con una base de datos de identificación con datos biográficos y datos empresariales, a los cuales también pueden acceder las autoridades policiales de los estados miembro de la UE, además de Europol y Eurojust.

En general, sobre la base de la información contenida en los informes nacionales, no puede determinarse claramente si el acceso a las bases de datos por parte de la policía se permite solo en el ámbito de una investigación penal ya abierta, o si ese acceso también es posible con la finalidad de elaborar posiciones de información. En los USA, sin embargo, sí se señalan específicamente cuáles son las bases de datos que pueden accederse sin vulnerar los derechos de la 4ª Enmienda: las autoridades policiales de ese país pueden acceder directamente sin previa autorización judicial a datos externos de comunicaciones o *metadata*, rastrear las páginas webs visitadas, los números de teléfonos marcados, además de los datos del suscriptor de servicios de telefonía o comunicaciones, porque se considera que respecto de esos datos no puede existir una expectativa razonable de privacidad.

Si nos centramos en las bases de datos de ADN, las respuestas son muy variadas: mientras que en Italia se necesita una orden judicial, en Austria, Bélgica, China (*State Bureau Agency*), Croacia, Japón y España parece que pueden consultarse esos datos sin previo control judicial. Sin embargo, no resulta claro si además de poder acceder a los datos de AND, la policía también puede proceder al cotejo de los perfiles de ADN. Por su parte, el rapport de Turquía informa que ese país carece de base de datos de ADN.

Las bases de datos privadas solo son accesibles dentro del ámbito de la investigación penal de un delito, pero no con fines de carácter preventivo o para la elaboración de posiciones de información (Austria, Bélgica, Brasil, Colombia, Finlandia, Japón, Holanda, España), y de ordinario solo previa orden judicial, a excepción de las bases de datos de acceso abierto.

*2. (3) ¿Pueden aplicarse técnicas de rastreo y cotejo de datos (*data mining y data matching*)? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? Si es así, ¿se han desarrollado herramientas especiales para las fuerzas policiales y de seguridad?*

El desarrollo de programas de software altamente sofisticados[41] ha hecho posible que puedan rastrearse una enorme cantidad de datos tanto de los archivos de inteligencia como a través de búsquedas y rastreos en internet. Como ha sucedido en USA[42], se han aunado los recursos del sector público y del sector privado, para crear unos centros integrados conocidos como *fusion centres*, para optimizar la obtención, análisis, e intercambio de información relativa a datos bancarios y financieros, datos de propiedad inmobiliaria, educación, ventas minoristas, servicios sociales, transportes, envíos postales y mediante mensajería, contratos y operaciones de establecimiento y alojamiento, etc. Toda esta información puede recabarse introduciendo simplemente el nombre, una dirección, un número de teléfono o el número del documento de identificación o de la seguridad social. Estas herramientas de rastreo de datos o *data mining* permiten obtener en un brevísimo espacio de tiempo una inmensa cantidad de información sobre determinadas personas, permitiendo que se elabore perfiles de posibles sospechosos o de grupos de riesgo. El rastreo de datos puede centrarse en un concreto objetivo (*target-driven*),

[39] Vid. E. De Busser, p.17.
[40] Vid. E. De Busser, p.18-19.
[41] Como, por ejemplo, ADVISE (*Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement*), Verity K2 Enterprise (un programa del Departamento de Defensa de los Estados Unidos dirigido a la identificación de terroristas extranjeros y ciudadanos estadounidenses relacionados con actividades de espionaje e inteligencia internacional), TALON (*Threat and Local Observation Notice*), STAR (*System-to-Assess-Risk*), "XKeyscore" (que filtra la información y la traduce a texto, además de registrar aquellos datos de tráfico y de contenido de las comunicaciones, que se ajustan a unos determinados parámetros o palabras clave), o CARNIVORE (un programa específico para la interceptación y copiado de correos electrónicos en tiempo real), tal y como se señala en el informe USA, pp. 57- 61.
[42] Informe nacional USA, p. 60.

lo cual consiste en recabar información sobre un sospechoso identificado; bien centrarse en determinados factores relevantes o factores de búsqueda (*match-driven*), con el fin de determinar si una persona encaja dentro de los parámetros de posible objetivo; o bien centrarse en un determinado suceso o evento, con el fin de descubrir al autor o autores de un suceso o acto acaecido en el pasado[43]. Sin duda, el procesamiento y análisis de tal cantidad de datos y fuentes de información, aunque se hayan obtenido a través de bases de datos o webs de libre acceso, pueden suponer una grave intromisión en la esfera de la privacidad de los ciudadanos.

A pesar de ello, la mayoría de los sistemas jurídicos no regulan de manera precisa la medida de rastreo de datos, ni señalan en qué casos puede realizarse, frente a quién y cuáles son las condiciones y requisitos para recabar y procesar esa ingente cantidad de información. Tampoco hay normas acerca de si el *data mining* puede llevarse a cabo con fines preventivos para crear perfiles de potenciales delincuentes. Llama la atención que la ausencia de regulación jurídica (por ejemplo, en Argentina, Brasil, Bélgica, Colombia, España, o Italia, aunque algunas de éstas sí regulan el cotejo de datos de ADN), no parece impedir que en la práctica se efectúen estos rastreos de datos de manera generalizada en la mayoría de los países, al menos en el ámbito de la prevención de riesgos y también por parte de los servicios secretos de inteligencia. El único informe que de manera expresa señala que el *data mining* no está permitido es el de Argentina.

La realidad descrita indudablemente supone un problema importante, pues refleja que la medida de rastreo y cotejo de datos electrónicos se está llevando a cabo sin una base legal específica. De ordinario si los datos se obtienen en sitios red de libre acceso, se considera que son datos disponibles para cualquiera que accede a internet, y por tanto, las garantías del derecho a la privacidad no deberían ser de aplicación: equivaldría a un dispositivo de vigilancia y seguimiento en la calle realizado por agentes. En cambio, si los datos no son libremente accesibles, el rastreo de esos datos debería estar sometido a las mismas normas y condiciones de la intervención de las comunicaciones. No obstante, nos encontramos con que no se cumple el requisito de la suficiente base legal, exigida para garantizar la adecuada protección de la privacidad de los ciudadanos y que éstos puedan prever cuando pueden producirse esas intromisiones y cuáles pueden ser las consecuencias. En la práctica, la mayoría de las personas desconocen hasta qué punto sus datos personales que figuran en internet pueden ser objeto de un rastreo masivo y analizados en cuestión de segundos, de tal manera que es posible hacer un seguimiento preciso y exhaustivo de sus movimientos, sus actividades, y las transacciones que hayan realizado. Faltando una base legal suficiente, no queda establecido si el *data mining* solo puede llevarse a cabo cuando concurra una sospecha inicial de la comisión de un delito o si, por el contrario, puede también efectuarse con el fin de crear perfiles de grupos de riesgo o de delincuentes potenciales.

Los pocos países que sí cuentan con una regulación específica sobre el rastreo de datos electrónicos, someten esta medida a requisitos muy diversos. Austria permite el *data mining* para la investigación de delitos cuya pena privativa de libertad sea al menos de 10 años y siempre que existan elementos de la sospecha de la comisión del delito. Si el rastreo afecta a datos sensibles, como por ejemplo, datos sobre el origen étnicos, ideas políticas, creencias religiosas o datos sobre la vida sexual, entonces la medida está sometida a previa orden judicial. Como regla, fuera de los casos señalados en Austria no se permite el rastreo de datos, debido a la normativa sobre protección de datos. En Bélgica, el *data mining* está previsto en el ámbito tributario para que la administración tributaria pueda rastrear y cruzar datos con el fin de detectar fraudes tributarios. Fuera de esos casos, no se permite utilizar el *data mining* para crear perfiles de posibles delincuentes o grupos de riesgo. Japón, Turquía y Holanda utilizan el rastreo de datos, aunque no con el objeto preventivo ni de crear perfiles de riesgo. En Suecia, por el contrario, esta última finalidad sí está admitida. En definitiva, lo que se desprende de los informes nacionales es que el *data mining* está siendo utilizado tanto con fines preventivos como de investigación de penal, pero sin que quepa identificar ni las condiciones ni los límites de su uso, pues falta un desarrollo legal adecuado.

Sin duda es en los países grandes, con un papel más relevante en la esfera de la seguridad global y con presencia e intereses económicos en todo el mundo, donde más se ha avanzado en el desarrollo de herramientas sofisticadas para el rastreo masivo de datos. Este tipo de países con protagonismo en materia de seguridad a nivel mundial, invierten enormes cantidades de dinero en el desarrollo de programas de seguridad y para la lucha contra el terrorismo. Parece que en este contexto, los USA ocupan una posición de liderazgo en cuanto a obtención y procesamiento de información a través de programas de *data mining*. Aunque puede suceder que aparezcan como los líderes del *data mining*, simplemente porque sus actividades se han filtrado a los medios de comunicación recientemente, pero no cabe descartar que otros países también lleven a cabo las mismas prácticas, pero sencillamente esa información no ha trascendido al público.

El ordenamiento jurídico estadounidense regula las actuaciones de obtención y análisis de datos relativos a seguridad exterior y espionaje de otros poderes extranjeros (*foreign intelligence*) por parte de la NSA. También se regula la obtención y procesamiento de datos, tanto de sujetos extranjeros como de ciudadanos norteamericanos, que estén en contacto o que tengan relación con sujetos o poderes extranjeros. Sobre la base legal de la FISA

[43] Seguimos aquí la definición contenida en el informe nacional USA, p.1.

(*Foreign Intelligence Surveillance Act*), los USA llevaron a cabo un programa denominado *Prism*, cuyo objetivo era recabar información de extranjeros residentes en el extranjero, requiriendo a compañías privadas para que procedieran a entregar los datos de los que dispusieran respecto de los mismos. Estas peticiones se cursaban en la forma de *National Security Letters*, una especie de orden para aportar datos, que no está sometida a control judicial. Otro programa, conocido con el nombre de *Boundless Informant*, tenía como objetivo la interceptación de datos telefónicos en tiempo real, tanto en el interior de los países vigilados, como de comunicaciones provenientes o destinadas a esos países. Si la información afecta o pudiera afectar a un ciudadano estadounidense, el gobierno ha de solicitar la previa autorización judicial. Para ello se estableció un tribunal específico (*Foreign Intelligence Surveillance Court*), formado por 11 jueces federales de distrito, designados por el Presidente del Tribunal Supremo norteamericano, competente para resolver esas solicitudes, las cuales parece que se conceden prácticamente en su totalidad.

Además de la NSA, los USA desarrollan planes de inteligencia interior que llevan a cabo el FBI y la CIA.

A nivel europeo, los datos proporcionados por las autoridades policiales y de seguridad de los distintos estados miembros se centralizan en Europol, y se utilizan para efectuar *data mining*, cotejo de datos y procesamiento y análisis de los mismo. Los análisis se clasifican en función de su autenticidad y del grado de fiabilidad (información confirmada y no-confirmada)[44].

2. (4) ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la elaboración de posiciones de información?

A pesar de que esta pregunta iba dirigida a determinar el uso de medidas coercitivas y restrictivas de derechos fundamentales en la fase pro-activa del proceso o con el fin de elaborar posiciones de información, las respuestas se centran principalmente en la intervención de comunicaciones, y a este respecto los ordenamientos jurídicos estudiados presentan soluciones muy diversas en función de la fase en que se encuentre la investigación. Algunos países excluyen completamente la posibilidad de intervenir las comunicaciones en una fase de investigación pro-activa (Bélgica, Suecia), mientras que otros países las permiten, confiriendo amplios poderes a las autoridades en esta fase de elaboración de posiciones de información (por ejemplo, Finlandia y China). La mayoría de los ordenamientos jurídicos condicionan la utilización de medidas coercitivas en la fase preventiva o proactiva a la previa autorización judicial, aunque esa autorización en muchos casos sea una mera formalidad, porque el órgano judicial no revisará los motivos de fondo que justificarían la adopción de dicha medida (Argentina, Brasil, Japón, Italia, España o USA, por ejemplo). Otros países limitan las medidas coercitivas en esta fase a cierto tipo de delitos, como los relacionados con la delincuencia organizada o los delitos informáticos (por ejemplo, Austria y Croacia). Si bien los informes nacionales aportan información interesante, lo cierto es que sería aventurado sacar conclusiones definitivas sobre la utilización de medidas coercitivas con fines de elaboración de posiciones de información. Ello se debe, una vez más, a que algunos informes nacionales no diferencian claramente entre las actividades propias de los servicios secretos de inteligencia, encargados de cuestiones de seguridad nacional y las medidas de recabar información con el fin de elaborar estrategias de actuación y prevención por parte de las fuerzas policiales.

Este es el caso, en particular, de los USA, donde el concepto "elaborar posiciones de información" es completamente desconocido. De ahí que la información que se contiene en ese informe —por lo demás, excelente— se refiere a actuaciones de los servicios secretos de seguridad, ya sea a nivel nacional o dirigidas a la vigilancia y control de personas o estados extranjeros. Entre las actuaciones de inteligencia, ya sea llevadas a cabo por la CIA o por la NSA, pueden acordarse tanto el acceso a correos electrónicos almacenados, como la interceptación de comunicaciones. Estas medidas, sin embargo, están sometidas a previa autorización judicial, siempre que se dirijan contra un ciudadano de nacionalidad estadounidense. En caso contrario, el control judicial no es requerido. En el caso de las actividades que se realizan bajo la ley FISA, la interceptación de comunicaciones así como el registro de comunicaciones electrónicas se somete a previa autorización judicial por parte del tribunal específico para este tipo de actuaciones de vigilancia, *Foreign Intelligence Surveillance Court.*

A los efectos del proceso penal no sólo resulta necesario determinar si en una fase de investigación proactiva pueden acordarse medidas de vigilancia e interceptaciones restrictivas de los derechos fundamentales, sino clarificar si la información así obtenida puede adquirir eficacia probatoria en un eventual juicio posterior. A pesar de tratarse de medidas muy intrusivas, en particular desde la perspectiva de la protección del derecho fundamental a la privacidad, su utilización como prueba en el proceso penal no debe ser necesariamente rechazada, siempre y cuando se respeten las reglas de exclusión de prueba. Italia traza una clara línea: la interceptación de comunicaciones acordada por el ministerio fiscal en el ámbito preventivo no tendrá eficacia probatoria. El problema radica en que —tal y como se señala en el informe de Turquía— las reglas de exclusión de prueba no siempre son respetadas, y las intervenciones que se acordaron con fines meramente investigativos

[44] Vid. E. De Busser, pp. 34-35.

y preventivos sin previa existencia de indicios, y sin previa autorización judicial, terminan siendo valoradas como prueba en el juicio.

2. (5) ¿Qué sujetos o entidades privados (por ejemplo, proveedores de internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para fines policiales o de seguridad?

Todas las compañías telefónicas, y después las proveedoras de servicios de comunicaciones vía internet, siempre han efectuado un registro de las comunicaciones de sus clientes, el origen y el destino de la llamada o comunicación, así como la duración de la misma, con el fin de poder facturar el servicio prestado. Una vez concluido el proceso de facturación, esos datos generalmente eran borrados. No obstante, con el tiempo se ha puesto de relieve que esos datos sobre el registro de las comunicaciones y conexiones a internet han resultado ser decisivos en la investigación de delitos graves, especialmente en la investigación de delitos de terrorismo. Ello ha llevado numerosos países a considerar la conveniencia de imponer legalmente la obligación de retener y conservar esos datos por un tiempo determinado, por si fueran necesarios para esclarecer la comisión de determinados delitos graves. En el ámbito de la Unión Europea, esto se tradujo en la aprobación de la muy discutida Directiva sobre retención de datos. Esta directiva se aplica a datos sobre el tráfico de las comunicaciones y datos de localización, tanto de personas jurídicas como físicas, además de a aquellos datos que son necesarios para identificar el usuario registrado. La directiva no afecta al contenido de las comunicaciones electrónicas ni tampoco a la información consultada mediante la utilización de sistemas de comunicación electrónicos (art. 1.2 Directiva 2006/24/CE sobre la conservación de datos). La directiva EU establece la obligación de retener los datos por un plazo no inferior a 6 meses (art. 6); define cuáles son los datos que las compañías están obligadas a retener (arts. 3 y 5); regula las condiciones para permitir el acceso a esos datos (arts. 4 y 8); y además contempla la exigencia de respetar el derecho a la protección de datos (art. 7). Así, en el ámbito de la UE puede afirmarse que existe un marco legal armonizado en material de obligación de retención de datos por parte de compañías privadas de servicios de telecomunicaciones[45].

En USA, la *Electronic Communications Privacy Act* 18 U.S.C. *§§* 2701-2711, también regula la obligación de retener los datos por parte de las proveedoras de servicios de telefonía y comunicaciones. Pero, por lo que se refiere a los otros países no europeos analizados, los informes indican que esa obligación de retención y conservación de datos se da en los casos en que una orden judicial así lo exija (Argentina, Brasil, Colombia, Turquía). No obstante, al igual que en relación con otras cuestiones, no queda claro si la orden judicial de retener y conservar los datos de comunicaciones electrónicas tiene que estar vinculada a la investigación de un delito concreto, o bien puede acordarse con fines preventivos o proactivos. Parece que este es el caso de Turquía, donde se contempla un plazo de retención y conservación que va desde los 6 meses a los 2 años, pero fuera del ámbito europeo no parece que la ley obligue a las compañías privadas que prestan servicios de telecomunicaciones a retener los datos de comunicaciones[46].

2. (6) ¿Qué sujetos o entidades privados pueden o están obligados a proporcionar información a las fuerzas policiales o de seguridad?

Al preguntar acerca de la cooperación entre entidades privadas y las fuerzas policiales en lo relativo al uso de las TICs, las respuestas tienden a centrarse en la cooperación prestada por compañías proveedoras de servicios de telefonía y de internet. Esto resulta lógico, puesto que la cooperación con este tipo de compañías resulta esencial en la prevención y persecución de delitos graves. Sin embargo, no hay que olvidar que, además de las empresas de telecomunicaciones, otras compañías privadas relacionadas con el uso de TICs también pueden desempeñar un papel importante a la hora de prevenir e investigar de actividades delictivas, como puede ser el caso de la vídeo vigilancia. No obstante, en este apartado nos centraremos en los datos relativos a servicios de comunicaciones y en los datos electrónicos almacenados.

La Convención sobre Ciberdelincuencia de 2001 ya destacó la importancia de contar con la cooperación de este tipo de empresas. En concreto, en su art. 18.1, establece que las normas procesales penales han de contemplar medidas que permitan solicitar y obtener datos sobre los usuarios y sus comunicaciones, que tengan empresas

[45] En el momento de escribir este informe esta Directiva se encuentra en proceso de revisión. El Informe de Evaluación realizado por la Comisión EU, Bruselas 18.4.2011 (COM(2011) 225 final), concluía que la UE debía seguir apoyando y regulando la retención, el acceso y el uso de los datos de telecomunicaciones. No obstante, la normativa europea en este ámbito requería mejorarse con el fin de evitar que los diversos tipos de operadores de telecomunicaciones se vieran sometidos a trabas injustas en el mercado interno, así como para asegurar un alto nivel de garantías del derecho a la protección de datos. La Unión Europea ha creado un grupo de trabajo para revisar este instrumento jurídico. Sobre el impacto de esta Directiva EU puede verse el interesante estudio independiente "Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries", de noviembre de 2012, accesible en http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf .

[46] Vid. UNODC *Comprehensive Study on Cybercrime*, p. 145.

privadas o personas físicas. Esa cooperación resulta esencial tanto para la investigación de delitos informáticos, como para esclarecer y perseguir cualquier otro tipo de delitos que implique el uso de las TICs y cuyo acceso sea necesario y esté permitido.

En este punto, más allá de constatar una general obligación de cooperación, resulta de especial interés determinar en qué medida y bajo qué condiciones están las compañías privadas obligadas a facilitar a las autoridades policiales la información sobre comunicaciones y clientes que les es requerida. La cuestión problemática radica en definir el alcance de esta obligación en la fase proactiva o con el fin de elaborar posiciones de información, porque parece claro que, en el ámbito de una investigación penal por un concreto delito, la obligación de facilitar datos en posesión de las empresas de telecomunicaciones vendrá determinada por lo que ordene la autoridad judicial competente dentro del proceso penal. Aunque es precisamente en ese ámbito proactivo donde más necesario resulta clarificar el alcance de la obligación que tienen las compañías proveedoras de internet de cooperar con las autoridades públicas, lo cierto es que aquí, como en tantas otras cuestiones de este estudio, las esferas de investigación proactiva, investigación y enjuiciamiento penal no aparecen nítidamente diferenciadas.

Todos los países señalan que las entidades privadas están obligadas a facilitar a la policía la información requerida si consta una orden judicial, y en algunos países también a petición del ministerio fiscal (Italia u Holanda). Esto podría interpretarse en el sentido de que sólo habría obligación de entregar la información solicitada por las autoridades judiciales —y excepcionalmente por la fiscalía— pero no por la policía. Sin embargo, esa conclusión podría no ser correcta, puesto que el cuestionario no distingue en este punto entre los diferentes tipos de datos, y de ahí que las respuestas en los informes nacionales no aludan por separado a los datos de tráfico de las comunicaciones y al contenido de las mismas. En todo caso, si valoramos estas respuestas en conexión con las ofrecidas a la pregunta anterior, cabe deducir que la regla general es que el acceso al contenido de las comunicaciones no puede obtenerse sin previa autorización judicial, y de ordinario sólo en el contexto de un proceso de instrucción penal. Respecto de los demás datos distintos del contenido de la comunicación, el informe de Croacia claramente señala que la policía puede obtener de las compañías de telecomunicaciones esos datos (identidad del titular de una cuenta de internet o de telefonía, datos de tráfico de comunicaciones, y geo-localización) con fines preventivos, previa solicitud y autorización por parte del Director general de la policía criminal. En España, la dirección IP puede obtenerse sin previa orden judicial: a pesar de que esta cuestión no está regulada legalmente, el Tribunal Supremo español sostiene que, en la medida en que la dirección IP no permite identificar a una persona o usuario concreto, ese dato no se ve amparado por el derecho a la protección de datos, por lo que la autorización judicial no es preceptiva. Sólo uno de los países estudiados (Japón) afirma que no existe obligación por parte de las compañías de telecomunicaciones de prestar cooperación a las fuerzas policiales en la elaboración de posiciones de información.

La situación en los Estados Unidos merece un análisis particular, no sólo porque en este país existe una extendida práctica de cooperación entre compañías privadas de servicios de telecomunicaciones y las autoridades policiales, sino también porque existe una amplia regulación normativa sobre las condiciones y requisitos de esa cooperación. En virtud de FISA y la ley sobre asistencia a las fuerzas policiales en materia de comunicaciones (*Communications Assistance for Law Enforcement Act*, CALEA), las compañías privadas de servicios de telecomunicaciones están obligadas a facilitar a la policía los datos que requieran, pero también dar información y prestar la asistencia técnica necesaria para que procedan a la interceptación de comunicaciones telefónicas, electrónicas y conversaciones directas, además de facilitarles que puedan llevar a cabo medidas de vigilancia electrónica. En caso de no cumplir con las solicitudes legítimas remitidas por la policía, procedería obtener una orden judicial para lograr el cumplimiento de las obligaciones de cooperación y asistencia. Si la empresa no atendiera a la orden judicial, podría ser sancionada con una multa económica.

Las compañías deben guardar confidencialidad acerca de la interceptación o intervención realizada, incurriendo en responsabilidad civil por daños y prejuicios en caso de revelar la existencia del operativo de intervención o vigilancia de las comunicaciones. Además, la ley establece que las compañías no incurrirán en responsabilidad civil frente a sus clientes como consecuencia del cumplimiento de su obligación legal de cooperar con las autoridades policiales o al dar cumplimiento a una orden judicial de intervención de las comunicaciones. El informe nacional USA señala que solo la compañía AT&T atiende una media de 700 solicitudes diarias provenientes de autoridades policiales o de investigación, de las cuales unas 230 se califican como urgentes y han de tramitarse sin previa autorización judicial. En la práctica, se ha observado que existía una relación especial entre la NSA y determinadas compañías de servicios de telecomunicaciones (en particular con AT&T), de tal forma que la agencia de inteligencia tenía acceso directo a los contenidos de las comunicaciones. Mediante un programa especial, la NSA también ha obtenido acceso a los datos de Microsoft, Google o AOL, con el fin de llevar a cabo medidas de rastreo de datos. Recientemente se ha publicado que la NSA tenía control sobre los cables de fibra óptica, de tal manera que podía acceder directamente a todos los datos sin necesidad de firmar acuerdos con las compañías privadas de servicios de telecomunicaciones.

En cuanto a la cooperación de estas compañías privadas con autoridades extranjeras, normalmente sólo procede previa orden judicial o autorización emitida en el lugar donde tenga la sede la compañía. No obstante, Google, por ejemplo, ha declarado que en ocasiones ha prestado su colaboración a autoridades extranjeras voluntariamente, siempre que la petición de asistencia fuera compatible con la normativa internacional[47].

El informe de Holanda hace mención de otro tipo de colaboración entre fuerzas policiales y empresas privadas: el seguimiento y vigilancia de determinadas personas o lugares que llevan a cabo empresas de seguridad privadas (Securitas). Las autoridades policiales muestran a esa empresa a través de fotografías las personas, vehículos o lugares que han de ser vigilados y la empresa a su vez envía a esas autoridades todas las imágenes o videograbaciones que hayan obtenido como resultado de su actividad de seguimiento[48].

2. (7) ¿Está sometida la actividad de elaboración de posiciones de información (information positions) a control judicial?

La respuesta es diferente según los países. En la mayoría de los países estudiados parece que la actividad de elaboración de posiciones de información, si existe regulación legal sobre la misma, no está sometida a previo control judicial (Bélgica, Croacia, Italia, Holanda, España), salvo que se lleven a cabo medidas restrictivas de derechos fundamentales (Colombia o Croacia) o cuando afecte a información especialmente sensible para el derecho a la privacidad (Holanda). En Austria, aunque las actuaciones de la policía en el marco de sus funciones de seguridad, prevención o inteligencia no requieren previo control judicial, sí están sometidas al control de un abogado independiente ubicado en el ámbito del Ministerio de Interior. Este abogado lleva a cabo tres tipos de supervisión: un control previo, otorgando la autorización; un control ex post, informando acerca de las medidas acordadas; y finalmente, una notificación a las autoridades oportunas sobre las actuaciones llevadas a cabo. Por su parte, Bélgica no prevé un previo control judicial sobre las actividades de la policía en la elaboración de posiciones de información, pero una Comisión Parlamentaria específica tiene encomendada la función de proteger el derecho a la privacidad y el derecho a la protección de datos. El sistema funciona sobre la base de las quejas recibidas. Una vez que éstas son analizadas, se intenta lograr una solución a través de la mediación o la conciliación, y sólo en caso de no alcanzarse esta solución se emite una recomendación o una advertencia. La Comisión también podrá recibir quejas relativas a infracciones del derecho a la protección de datos por parte de órganos policiales. De este modo existiría un control de la actividad policial en el ámbito de inteligencia, pero con las limitaciones que implica un sistema de control a posteriori y con un alcance limitado a la protección de datos.

3. Las TIC en la investigación penal

3. (1) ¿Pueden las fuerzas policiales y de seguridad llevar a cabo intervenciones electrónicas en tiempo real a) de datos sobre la comunicación (e-traffic data), b) sobre el contenido de los datos?

Muchos datos electrónicos puede que nunca lleguen a guardarse, por lo que para acceder a los mismos en casos de urgencia y debido al carácter volátil de los mismos, la medida de interceptación en tiempo real puede ser imprescindible. Diversos convenios internacionales y regionales, además de diferentes instrumentos jurídicos en materia de ciberdelitos, contienen normas sobre la interceptación en tiempo real de datos electrónicos[49]. Todos los países estudiados, excepto Japón, indican que en su ordenamiento jurídico pueden interceptarse en tiempo real las comunicaciones electrónicas, bien sobre la base de la normativa general de intervención de comunicaciones, la normas sobre escuchas telefónicas (así, por ejemplo, en Argentina, Italia, España o Turquía), o aplicando la normativa específica sobre interceptación y registro de comunicaciones electrónicas. En la práctica, es frecuente que se tome como base legal autorizante la regulación de las escuchas telefónicas, lo cual plantea diversos problemas[50]. Por ejemplo, en Turquía el precepto sobre escuchas telefónicas utiliza el verbo "escuchar", el cual obviamente no es adecuado para referirse a imágenes o mensajes, por lo que surgió la cuestión acerca de si esa norma realmente podía servir como base jurídica para las interceptaciones electrónicas, tanto de datos de tráfico como de contenido, en tiempo real. La jurisprudencia de los tribunales turcos ha admitido una interpretación extensiva del término "escuchar", y con ello en la práctica las intervenciones de comunicaciones electrónicas se efectúan sobre la base legal de la regulación prevista para escuchas telefónicas, siempre que se cumplan los requisitos exigidos en la misma.

La mayoría de los países —China parece ser la excepción— requieren una previa autorización judicial para acordar esta medida: Austria (arts. 134 y 135 CPC), Bélgica (art. 88bis y 90 CPC) Brasil, Croacia (art. 332 CPC), Finlandia, Italia (art. 266 bis CPC), Holanda, España (art. 579 CPC, excepto para los meta-datos, que pueden

[47] Vid. UNODC *Comprehensive Study on Cybercrime*, p. 150.
[48] Informe de Holanda, p. 7.
[49] Por ejemplo, art. 20 del Convenio sobre Ciberdelincuencia del Consejo de Europa; art. 29 de la *League of Arab States Convention* o el art.19 de la *Commonwealth Model Law*.
[50] En España sobre este tema, vid. J.C. Ortiz Pradillo, "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en *El proceso penal en la sociedad de la información* (J.Pérez Gil ed.), Madrid 2012, pp. 267-310, 300.

obtenerse sin previa autorización judicial), Suecia, Turquía (art. 135 CPC) y los USA (excepto los meta-datos, para los cuales en algunos estados no se requiere previa autorización judicial). El ordenamiento jurídico norteamericano, sin embargo, distingue entre intervenciones de comunicaciones telefónicas y electrónicas. Para acceder a las comunicaciones electrónicas, almacenadas en un servidor por un espacio de tiempo de 180 días o menos, se requiere una orden judicial basada en la previa acreditación de indicios de criminalidad. Pero si los datos de comunicaciones llevan almacenados más de 180 días, una orden de aportación de datos o decisión judicial sin necesidad de acreditar la existencia de indicios será suficiente. Esta diferencia de requisitos, según se explica en el informe USA, se debe a que el Congreso de los USA equiparó los datos electrónicos almacenados por corto tiempo con una caja de seguridad para depósitos, mientras que los datos almacenados por un espacio de tiempo amplio se equiparaban a los archivos empresariales en posesión de un tercero. Este tratamiento particular, ajeno a la práctica de los demás países, se complica aún más debido a que la normativa cambia en función de si el destinatario de la comunicación ha accedido a sus datos o mensajes dentro del plazo de 180 días o no. En este contexto resulta interesante destacar los datos estadísticos relativos al funcionamiento de esta medida de intervención en la práctica en los USA: según una investigación llevada a cabo por el Congreso USA determinó que las compañías proveedoras de servicios de telefonía móvil respondieron en 2011 a 1.3 millones de peticiones provenientes de agentes policiales para el acceso a mensajes de texto o información relativa a los abonados de esas líneas.[51]

Excepcionalmente, en casos de urgencia, algunos países permiten que la intervención de comunicaciones electrónicas sea acordada por el ministerio fiscal con control judicial *a posteriori.* Una vez autorizada la medida por el fiscal o por el juez, algunos sistemas jurídicos permiten a las fuerzas policiales acceder directamente a los datos, mediante la utilización de un software especial (por ejemplo, Brasil, España o USA), mientras que otros países han de contar con la cooperación de las compañías de telecomunicaciones para efectuar la intervención. La orden judicial autorizante ha de estar motivada y debe como regla cumplir con los requisitos de necesidad, adecuación y proporcionalidad exigidos por el TEDH al analizar las intromisiones que afectan al Artículo 8 del CEDH. Ciertos países limitan el uso de esta medida —en términos parecidos a lo establecido para las comunicaciones telefónicas— a una categoría de delitos enumerados en la legislación procesal penal o bien definidos como delitos graves. El ámbito de aplicación varía de manera significativa de unos países a otros, pues varía la definición de lo que se considera "delito grave", o "delito complejo", y también se aprecian disparidades en la exigencia de otros requisitos, o "razones especiales" (esto último se exige en Croacia).

En general, al describir los requisitos, condiciones y duración de las intervenciones electrónicas, los informes nacionales no diferencian entre interceptación de comunicaciones en tiempo real cuyo objetivo es obtener datos de tráfico, de aquellas que persiguen acceder a los contenidos de las comunicaciones, a pesar de que el grado de intromisión en este último caso es claramente más alto. De los informes parece desprenderse que se utiliza la misma norma legal para los dos tipos de intervenciones –decisión judicial motivada, proporcionalidad, especialidad y duración limitada–, pues no se indica que existan normas diferentes para la intervención de comunicaciones en tiempo real en relación con datos de tráfico y contenidos. Las diferencias parece que se encuentran en la aplicación práctica de esta normativa, a la hora de valorar el requisito de la proporcionalidad de la medida en la resolución judicial.

Bélgica constituye una excepción en este respecto, puesto que la interceptación electrónica de datos de tráfico se regula separadamente de la interceptación de contenidos y ambas medidas se someten a requisitos ligeramente diferentes. Por un lado, el art. 80 bis del *Code d'Instruction Criminelle* (tras la reforma de 1998) se aplica a todo tipo de telecomunicaciones y regula la *recherche et localisation des telecommunications*. Este precepto da cobertura a la interceptación de datos de tráfico: dirección IP, dirección de correo electrónico utilizada, páginas web visitadas, servidores a los que se ha conectado, logins usados para entrar en sitios privados (*peer-to-peer*, *file sharing*, etc.) e historial de conexiones. Como regla, además de requerir autorización judicial, esta medida solo puede adoptarse dentro del ámbito de un proceso penal para la investigación de un delito (y no dentro del ámbito preventivo o de inteligencia policial), su duración está limitada a dos meses (prorrogables) y no existe un listado de delitos para los que se pueda autorizar. Para justificar la necesidad de la medida, el juez de instrucción no tiene que acreditar que otras medidas menos intrusivas han resultado ineficaces.

Por otro lado, el art. 90 *ter* y *quater* del *Code d'Instruction Criminelle* regula la *informaticatap*, o interceptación del contenido de comunicaciones electrónicas en tiempo real. Las principales diferencias entre el acceso a datos de tráfico y el acceso a datos de contenido son: el grado de sospecha requerido (más alto para los contenidos), la duración (más corta para los contenidos), y el hecho de que el acceso a datos de contenido se limita a delitos graves y permite la entrada en domicilio o espacio privado para instalar aparatos que faciliten el acceso al contenido de las comunicaciones. En la práctica, el precepto más usado a la hora de intervenir comunicaciones electrónicas es el art. 90 *ter* y *quater*, pues permite acceder a mucha más información.

[51] Vid. el informe nacional USA, p.28.

El informe belga hace referencia a otra cuestión interesante, en relación con la interceptación de comunicaciones electrónicas en tiempo real. Se da a entender que pueden intervenirse comunicaciones electrónicas en el momento en que se produce la transmisión (*en transmission*). Sin embargo, no resulta fácil determinar en qué momento se encuentra un mensaje electrónico "en transmisión" y cuándo ha sido ya enviado y por tanto se enmarca dentro de la categoría de mensaje o dato "almacenado" (*stored data*). Inicialmente la jurisprudencia belga consideró que la transmisión de una comunicación electrónica no había finalizado hasta que el destinatario hubiese accedido al mensaje[52], pero posteriormente en otras sentencias ha entendido que la transmisión queda concluida al momento en que el mensaje está en el *web mail* y por tanto accesible a su destinatario, con independencia de cuándo éste lo lea.

*3. (2) ¿Pueden las fuerzas policiales y de seguridad tener acceso / bloquear / investigar / decomisar los sistemas de información para obtener: a) datos relativos al tráfico de las comunicaciones (*e-traffic*), b) datos relativos al contenido de las comunicaciones?*

Todos los informes responden a esta cuestión en sentido afirmativo, de conformidad con los instrumentos internacionales y regionales más relevantes en materia de ciberdelincuencia, en los cuales se prevé que los estados firmantes regulen el acceso a datos electrónicos o informáticos y mecanismos para evitar su borrado[53]. Sin embargo, muchos países indican que sus sistemas jurídicos carecen de normas legales específicas sobre el acceso, registro y bloqueo de datos electrónicos, por lo que tales medidas se llevan a cabo bajo aplicando las normas generales sobre acceso y registro de objetos muebles o utilizando las órdenes de aportar objetos o documentos (así, por ejemplo, Argentina, Austria, Croacia, Bélgica, o España). Estas soluciones pueden resultar aceptables en la medida en que sean de carácter provisional, mientras el legislador actualice el marco legislativo, pero sin duda las normas existentes sobre registro y órdenes de aportación de datos no son apropiadas cuando se trata de obtener y registrar datos electrónicos y *on-line*. La lentitud del legislador en adoptar nuevas normas procesales en esta materia es cuando menos llamativa, especialmente en el ámbito pan-europeo, en el que la Recomendación del Consejo de Europa R(95) 13 de 11 de septiembre de 1995 ya destacó la necesidad de "adaptar la legislación procesal de las medidas que legítimamente pueden utilizar las fuerzas policiales en la investigación criminal a las características específicas de las investigaciones en sistemas de información y comunicación electrónicos"[54].

En este contexto, hay varias cuestiones relativas al acceso de datos electrónicos que no quedan bien resueltas recurriendo a la normativa tradicional de registro e incautación de objetos o bienes muebles. Si el objetivo de la medida es obtener datos que se encuentran almacenados en algún *hardware* (disco duro, CDRom, memoria USB, GSM o tablets, por ejemplo), en principio no habría problema en aplicar analógicamente las normas clásicas sobre registro y decomiso de bienes muebles, y de ordinario esa normativa será suficiente. No obstante, pueden surgir problemas a la hora de identificar el concreto precepto aplicable. El siguiente ejemplo puede ilustrar alguno de estos problemas. En el caso de que el ordenador se encuentre en un domicilio privado, para acceder a los datos almacenados en el disco duro de ordinario será necesario obtener una orden judicial de entrada y registro domiciliario, y así registrar o decomisar el equipo informático. En este caso se aplicarán las normas sobre entrada domiciliaria, que en la mayoría de los ordenamientos jurídicos estudiados —no en todos— permite también proceder al registro de equipos informáticos (disco duro, memoria USB, etc.) hallados en ese lugar. Sin embargo, si los datos que han de obtenerse están almacenados en un ordenador situado en un espacio público —por ejemplo en un cibercafé o en una biblioteca pública— no queda claro qué normas deberían aplicarse: ¿las de registros en espacios públicos, o las normas de registro en domicilios, puesto que el equipo informático es un espacio susceptible de privacidad y susceptible de equipararse a "espacio privado"? La doctrina no se pone de acuerdo en este punto y los autores defienden una u otra posición dependiendo de cuál sea la concepción de la privacidad que asuman. Si se centran en la protección de la privacidad de los datos, el hecho de que el equipo informático se ubique en un espacio público o privado sería prácticamente irrelevante, pues el registro del ordenador en todo caso se enmarcaría dentro de las garantías del art. 8 CEDH, y en principio habría de cumplir con los requisitos previstos para los registros domiciliarios. Al contrario, si el acento se pone no tanto en la privacidad de los datos, sino en el lugar en donde se encuentra conectado el ordenador, al ubicarse éste en un espacio público podría considerarse que son de aplicación las normas sobre entrada y registro en espacios públicos.

La cuestión se torna aún más compleja cuando se trata de acceder a datos que se encuentran en un sistema informático o son accesibles a través de una red informática. En estos casos, la normativa sobre registro y decomiso de objetos muebles no resulta siempre apropiada. En primer lugar, porque todo el sistema informático

[52] Informe nacional de Bélgica, p. 36.

[53] Vid. por ejemplo el art. 16 del Convenio de Budapest sobre Ciberdelincuencia de 2001. En relación con otros convenios internacionales vid. el *UNODC Comprehensive Study on Cybercrime*, p.127.

[54] Recomendación del CoE R(95) 13 del Comité de Ministros a los Estados Miembros relativa a los problemas de la legislación procesal penal sobre tecnologías de la información, adoptada en Estrasburgo el 11 de septiembre de 1995.

no puede trasladarse físicamente a las instalaciones policiales para proceder al registro y análisis del mismo (piénsese en todo el sistema informático de, por ejemplo, un hospital o una entidad bancaria). Ello obliga a realizar el registro en el propio lugar, sin trasladar ni decomisar los soportes informáticos o hardware, por lo que para asegurar los datos en ese sistema será necesario proceder al bloqueo de los mismos directamente. En segundo lugar, si el acceso a un ordenador permite acceder a toda la red de ordenadores conectados en línea, ha de abordarse la cuestión relativa acerca de si la orden para registrar un concreto ordenador cubre también el registro de todos los equipos conectados en red.

Los problemas que plantea este "registro ampliado" (*extended search*, o *netzwerkzoeking*, en holandés) se describen en detalle en el informe belga. Si la autorización de registro se refiere a un ordenador ubicado en un domicilio, en principio esa autorización sólo cubre el registro de objetos ubicados en el mismo. Si ese ordenador se encontrara conectado a otros equipos en línea, ubicados en otros lugares, para acceder a los datos contenidos en esos otros equipos sería preciso obtener una autorización judicial adicional. Este sería el modo de proceder si equiparamos el registro de un ordenador al registro de objetos o bienes muebles. Por el contrario, si el registro del ordenador se asimila a un registro domiciliario, el consentimiento del dueño o usuario del ordenador en cuestión permitiría acceder a todos los ordenadores conectados al mismo en red. Este caso sería equiparable al consentimiento que presta el dueño del domicilio, el cual al permitir la entrada está implícitamente autorizando el acceso a todas las habitaciones de la casa. No obstante, el consentimiento del dueño o usuario del ordenador sólo abarcaría el acceso a aquellos ordenadores y datos a los que el propio dueño o usuario del ordenador sujeto a registro podría acceder. Dicho de otro modo, no puede aceptarse el acceso remoto a ordenadores a través de hacking por parte de los agentes encargados de la investigación penal sin autorización judicial, pues sería equivalente a una entrada domiciliaria ilícita. La legislación holandesa regula esta medida, pero somete el acceso remoto de ordenadores mediante software específico a la previa autorización judicial por parte del Juez de Instrucción, una vez que se hayan acreditado indicios suficientes de la comisión de un hecho delictivo[55].

Los ejemplos que se han citado muestran la necesidad de llegar a una definición común de lo que haya de entenderse por "registro y confiscación" (*search and seizure*) de un ordenador, además de evidenciar la necesidad de desarrollar un marco legal que clarifique cuál es el ámbito y los requisitos para llevar a cabo un registro remoto de equipos informáticos. En otras palabras, en todos los países estudiados se echa en falta una regulación legal clara en esta materia. A pesar de que el Convenio de Budapest de 2001 sobre Ciberdelincuencia ya establece que los estados miembros adoptarán normas con el fin de que en la investigación de delitos puedan llevarse a cabo registros ampliados (art. 19.2), varios de los estados miembros de este convenio no parecen haber implementado esta norma en sus respectivos ordenamientos jurídicos nacionales. La ausencia de una regulación específica también es destacada en el informe de UNODC *Comprehensive Study on Cybercrime*: al analizar las medidas de investigación criminal, se señala que la ausencia de previsión legal para acceder a equipos informáticos en red o redes informáticas, con el fin de obtener pruebas y proceder al aseguramiento de los datos de forma rápida y efectiva, es uno de los principales fallos detectados a nivel global[56].

En relación con el decomiso, el aseguramiento y el bloqueo de datos electrónicos o digitales, los problemas no son tan complejos, pero no puede decirse que no existan en absoluto. Lo normal es que puedan ser retenidos los datos obtenidos a través de un registro ordinario, registro informático de un ordenador o registro de una red de ordenadores que resulten de relevancia para la investigación criminal. Si los datos se encuentran en el disco duro de un ordenador, en un pen-drive de memoria USB, en un tablet, Smartphone o CDRom, podrán incautarse esos soportes aplicando las normas tradicionales sobre retención y conservación de piezas de convicción consistente en cualquier objeto o bien mueble. Si los datos se encuentran en un servidor, en una red o en la nube, la normativa sobre retención o embargo de cosas u objetos no resultará aplicable; en este caso se precisan normas específicas que regulen la confiscación, retención y bloqueo de datos electrónicos o digitales, como ya existen en Italia (art. 254 bis CPC). Como señala el informe de Japón con todo acierto, sólo los soportes de hardware son susceptibles de ser confiscados o decomisados, mientras los datos electrónicos propiamente sólo pueden asegurarse. En ese contexto, confiscar los datos significaría extraerlos del lugar o servidor donde se encuentran almacenados y transferirlos a otra ubicación. Esto, como regla general, no está permitido en los ordenamientos jurídicos aquí estudiados, los cuales suelen prever que esos datos sean asegurados mediante copia o haciendo una imagen del disco. Así sucede en Japón, Turquía o Bélgica, en los cuales no se permite confiscar o extraer los datos obtenidos on-line cambiando su ubicación. El aseguramiento de los datos se consigue de ordinario a través de una orden de conservación de ese dato o de embargo, las cuales han de ejecutarse con gran celeridad[57].

---

[55] Vid. el informe nacional de Holanda, p. 16.

[56] Vid. pp.124 ss.

[57] La conservación rápida o *quick-freezes* de datos electrónicos está regulada en los arts. 16 y 17 del Convenio sobre Ciberdelincuencia. En el art. 35 se prevé el establecimiento de un punto de contacto permanente, que funcione 24 horas, los 7 días a la semana para facilitar la cooperación relativa a peticiones de asistencia internacional mutual en materia de

En materia de acceso, confiscación y aseguramiento de datos electrónicos quedan aún varias cuestiones por clarificar. En primer lugar, si la "confiscación" y aseguramiento de datos ha de producirse a través de una orden judicial de retención y conservación de datos, surge el problema de que esas órdenes requieren en principio identificar el objeto sobre el que se proyecta la medida, esto es, el objeto, información o documentos que han de ser aportados, retenidos o conservados. De ordinario esto no puede hacerse al realizar el registro de una red informática, puesto que no será posible que pueda identificarse cuál es la concreta comunicación que resulta relevante para la investigación penal y que, por tanto, ha de asegurarse o aportarse. Además, las órdenes de conservación o aseguramiento suelen estar sometidas al cumplimiento del requisito de la proporcionalidad, un requisito que no resulta fácil de valorar en un breve espacio de tiempo, ya que ello requeriría revisar una enorme cantidad de datos antes de emitir la orden para conservar la comunicación o comunicaciones que son relevantes para el concreto proceso penal. Debido al elevado riesgo de que datos esenciales para la investigación sean eliminados mientras se comprueba y valora la proporcionalidad de la medida, parece que no queda otra opción que asegurar todos los datos desde un inicio.

Por tanto, el aseguramiento de los datos electrónicos de ordinario se efectúa realizando una copia de esos datos. No obstante, surge la duda de si el copiado de los datos solo resulta procedente si la incautación del soporte no es posible o resulta excesivamente compleja. Esta es una cuestión que no se regula en aquellos ordenamientos jurídicos que sí cuentan con normas específicas sobre interceptación, confiscación y conservación de comunicaciones electrónicas. Una vez que los datos han sido copiados, deben adoptarse las necesarias medidas para garantizar su autenticidad, evitando que dichos datos sean manipulados. Para ello se utilizan programas especiales, claves, o técnicas de encriptado. Este es uno de los puntos cruciales para que esos datos puedan adquirir posteriormente eficacia probatoria en el juicio. Una vez más, a pesar de la importancia de esta materia, en general los ordenamientos jurídicos estudiados carecen de normas específicas al respecto.

Finalmente, en algunos estados la conservación de datos electrónicos implica que se bloquee el acceso a esos datos, como sucede en el ordenamiento jurídico belga, mientras que en otros estados esa medida de bloqueo puede acordarse en paralelo a la orden de conservación y al copiado de los datos, con el fin de evitar la distribución de los mismos —por ejemplo, para evitar la distribución de imágenes de pornografía infantil o *hackertools*. La terminología no es clara en este aspecto, pues se utiliza el mismo término de "bloqueo" o *freezing* que el empleado en relación con bienes o activos financieros, si bien la finalidad de una y otra medida son bien distintas.

En suma, todos los países informan que tanto las órdenes de conservación como los registros informáticos y la confiscación de datos electrónicos se utilizan ampliamente en la práctica, en la gran mayoría de los casos aplicando analógicamente las normas tradicionales previstas para registro, confiscación y conservación o embargo de bienes. Pero, como estas normas están pensadas para objetos físicos y por tanto tienen una dimensión espacial, además de proyectarse sobre un concreto objeto, no siempre son adecuadas para regular el acceso y conservación de comunicaciones o datos electrónicos almacenados o en tiempo real, puesto que los datos electrónicos no encajan dentro de la categoría de bien mueble ni son un objeto físico. Las normativa general sobre registro y confiscación de bienes es claramente insuficiente para dar respuesta a la problemática que se suscita en este ámbito, y en particular en relación con el acceso de datos a través de registros de redes informáticas, conocidos como registros ampliados o remotos. Aunque estas lagunas legislativas han sido paliadas en parte por la jurisprudencia, sigue existiendo la necesidad de desarrollar un marco legislativo que confiera la suficiente previsión legal y seguridad jurídica en relación con estas medidas restrictivas de los derechos fundamentales.

3. (3) ¿Pueden las empresas de telecomunicaciones o proveedores de servicios ser obligadas a compartir los datos con las fuerzas policiales y de seguridad? En caso de negativa, ¿podrían aplicarse medidas coercitivas o sanciones?

Esta cuestión ya fue abordada con carácter general en el punto (3)(5), debido a que la mayoría de los ordenamientos jurídicos estudiados no trazan una clara línea entre la cooperación con fines de inteligencia policial o elaboración de posiciones de información, y la cooperación en el ámbito de un concreto proceso penal para la investigación de un delito.

Normalmente las compañías proveedoras de servicios de telefonía y comunicaciones están obligadas contractualmente a proteger la privacidad de sus clientes y no deberían revelar datos de los mismos ni de sus comunicaciones, salvo que sean pedidos por la autoridad judicial competente y cumpliendo los requisitos legales. En la práctica, sin embargo esa vía legal se ha obviado con frecuencia, tal como evidencia la información proveniente de los Estados Unidos, bien a través de acuerdos entre la NSA y las compañías proveedoras de

ciberdelincuencia, y entre ellos, la conservación rápida de datos. En qué medida estos puntos de contacto están funcionando de manera eficaz, no está claro y excede de este estudio.

servicios o bien mediante mecanismos que han permitido que las agencias policiales y de seguridad accedieran directamente a esas comunicaciones.

Al margen de estas prácticas, la mayoría de los países informan que las compañías privadas de servicios de telecomunicaciones tienen la obligación de cooperar con las autoridades judiciales, siempre y cuando se les requiera mediante resolución judicial motivada o mediante orden judicial de revelación o aportación de datos. El plazo para dar cumplimiento a esas órdenes judiciales varía dependiendo del tipo y la cantidad de datos requeridos, y de ordinario suele venir fijado en la propia resolución judicial. Una cuestión que surge en este punto, y que debería analizarse con mayor detenimiento, es la relativa a si estas compañías privadas están obligadas a cooperar revelando datos en aquellos casos en que la propia compañía ocupa la posición de acusada, puesto que muchos ordenamientos jurídicos contemplan ya la responsabilidad penal de las personas jurídicas.

En cuanto a las consecuencias en caso de incumplimiento de la obligación de cooperar, todos los informes nacionales, a excepción de Japón, mencionan la posibilidad de imponer multas pecuniarias –bien de naturaleza administrativa o penal– a la empresa o persona cuya cooperación se solicitó (en Bélgica, por ejemplo, la multa puede ascender a 20.000 euros). Además, en algunos ordenamientos la infracción de este deber de cooperar puede incluso llevar aparejada una pena privativa de libertad –por delito de desobediencia u obstrucción a la justicia– de hasta un año (Croacia y Bélgica) o de hasta dos años (Turquía). Obviamente la privación de libertad sólo puede imponerse a personas físicas, pero los informes no especifican sobre qué persona recaería la responsabilidad en caso de que la empresa incumpla la orden o resolución judicial requiriendo la cooperación de la empresa. Parece que la pena privativa de libertad podría recaer sobre la persona física que tiene acceso a los datos reclamados o que dispone de las claves para acceder a los mismos, pero no queda claro si también otras personas o representantes de la empresa podrían ser sancionados penalmente por no cooperar con la autoridad judicial en la investigación penal. En Suecia la infracción del deber legal de cooperar no sólo puede dar lugar a responsabilidad civil, sino que también puede implicar la prohibición de que la empresa de telecomunicaciones siga operando en el mercado.

En la práctica no parecen darse problemas de cooperación por parte de las compañías proveedoras de servicios de telecomunicaciones, pues ninguno de los informes menciona casos de negativa o incumplimiento por parte de las empresas. Ello es así en relación con las empresas ubicadas en el mismo estado del cual emana la decisión judicial. Más difícil resulta determinar hasta qué punto puede obligarse a cooperar a una empresa situada en el extranjero y en qué medida podrían serle impuestas medidas coercitivas (como destaca el informe de Argentina).

El motivo por el cual la cooperación de las empresas de servicios de telecomunicación con las autoridades judiciales funciona de manera fluida, puede deberse a que éstas son compensadas económicamente por colaborar con la justicia. Por ejemplo, el informe de Finlandia indica que el nivel de cooperación es muy bueno con estas compañías privadas, quizás porque legalmente está previsto que les sean reembolsados los gastos ocasionados por su asistencia. En Bélgica las compañías que prestan servicios de telefonía e internet, también tienen derecho al reembolso de los costes generados, y será el juez de instrucción quien se encargue de verificar que la factura se ajusta a los importes fijados legalmente, y se abonará con cargo al presupuesto del Ministerio de Justicia. En Estados Unidos, este tipo de compañías privadas también facturan por estos servicios de cooperación con la justicia cumpliendo con las peticiones de datos relativos a las comunicaciones. El importe total de estas facturas indica la enorme cantidad de peticiones de interceptación y conservación que han atendido estas empresas en cumplimiento de su obligación de colaboración. Conforme al informe nacional USA, las facturas de AT&T por la ejecución de solicitudes de cooperación provenientes de las autoridades policiales, en solo un año ascendió a 8.3 millones de dólares USA, lo cual da una idea de la intensidad de la cooperación. La legislación belga contempla a su vez la posibilidad de reducir el importe que ha de pagarse a las compañías de servicios de telecomunicaciones en el supuesto de que éstas no ejecuten adecuadamente las peticiones de cooperación. Bélgica, además prevé otra medida para incentivar la cooperación o forzar que cumplan con su obligación de obtener o retener de datos a petición del órgano judicial: los operadores de telecomunicaciones están obligados a desconectar aquellas compañías de prestación de servicios de que no cumplan con estas obligaciones legales (vid. p. 56).

La carga de trabajo que supone para las compañías proveedoras de servicios de telecomunicaciones ejecutar las peticiones de asistencia provenientes de autoridades policiales y/o judiciales, ha llevado a que muchas de ellas establezcan departamentos o unidades específicas para coordinar la cooperación con las autoridades de investigación penal, así como para controlar el cumplimento de las solicitudes (así, por ejemplo, Bélgica, España o USA).

En conclusión, aunque pueda resultar discutible que las autoridades policiales y judiciales deban abonar a las compañías los gastos generados en la ejecución de solicitudes de cooperación, lo cierto es que de no existir esa previsión, los gastos generados terminarían por ser asumidos o por los accionistas que verían disminuidos sus beneficios o por los consumidores que verían incrementar sus facturas, o por ambos.

3. (4) ¿Pueden las fuerzas policiales y de seguridad realizar vídeo vigilancia? ¿Pueden obligar a personas físicas o jurídicas a cooperar en su desarrollo?

Para comprender correctamente las respuestas contenidas en los informes nacionales a esta pregunta, es preciso diferenciar tres tipo de situaciones: 1) el uso de la vídeo vigilancia por parte de fuerzas policiales en espacios públicos, ya sea con fines preventivos y de seguridad o dentro de las actuaciones de una investigación criminal[58]; 2) la vídeo vigilancia por parte de autoridades policiales en espacios privados; y 3) la vídeo vigilancia llevada a cabo por personas privadas, ya sea en espacios públicos o privados.

Todos los informes nacionales indican que en sus ordenamientos jurídicos las autoridades policiales pueden llevar a cabo vídeo vigilancia en espacios públicos. La cuestión relativa a si pueden utilizarse cámaras fijas o móviles con el fin de elaborar posiciones de información o para garantizar la seguridad en espacios públicos, ya fue abordada en el apartado (2)(1). Por ello, en este epígrafe nos centraremos en analizar el uso de la vídeo vigilancia como medida de investigación dentro de un proceso penal, esto es, una medida dirigida al esclarecimiento de un concreto delito y acordada una vez que se ha comprobado la existencia de indicios de un hecho delictivo.

En este contexto, en primer lugar ha de señalarse que no resulta fácil identificar qué se considera como medida de vídeo vigilancia. Por ejemplo, en Bélgica, la vídeo vigilancia consiste en una vigilancia sistemática y continuada de una concreta persona o lugar por un espacio de tiempo de al menos cinco días consecutivos. En consecuencia, en este país las filmaciones de un sospechoso o un lugar que no se ajusten a esos parámetros no se definen como medidas de vídeo vigilancia (*observation systematique*) y, por tanto, no les son de aplicación los mismos requisitos legales.

Los requisitos para acordar esta medida de investigación varían notablemente en los diversos ordenamientos estudiados. En algunos países se exige una autorización judicial (Austria o Bélgica) y se limita en el tiempo o sólo se permite en relación con delitos sancionados con una pena privativa de libertad de cierta entidad (por ejemplo, Austria, que exige que la pena sea superior a 1 año de prisión). Otros países no exigen previa autorización judicial, siempre y cuando la vigilancia tenga lugar en espacios públicos (p. ej. Croacia, Finlandia, Italia, España, Turquía, o USA). El sistema estadounidense considera que las actividades desarrolladas en espacios públicos no se encuentran protegidas por la Cuarta Enmienda y, en consecuencia, la vídeo vigilancia no se equipara a una intromisión en la esfera de privacidad, no se le aplican las normas de los registros, y no requiere autorización judicial. Igualmente la utilización de sistemas tecnológicos de reconocimiento facial a partir de imágenes de personas tomadas en espacios públicos, tampoco se somete a autorización judicial. Este planteamiento ha sido objeto de críticas sobre la base del siguiente razonamiento: si bien es cierto que los ciudadanos no tienen una expectativa de privacidad en espacios públicos, pues asumen que pueden ser observados por otras personas, no es lo mismo contar con la posibilidad de ser observado visualmente por otras personas, que ser filmado y vigilado mediante el uso de cámaras o instrumentos de seguimiento en un espacio público. Es más, los ciudadanos tienen la expectativa contraria, de que no serán objeto de seguimiento, observación o grabación con aparatos electrónicos o digitales cuando se encuentran en espacios públicos. Pero, además no sólo el nivel de intromisión es muy diferente entre una observación visual por una persona física y un seguimiento electrónico o filmación, sino que además, el carácter oculto o secreto de estas últimas medidas obviamente altera la percepción que tiene el sujeto vigilado y por tanto sus expectativas de privacidad en ese espacio público[59]. A este respecto el TEDH ha señalado que una grabación sistemática o continua supone una intromisión en la esfera del derecho a la privacidad de los individuos, aún en el caso de que las conductas sometidas a vigilancia tengan lugar en un espacio público[60].

Para comprender el alcance de esta medida y evaluar su utilización desde un perspectiva de derecho comparado sería necesario conocer cuál es el concepto de espacio público que se aplica en cada uno de los ordenamientos

[58] Sobre este tema vid. el interesante informe especial de G. Paolo "Judicial Investigations and Gathering of Evidence in a Digital Online Context", centrado específicamente en los sistemas jurídicos de Canadá, Italia y USA, publicado en el volumen dedicado al Coloquio Preparatorio de la Sección III celebrado en Pula (Croacia) del 6-9 de noviembre de 2008, *Revista Internacional de Derecho Penal*, 1-2 2009, pp. 201-246. Vid. en particular pp. 209-225.

[59] Vid. G. Paolo, p. 244 ss.

[60] Sentencia del TEDH *Rotaru v Romania*, de 4.5.2000, Appl. no. 28341/95, aunque este caso versa sobre el derecho de acceso a datos en posesión de entidades públicas y el derecho a que sean destruidos los archivos secretos del estado con información de ciudadanos que habían sido sometidos a vigilancia sistemática y a persecución penal por razones políticas durante el régimen dictatorial en Rumania. El Tribunal de Estrasburgo en esta sentencia no define el derecho a la privacidad ni el derecho al anonimato de los ciudadanos en espacios públicos, ya que estima la demanda apreciando la infracción del art. 8 CEDH por falta de suficiente previsión legal y la falta de un remedio efectivo para impugnar la legalidad de esos actos de vigilancia. Sobre esta sentencia vid. también L. Bachmaier, "Criminal investigation and the right to privacy in the case law of the European Court of Human Rights", *Lex et Scientia*, nº XVI, vol. 2/2009, Bucharest, pp. 9-29.

jurídicos, lo cual no nos resulta posible con los datos que tenemos[61]. Obviamente, el grado de invasión en la esfera de la privacidad será muy diverso si la filmación tiene lugar en un espacio abierto o en un espacio semi-público, como puede ser un hospital. Lo mismo sucede en relación con la vídeo vigilancia: hemos partido aquí de que la misma consiste en grabar imágenes, pero sin registrar sonidos. A pesar de las dificultades a la hora de definir las características y el ámbito de aplicación de esta medida, una cosa parece clara: la vídeo vigilancia se utiliza en todos los países estudiados para grabar imágenes en espacios públicos dentro de los fines de una investigación penal, bien sea a través de cámaras fijas o móviles.

Más complejo resulta determinar en qué países y bajo qué condiciones se puede llevar a cabo una vídeo vigilancia en espacio privados. En USA, este tipo de grabación oculta en un domicilio o en otro espacio privado está sometido a lo que allí se denomina "*super warrant*", es decir, una autorización específica sometida a criterios más estrictos, sólo posible en relación con determinados delitos graves que se enumeran en la ley, y que coinciden con aquellos respecto de los cuales puede autorizarse una escucha telefónica. El informe de Austria indica que la instalación de cámaras en espacios privados no está permitida, si bien un agente encubierto operando en el ámbito de la lucha contra el crimen organizado, puede llevar a cabo filmaciones en espacios privados. Esto mismo sería admisible en España. En USA, algunos tribunales federales han admitido que se instalen aparatos ocultos de grabación tanto de imagen como de sonido en el domicilio del sospechoso, sin necesidad de autorización judicial si en el momento de las grabaciones se encuentra presente un informante. No obstante, en algunos estados USA esta misma medida se somete a previa autorización judicial[62].

En Croacia y Bélgica se autoriza, previa resolución judicial, la filmación en espacios privados con medida excepcional con el fin de obtener pruebas y solo en relación con un limitado listado de delitos graves. Finlandia e Italia también contemplan esta medida, si bien en Italia, en virtud de una sentencia del Tribunal Constitucional italiano, sólo puede autorizarse en relación con conductas comunicativas, pero no pueden ser grabadas conductas no comunicativas. En todo caso, parece que las grabaciones como regla no tendrán eficacia probatoria.

Finalmente, en cuanto al papel que desempeñan sujetos o entidades privadas en la ejecución de la medida de vídeo vigilancia, es preciso abordar dos cuestiones. La primera, si pueden verse obligadas a cooperar con las autoridades policiales en el desarrollo de la videogivilancia. Y la segunda, si las personas o entidades privadas pueden realizar actuaciones de vídeo vigilancia por sí mismas, y en ese caso, si estarían obligadas a entregar a la policía las imágenes obtenidas en caso de ser requeridos para ello y si esas grabaciones tendrían eficacia probatoria.

En primer lugar, la cooperación de personas o entidades privadas con las autoridades policiales en materia de vídeo vigilancia puede adoptar diversas formas. Por ejemplo, la policía podría solicitar a personas físicas o jurídicas permiso para utilizar su domicilio o sus locales porque desde los mismos podría efectuarse en mejores condiciones la vídeo vigilancia del domicilio del sospecho o del espacio público en el que el sospechoso suele pasar el tiempo. La cooperación podría consistir también en obtener la autorización del dueño de un edificio privado para colocar cámaras de vídeo vigilancia en su fachada; i en permitir el acceso a un determinado ordenador con el fin de activar el funcionamiento de la webcam para realizar grabaciones de manera oculta; o utilizar satélites de empresas privadas para tomar imágenes y vigilar actuaciones en un concreto territorio, como se hace con frecuencia en el ámbito de la seguridad nacional y de las actuaciones de defensa, para las cuales los ministerios de defensa utilizan sus propios satélites. Además de las mencionadas, cabe imaginar muchas otras formas de cooperación, como por ejemplo, pedir la colaboración de un individuo para que porte una cámara oculta y realice grabaciones en espacios públicos o privados.

En definitiva, todos estos ejemplos muestran cómo la obligación de cooperación por parte de sujetos privados en la realización de actuaciones de video vigilancia con fines de un proceso penal, dependerá del tipo de colaboración que se requiera y si la misma está legalmente prevista o no. No obstante, los informes nacionales no entran en tanto detalle. La mayoría señala que en sus ordenamientos jurídicos no se contempla una obligación de las personas o entidades privadas de colaborar en el desarrollo o ejecución de la vídeo vigilancia. La excepción parece ser Turquía en cuya legislación se establece que los dueños de cibercafés están obligados a instalar cámaras de vídeo vigilancia en sus locales y grabar el área de acceso a los servicios de internet, aunque esta medida se enmarca en el ámbito preventivo y no tanto en de la investigación procesal penal. Los informes no señalan otro tipo de cooperación en materia de vídeo vigilancia, si bien los sujetos privados pueden ser obligados a aportar imágenes que voluntariamente hayan tomado y que sean relevantes para la investigación y prueba penal. Esa obligación habría de formalizarse como una orden judicial de aportación de ese material videográfico.

---

[61] Las posiciones adoptadas en relación con la protección del derecho a la privacidad en espacios públicos son muy diversas, al igual que la definición de lo que sea "espacio público" a estos efectos. Al respecto, vid., por ejemplo, G. Paolo, pp.221 ss.

[62] Siguiendo el voto discrepante de los jueces Harlan y Douglas en la sentencia del Tribunal Supremo norteamericano *United States v. White*, 401 U.S. 745(1971), tal y como se señala en el informe USA, p.52.

3. (5) ¿Pueden o deben los agentes policiales y de seguridad grabar los interrogatorios de sospechosos o testigos en vídeo?

Muchos de los rapports nacionales indican que las normas sobre interrogatorios policiales contemplan la posibilidad de grabación audio-visual de los mismos, pero en general no es obligatorio que se graben los interrogatorios ni con sospechosos ni con testigos. Por ejemplo, en Finlandia, desde 2004, las autoridades policiales pueden grabar en video todos los interrogatorios, de manera completa o parcial, pero están obligados a grabar los interrogatorios a la víctima, así como a los testigos que sean vulnerables o que podrían no estar disponibles en el futuro para testificar en el juicio.[63] En los Estados Unidos no existe ninguna obligación a nivel federal, pero algunos estados establecen que se grabe obligatoriamente los interrogatorios a sospechosos (p. ej., Missouri, desde 2009), y otros estados incluso requieren que se excluya la confesión que no fue grabada digitalmente.[64] En la práctica, aunque en muchos estados no exista una obligación legal al respecto, se tiende cada vez más a grabar los interrogatorios a sospechosos que se encuentran detenidos. Croacia exige que el primer interrogatorio a un sospechoso sea grabado audio-visualmente (art. 275.2 CPC) y contempla también la obligación de grabar en video la confrontación entre testigos realizada en la fase de instrucción, así como los interrogatorios de testigos que se realizan mediante intérprete. Italia y Turquía también establecen la obligatoriedad de la grabación audio-visual del interrogatorio que se efectúe al detenido sospechoso fuera de una vista oral. En los países donde no existe la obligación de grabación audio-vidual la praxis varía enormemente; en algunos, esta medida se utiliza con frecuencia (Austria, USA), mientras que en otros el uso de ese procedimiento no es uniforme o es incluso casi desconocido (Colombia, Argentina, España). El rapport nacional de Brasil es el único que señala la ausencia de prescripción legal a este propósito, aunque esa prescripción se incluye en el proyecto de ley sobre interrogatorios policiales.

Mientras que la videograbación de declaraciones sumariales de adultos difiere mucho según los países, en relación con el interrogatorio de menores se hace notar en muchos rapports nacionales que es obligatorio cuando los menores han sido víctimas de delitos, sobre todo en el caso de delitos contra la libertad sexual (Argentina, Croacia, Finlandia —según el nuevo CPC que entra en vigor en 2014— y Turquía).

En una sociedad de la información, en la que el uso de TIC está tan presente y tan implantado en todos los ámbitos (económico, social, cultural, jurídico y político), resulta en cierto modo sorprendente que la ley no obligue en todos los países a la grabación audiovisual de las declaraciones sumariales de sospechosos y testigos, y que la mayoría de países continúe recurriendo a transcripciones escritas de esas declaraciones realizadas en la fase de instrucción. Para asegurar la prueba, podría resultar útil hacer la videograbación obligatoria, aunque la grabación automática de todas las declaraciones realizadas en la fase de instrucción puede tener un impacto negativo en el principio acusatorio y en el de la inmediación. Esto quizá explica por qué algunos ordenamientos jurídicos todavía se muestran reticentes a la utilización extensiva de la grabación audiovisual de las declaraciones realizadas con carácter previo al juicio oral, probablemente movidos por el temor de que esas grabaciones puedan terminar por convertir el juicio en un mero expediente que confirme lo efectuado en la fase de instrucción.

4. Las TIC y la prueba

(En las distintas fases: obtención/ almacenamiento / retención / práctica / presentación / y valoración de la prueba electrónica)

4. (1) Existen normas probatorias específicas para los datos obtenidos o relacionados con las TICs?

La utilización de las TIC en la obtención de pruebas en un proceso penal se ha analizado en el epígrafe anterior (3), por ello aquí sólo nos referiremos a la garantía de integridad y admisibilidad de la prueba TIC. Hemos de advertir que las preguntas 2 a 5 de este capítulo se solapan parcialmente de tal manera que si la pregunta general sobre la existencia de normas específicas para las pruebas relacionadas con las TIC se ha respondido en sentido negativo –si no existe una regulación específica–, lo más probable es que las siguientes cuatro preguntas también se respondan en el mismo sentido. Hemos intentado reducir reiteraciones al mínimo, aunque algunas podrán encontrarse.

Sobre la fiabilidad y admisibilidad de las pruebas electrónicas y relacionadas con las TIC se viene discutiendo desde hace mucho tiempo, especialmente por la facilidad con que pueden manipularse y alterarse. En España este asunto ya fue objeto de controversia a finales de los años 70 y principios de los 80, cuando se suscitó por primera vez la admisibilidad de las grabaciones de voz y videográficas. Tradicionalmente los códigos de procedimiento penal del área continental europea enumeraban los medios de prueba que eran admisibles en el proceso penal y como los medios de prueba tecnológicos no se encontraban mencionados en ese listado, en un inicio eran sistemáticamente rechazados, sobre la base de que no eran medios de prueba fiables por ser

[63] Vid. el informe nacional de Finlandia, pp. 5-6.
[64] Vid. el informe nacional USA, p. 66.

fácilmente manipulables. Ese rechazo inicial lentamente fue superándose y la prueba electrónica comenzó a admitirse sobre la base de las normas de la prueba documental[65].

En general, puede afirmarse que la cuestión de la admisibilidad y legalidad de la prueba relacionada con las TIC es un tema que pertenece al pasado. La autenticidad de la prueba habrá de ser analizada y probada si se cuestiona por la parte contraria, pero el argumento de la posibilidad de manipulación ya no conlleva la exclusión de la prueba relacionada con las TIC.

Como ya se ha señalado la legislación procesal de la mayoría de los países no ha sido actualizada debidamente para regular adecuadamente el uso de las TIC en el proceso penal. Y eso sucede también en relación con las normas sobre la prueba. Por ejemplo, Argentina, Bélgica, Brasil, Croacia, Italia, Japón, Turquía y Suecia no tienen una regulación completa sobre la prueba relacionada con las TIC. En este ámbito se aplican los principios generales de presunción de inocencia e *in dubio pro reo,* y las reglas generales sobre admisibilidad, aportación, exclusión y valoración de prueba. Los principios básicos de que la prueba ha de ser pertinente y relevante para el caso, gozar de fiabilidad, y que la prueba ha de practicarse respetando el principio de defensa contradictoria, también son aplicables a la prueba relacionada con las TIC.

La ausencia de normas probatorias específicas en materia de TICs no parece generar una preocupación especial, según se desprende de los informes nacionales. Algunos países, si bien no regulan de manera completa la prueba de TICs, sí contienen normas que contemplan aspectos específicos de las mismas. La mayoría de los países cuentan con una regulación completa de la medida de interceptación telefónica (necesidad de aportar la grabación original íntegra sin cortes, como es el caso de España). Otras normas se refieren a la protección de datos de las bases de datos de ADN, o a la exclusión de prueba cuando el cotejo de las muestras de ADN no se ha efectuado siguiendo un determinado protocolo; o sobre la admisibilidad y valora probatorio de las grabaciones de las declaraciones sumariales de los testigos y el o los acusados.

En definitiva, aunque los informes indican que en sus ordenamientos jurídicos no existen normas sobre la prueba relacionada con las TIC, lo cierto es que la mayoría contiene alguna previsión legal sobre medidas concretas o aspectos concretos sobre las mismas. Y en caso de no contar con esa regulación en la ley, la jurisprudencia ha establecido las pautas a seguir en la admisión, valoración y exclusión de la prueba relacionada con las TIC.

Entre los informes que indican contar con normas específicas para la prueba relacionada con las TIC podemos mencionar los siguientes: en USA se regula con detalle el mantenimiento de la cadena de custodia para preservar la integridad de la prueba electrónica. En Colombia las reglas sobre prueba documental son aplicables a las pruebas TIC. En Finlandia en cuyo sistema no se prevén normas legales sobre la exclusión de prueba, se indica específicamente que las vistas grabadas en vídeo, serán admisibles como prueba. Bélgica dispone de algunas normas sobre el almacenamiento de los datos informáticos. En Holanda, donde tampoco hay una norma general de exclusión de prueba obtenida ilegalmente, sí se contempla la exclusión de las conversaciones telefónicas interceptadas a una persona que goza de una especial protección de la confidencialidad de sus comunicaciones, como es el caso de los abogados. La legislación holandesa dispone de una regulación detallada de las herramientas técnicas que han de aplicarse a la hora de acreditar la fiabilidad probatoria de la prueba electrónica. El código procesal penal de Austria contiene una serie de normas que si bien no se aplican exclusivamente a las pruebas relacionadas con las TIC, sí tienen una especial relevancia respecto de las mismas: así, por ejemplo, los preceptos que regulan la confidencialidad, la protección de datos, o la obligación de destruir ciertos datos interceptados. Además, el informe de Austria señala que el Ministerio de Interior austríaco ha elaborado unas directrices sobre la copia, almacenamiento, grabación, conservación y aseguramiento de la integridad de los datos electrónicos (*Geheimschutzordnung*), con el fin de garantizar el derecho a la protección de datos. China sí prevé normas específicas para la prueba de TIC, en la legislación procesal en materia de delitos que conlleven pena de muerte: en esas normas no sólo se enumeran los dispositivos electrónicos que pueden admitirse como elementos probatorios, sino que también se incluyen disposiciones acerca del almacenamiento de la prueba electrónica, el modo de obtención y el control de la fiabilidad probatoria. De lo indicado en el informe parece deducirse que estas reglas, si bien previstas para la aplicación de la pena de muerte, son aplicables a todo tipo de procesos penales.

4. (2) ¿Existen normas sobre la autenticidad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, hacking) de la prueba relativa a las TIC?

La integridad y autenticidad de los datos relacionada con las TIC tiene un impacto directo en la eficacia probatoria de esos materiales, su fiabilidad y por tanto en su valor probatorio. La prueba electrónica puede ser manipulada, borrada, modificada o sobrescrita con facilidad, de ahí que las normas y protocolos para garantizar la integridad de este tipo de pruebas adquiere una importancia fundamental. Esta afirmación es válida para cualquier tipo de

[65] No obstante, tal como expresa el informe belga, todavía hay algunos tribunales que todavía se muestran reticentes a admitir prueba electrónica e incluso imagines de TV, porque consideran que, al ser susceptibles de manipulación, no son suficientemente fiables (por ejemplo, *Tribunale Correctionnel d'Anvers* de 25.10.2004). Vid el informe sobre Bélgica, p.73.

prueba y los problemas de garantizar la autenticidad y fiabilidad de los elementos probatorios no son nuevos. Ahora bien, en materia de prueba electrónica nos enfrentamos a un problema adicional y es que las medidas tradicionales para garantizar la autenticidad de la prueba no son adecuadas cuando se trata de datos informáticos o electrónicos que pueden fácilmente ser borrados, destruidos o manipulados, y con frecuencia, sin dejar rastro de esa manipulación. Esta es la razón por la cual las medidas de aseguramiento y confiscación de datos electrónicos son esenciales, utilizando por ejemplo, el dispositivo de bloque de escritura (*write-blocker*), para evitar alteraciones en los datos originales; o mediante la creación de una copia perfecta "bit a bit" de los datos almacenados.

Para probar la integridad de la prueba digital debería acreditarse: 1) que la información digital obtenida de un dispositivo o soporte as una verdadera y precisa representación de los datos contenidos en ese dispositivo (autenticidad); 2) que el soporte y los datos que se aportan como prueba en el juicio son los mismos que fueron originariamente descubiertos y que son los que quedaron custodiados (integridad)[66].

Los informes que manifiestan tener ciertas normas sobre la garantía de la integridad de las pruebas relacionadas con TIC son: Colombia, Croacia, Italia, Holanda, y USA). Así, en Holanda se prevé específicamente cuáles son las herramientas técnicas que habrán de emplearse para proteger la trazabilidad de los datos así como para evitar el riesgo de su alteración (art. 126 Decreto de 2006 sobre herramientas técnicas en el proceso penal)[67]. Si esas normas no se han respetado, el tribunal directamente excluirá la prueba sobre la base de falta de fiabilidad técnica. China tiene una serie de normas sobre obtención, almacenamiento, conservación y copiado de pruebas relacionadas con las TIC. Colombia indica que en ese país se utilizan los formatos SHA-1 y SHA-256 para garantizar la autenticidad de la prueba electrónica. En Italia, el órgano judicial puede ordenar que se apliquen controles técnicos y medidas de aseguramiento para preservar la integridad digital de la prueba electrónica, a pesar de que la ley no regula cuáles han de ser esas medidas. Croacia tiene normas específicas para la prueba electrónica y para la presentación de las grabaciones de declaraciones previas en el juicio oral. En Estados Unidos existe una completa regulación normativa dirigida a preservar la cadena de custodia, y la parte que propone la prueba, ha de probar a su vez que se ha respetado la normativa y la continuidad de la cadena de custodia[68].

La integridad de la prueba es una cuestión típicamente fáctica, mientras que el mantenimiento de la cadena de custodia se refiere al proceso seguido en el mantenimiento y documentación de la historia cronológica que ha seguido un elemento de prueba, al ser trasladado de un lugar a otros[69]. Finalmente, algunos países afirman tener ciertas normas generales en materia de cadena de custodia probatoria, y en particular en relación con las pruebas de ADN, pero no específicamente con las pruebas relacionadas con las TIC (Brasil, España).

4. (3) ¿Existen normas específicas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas relacionadas con las TIC?

La respuesta de los informes a esta pregunta es unánime: no existen normas específicas sobre la admisibilidad de las pruebas relativas a TIC, aplicándose a este tipo de pruebas las reglas generales sobre exclusión de prueba. El informe de Colombia señala que las pruebas relacionadas con TIC han de revestir una apariencia de autenticidad e integridad, por ejemplo, acreditando que se han respetado los estándares y principios que utiliza el FBI o el grupo de trabajo sobre la prueba digital (SWEDGE, *scientific working group on digital evidence*). No obstante no resulta fácil determinar si el respeto de esos protocolos constituye un presupuesto de admisibilidad de la prueba o si se trata de criterios a tomar en consideración a la hora de valorar la fiabilidad de la prueba y por tanto, conferirle mayor o menor credibilidad.

Si se tiene en cuenta que con frecuencia la prueba electrónica o digital habrá de ser obtenida en el extranjero, sin duda la existencia de normas comunes sobre obtención de prueba, tal y como ya se ha mencionado más arriba, sin duda facilitaría su admisión por parte del tribunal del estado del foro[70]. Pero, como esa armonización no resulta fácil de alcanzar, y menos aún a nivel global, sería deseable que se establecieran ciertos principios o estándares aplicables a la prueba en procesos penales transnacionales. Con ello se evitaría o limitaría el riesgo de que la prueba obtenida en el extranjero, finalmente no fuera admitida por el tribunal del foro, con el argumento

[66] UNODC *Comprehensive Study on Cybercrime*, p. 158.
[67] Vid. el informe nacional de Holanda, p.24.
[68] Acerca de la prueba digital, su utilización procesal, y la necesidad de acreditar su integridad y la continuidad en la cadena de custodia, vid. *Digital Evidence in the Courtroom: A guide for Law Enforcement and Prosecutors*, del Departamento de Justicia de los USA, publicado por el National Institute of Justice en 2007, p. 16, accesible en https://www.ncjrs.gov/pdffiles1/nij/211314.pdf.
[69] Vid. E. Casey, *Digital Evidence and Computer Crime: Forensic Science and the Internet*, New York 2011, citado en el UNODC *Comprehensive Study on Cybercrime*, p. 158.
[70] Una breve resumen de los problemas relativos a la obtención y admisibilidad de la prueba en procesos europeos transfronterizos vid. M. Simonato, pp.18 ss.

de que no se ajusta a la normativa procesal nacional[71]. El "principio" de que una regulación diferente no debería por sí misma ser un motivo para denegar la admisibilidad de prueba obtenida en el extranjero, ha sido incluido en la Propuesta de Reglamento para la creación de un Fiscalía Europea, con el fin precisamente de evitar la problemática que se suscita en la transmisión y admisibilidad de la prueba transfronteriza[72]. El cuestionario que se remitió a los rapporteurs nacionales no aludía específicamente a la admisibilidad de prueba obtenida o localizada en otro estado, por lo que aquí sólo podemos subrayar la importancia de elaborar principios generales para la prueba transnacional y también para la prueba relacionada con TIC, que no sólo tiene una importancia creciente en el enjuiciamiento de todo tipo de delitos, sino que además tiende a tener una dimensión transnacional[73].

4. (4) ¿Existen reglas específicas sobre la obligación de aportar y revelar prueba relacionada con las TIC?

En general, todos los informes nacionales expresan que no hay una regulación específica para la aportación de prueba relacionada con las TIC y que se aplican las normas generales sobre acceso a los autos y el derecho a examinar la prueba que aporta el ministerio fiscal u otros acusadores. Por las respuestas contenidas en los informes se deduce que están referidas a la aportación y revelación de prueba no-clasificada, puesto que ninguno de los informes –salvo el de USA–, menciona la posibilidad de limitar el acceso por parte de la defensa a determinadas pruebas, con el fin de proteger a la fuente o para evitar un riesgo para la posición de la acusación, en caso de revelar esas pruebas. Por ello, las respuestas a esta pregunta han de interpretarse como referidas a los supuestos ordinarios, y no a las normas o previsiones específicas en materia de información reservada, clasificada o secretos de estado.

En USA, las interceptaciones y registros secretos realizados bajo las normas de FISA (*Foreign Intelligence Surveillance Act*) habrán de ser reveladas a la parte contraria, a menos que el gobierno alegue que la aportación de escuchas telefónicas, comunicaciones electrónicas o imágenes de vídeo, podrían constituir una revelación de secretos de estado o de información clasificada. En tales casos, el tribunal deberá aplicar la normativa contenida en la legislación específica sobre protección de información clasificada, que permite privar a la defensa del acceso a esos datos, siempre que se le provea de un resumen de su contenido o se celebre una audiencia *in camera* con un abogado defensor autorizado[74].

4. (5) ¿Existen normas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?

Todos los informes nacionales señalan que no existen reglas especiales para la valoración de la prueba relacionada con las TIC, aunque resulta interesante observar cómo en los USA se aplican las reglas de exclusión de prueba aplicables a la prueba obtenida fuera del juicio o *hearsay evidence* a toda prueba obtenida mediante TIC, tal y como se verá en el siguiente epígrafe.

5. Las TIC en la fase de juicio

5. (1) ¿Cómo puede o debe presentarse en el juicio la prueba relacionada con las TIC?

La cuestión que se plantea aquí es ciertamente amplia, pues se refiere a la manera en que deben presentarse en juicio las pruebas relacionadas con las TIC, sin distinguir entre los deferentes tipos de información o prueba que se han obtenido o grabado mediante el uso de TIC. En este plano general, y centrándonos solamente en "cómo" la prueba ha de ser presentada en juicio, todos los rapports nacionales, excepto el de Estados Unidos, bien se remiten a las normas sobre prueba documental, o bien indican que la prueba grabada en cinta o film, o guardada en un ordenador, se presentará reproduciendo tales grabaciones o mostrando el ordenador con los datos correspondientes ante el tribunal. Además, las cintas de audio y los datos informáticos pueden ser acompañados de su transcripción escrita, aunque no resulta claro si esas transcripciones son siempre obligatorias o no. Si la prueba relacionada con TIC consiste en una filmación, los rapports de la mayoría de los países relatan que puede ser reproducida en la sala de juicios. Algunos países, como China, exigen que se presente en el juicio el archivo donde se contiene el documento original y, si se discute su autenticidad, el experto habrá de acreditar la

[71] Sobre esta materia vid. los trabajos que se publican en el volumen colectivo "Law Should Govern: Aspiring General Principles for Transnational Criminal Justice" *Utrecht Law Rev,*Volume 9, Issue 4, Special Issue, Sept 2013. En particular, vid. la nota de los editores de S. Gless y J. A.E. Vervaele, pp. 1-10, pp. 4 ss., accesible en *http://www.utrechtlawreview.org/index.php/ulr/article/view/URN%3ANBN%3ANL%3AUI%3A10-1-112945/233*.

[72] Vid. art. 30 de la Propuesta de Reglamento del Consejo relativa a la creación de una Fiscalía Europea, COM(2013) 534 final of 17.7.2013

[73] Sobre la prueba transfronteriza en particular, vid. S. Gless, *Grenzüberschreitende Strafverfolgung*, Baden-Baden, 2006; T. Krüssmann, *Transnationales Strafprozessrecht*, Baden-Baden, 2009; y para un estudio empírico sobre esta materia a nivel de la Unión Europea vid. G.Vermeulen, W. De Bondt, Y.Van Damme, *EU cross-border gathering and use of evidence in criminal matters. Towards mutual recognition of investigative measures and free movement of evidence?*, Antwerpen, 2010; y más recientemente S. Ruggeri (ed.) *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, Berlin-Heidelberg, 2013.

[74] Vid. el informe nacional USA, p. 69.

autenticidad de la prueba electrónica. Por otro lado, las autoridades que manejaron los datos o materiales grabados podrán ser interrogadas acerca del modo en que fueron obtenidos y las condiciones en fueron conservados, así como sobre las normas aplicadas para preservar la cadena de custodia.

Los Estados Unidos tienen un planteamiento diferente, debido a sus normas específicas sobre la prueba practicada fuera del juicio y la basada en el testimonio de referencia (*hearsay*). En este país, *hearsay* se define como la declaración, ya sea oral o escrita, o incluso realizada mediante gestos, que se formula fuera del juicio pero es introducida en el mismo para probar la verdad de lo que se afirma[75]. En consecuencia, cualquier declaración hecha fuera del juicio, ya sea resultado de un interrogatorio o de una interceptación legal de comunicaciones, es considerada prueba de referencia o *hearsay*. La regla general en Estados Unidos es que los materiales grabados serán presentados en juicio a través de declaración de testigos. Para que una grabación de sonido o imagen, o el registro de las comunicaciones que realizan las compañías proveedoras de servicios de telecomunicación sea admisible como prueba, los agentes al cargo de la grabación u operación de interceptación, deberán testificar acerca de cómo se llevaron a cabo esas intervenciones, acerca de la cadena de custodia y, en general, acerca de las garantías adoptadas[76]. No obstante, la legislación estadounidense contempla numerosas excepciones a la inadmisibilidad de *hearsay*. Por ejemplo, las declaraciones grabadas en audio-video pueden ser reproducidas directamente en juicio, como en el caso de las declaraciones realizadas por menores que han sido objeto de abusos sexuales.

Si entramos en más detalles, habría de explicarse aquí en qué circunstancias las declaraciones realizadas y grabadas en la fase de instrucción pueden reproducirse o leerse en el juicio oral. Ninguno de los rapports nacionales, con excepción de Estados Unidos, informa de las condiciones que permiten la presentación de declaraciones filmadas durante la instrucción, o la lectura de las transcripciones de esa clase declaraciones hechas por las víctimas, los acusados o los testigos. En el proceso penal norteamericano, las declaraciones de testigos grabadas en la fase de instrucción son admisibles de manera excepcional y entre esas excepciones se encuentran las denominadas de "*excited utterance*" o declaración realizada en un determinado estado emocional, la excepción de "*present sense impression*" o relativas a impresiones momentáneas, las declaraciones a propósito de tratamientos médicos, o relativas a condiciones físicas, emocionales o mentales, y las actas o datos relativos a actividad empresarial, que se consideran más acertados que lo que pueda declararse sobre esos hechos pasado un tiempo. Aplicando dichas excepciones, los tribunales han aceptado como prueba, por ejemplo, las declaraciones grabadas de una mujer que había realizado una denuncia a la policía por teléfono mientras era golpeada por su marido, si no le era posible testificar en juicio.

Para una mejor apreciación de la función de las TIC como prueba, sería necesario analizar también cuáles son las circunstancias que permiten escuchar y/o contemplar las declaraciones grabadas en la fase de instrucción, y en qué condiciones pueden ser valoradas como prueba. Sería interesante examinar si la confesión grabada durante la instrucción puede ser admitida en juicio cuando un acusado decide permanecer en silencio en la sala de juicios, o cuando un testigo invoca durante el juicio su derecho a no declarar como testigo después de haber testificado en la fase de instrucción.

De la información proporcionada por los rapports nacionales pueden deducirse algunas conclusiones claras. Primero, hay todavía muchos países que no tienen normas específicas para la presentación de pruebas relacionadas con TIC en el juicio, y se limitan a utilizar las normas tradicionales sobre prueba documental, aunque éstas no siempre resultan plenamente aplicables. Segundo, debería indicarse de manera precisa cómo deberían presentarse las prueba relacionadas con las TIC, aclarando cuándo y en qué medida habrían de exigirse transcripciones escritas (que a veces son costosas y llevan tiempo). Finalmente, sería deseable que las normas jurídicas sobre presentación de pruebas relacionadas con TIC especificaran cuándo se ha de dar preferencia a la reproducción de una filmación o escuchar una grabación de audio ante el tribunal, en lugar de escuchar el testimonio de las autoridades que intervinieron en dichas grabaciones, o en lugar de leer las transcripciones escritas de dichas grabaciones. En suma, puede afirmarse que, cuando la fuente directa de la prueba no puede ser escuchada en el juicio, sería preferible visionar o escuchar las declaraciones grabadas durante la instrucción, más que hacer testificar a los agentes que interrogaron a los testigos o leer la transcripción de sus declaraciones: una grabación de video –como regla general, si bien también puede implicar riesgos– parece una opción mejor y más precisa, pues permite al juez o al jurado una más directa valoración de esas declaraciones. Somos conscientes de que esta opción es ajena a la práctica procesal angloamericana, pero quizá habría de reconsiderarse ese aspecto de su tradición a la luz de los avances en materia de TIC.

5. (2) ¿Pueden realizarse interrogatorios a distancia (por ejemplo, a través de conexiones vía satélite)?

La respuesta general en todos los informes nacionales es que los interrogatorios a distancia son posibles en el proceso penal. Sin embargo, ha de distinguirse a este propósito entre acusados y testigos. Se da aquí por

[75] Vid. el rapport nacional de Estados Unidos, p. 69.
[76] Vid. el rapport nacional de Estados Unidos, p. 67.

sentado que los rapports nacionales que no hacen esa distinción se refieren sólo a los testigos, ya que la mayor parte de los países no aceptan, como norma general, la celebración de un juicio sin la presencia física del acusado. Pese a ese planteamiento general, y puesto que hay países que excepcionalmente permiten la comparecencia del acusado en juicio mediante videoconferencia o teleconferencia, me referiré a esas dos situaciones por separado.

El derecho de casi todos los países estudiados prevé diversas maneras de que un testigo pueda testificar a través de *video-link* o videoconferencia; esta posibilidad se utiliza normalmente para testigos cuya comparecencia física no es posible, es excesivamente gravosa o cuando se trata de testigos que están en el extranjero. Es el caso de Austria (art. 247a CPC), Bélgica, Colombia (art. 386, después de la Ley 906/2004), Croacia, España, Finlandia, Holanda, Italia y Turquía. Debe hacerse notar que el Convenio relativo a la Asistencia Judicial en Materia Penal entre los Estados Miembros de la Unión Europea, de 29 mayo 2000[77], contempla expresamente la posibilidad de oír el testimonio de testigos por videoconferencia, y no excluye la videoconferencia en el juicio (art. 10)[78]. La misma prescripción se incluye en el art. 9 del Segundo Protocolo Adicional al Convenio Europeo sobre Asistencia Mutua en Materias Penales elaborado dentro del Consejo de Europa[79]. Este Segundo Protocolo al Convenio Europeo de 1959 sigue de cerca, y a menudo literalmente, el antes citado Convenio de 2000 de la Unión Europea, sobre asistencia judicial internacional[80]. Por consiguiente, en los 47 Estados miembros del Consejo de Europa debería ser posible oír por videoconferencia a los testigos que se encuentran en el extranjero[81]. En contraste con el panorama pan-europeo, esa posibilidad no existe en Japón.

Además de para los testigos que se encuentran en el extranjero, muchos de los países estudiados autorizan también el uso de videoconferencia cuando un testigo está bajo un programa especial de protección de testigos (p. ej., España, Holanda, Italia o Turquía), o bien cuando no es factible —o resulta demasiado dificultoso— hacer que el testigo comparezca físicamente ante el tribunal. El interrogatorio de testigos mediante videoconferencia se promueve e impulsa también dentro de la UE[82].

Por otro lado, como se ha explicado antes, hay normas especiales para los menores que han sido víctimas de delitos sexuales. En tales supuestos, muchos países no sólo contemplan la posibilidad de que el menor declare mediante videoconferencia, sino que hacen obligatoria la grabación de las declaraciones durante la instrucción. Incluso en un sistema como el de los Estados Unidos, donde la aplicación del principio contradictorio o *confrontation clause* se concibe de manera muy estricta, los tribunales han aceptado la utilización de un circuito cerrado bidireccional de televisión, para evitar que un testigo menor de edad tenga que comparecer en juicio y confrontar al acusado. Se considera que en este caso una poderosa razón de interés público justifica la excepción. Nueva York tiene una ley que permite a los menores víctimas de abusos sexuales testificar por video, y la Corte Suprema de ese estado ha admitido la posibilidad de aplicar esta norma excepcional a otros casos, como el de una víctima de 83 años, que estaba demasiado débil como para comparecer físicamente en el juicio.

Por lo que concierne al acusado, la norma general es que no puede celebrarse el juicio sin su presencia física, y muchos países son reticentes a cambiar esta norma, por los riesgos que podría comportar para los derechos de defensa del acusado. La presencia del acusado se considera un elemento esencial para la adecuada valoración de la prueba y el respeto del derecho de contradicción, además de una condición *sine qua non* para la tutela de los derechos de defensa. Por esa razón, y a pesar de los espectaculares avances técnicos, sólo unos pocos países han abierto de momento las puertas a la posibilidad de que comparecencia del acusado en juicio tenga lugar mediante videoconferencia. Según los rapports nacionales, China, España, Holanda, Italia y Turquía, prevén la posibilidad de oír al acusado mediante video-link. En China, dicha posibilidad se reserva a los procedimientos de apelación y revisión, y parece ser utilizada ampliamente en la práctica, debido a la dimensión geográfica del país. En Italia, donde los juicios *in absentia* son aceptados de manera excepcional, la ley contempla que el acusado pueda comparecer por video-link cuando hay serias razones de seguridad. Esta norma está pensada para delitos relacionados con la mafia, en los que la complejidad del delito, los graves riesgos para la seguridad y

---

[77] Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:ES:PDF

[78] Sobre el uso de la videoconferencia en la cooperación judicial internacional vid., por ejemplo, T. Hackner & C. Schierholt, *Internationale Rechtshilfe in Strafsachen,* München 2012, p. 203. Vid. también K. Ambos, *Principios del proceso penal europeo. Análisis de la Convención Europea de Derechos Humanos,* Bogotá 2005, p. 90 y la bibliografía allí citada; y para su utilización en España, vid. A. Montesinos García, *La videoconferencia como instrumento probatorio en el proceso penal*, Madrid 2009, pp. 65-70.

[79] Disponible en http://conventions.coe.int/Treaty/en/Treaties/Html/182.htm.

[80] Aunque en ocasiones sigue el Convenio de 14 junio 1990 para la implementación del Acuerdo de Schengen de 14 junio 1985. Vid. la Exposición de Motivos de este Segundo Protocolo, n. 9.

[81] En relación con cuestiones prácticas actuales sobre videoconferencias transnacionales en la UE, vid. el Documento del Consejo No. 16269/13, p. 6, citado por D. Brodowski en su rapport *European Initiatives Concerning the Use of IT in Criminal Procedure and Data Protection. Special report for the Preparatory Colloquium for the Third Section*, nota 43.

[82] Vid. *Videoconferencing as a part of European e-Justice*, 2009, disponible en https://e-justice.europa.eu/attachments/vc_booklet_en.pdf.

los riesgos de fuga, pueden justificar que el acusado no sea llevado ante el tribunal, sino que permanezca custodiado en prisión y desde allí siga todo el proceso mediante video-link. Turquía permite que el acusado comparezca por videoconferencia solamente para la vista en la que ha de decidirse sobre la prisión preventiva, pero no para el juicio propiamente dicho. En España, donde también está vigente la misma norma general de que no puede haber juicio sin la presencia física del acusado, en casos excepcionales de terrorismo en los que el comportamiento de los acusados obstaculiza el normal desarrollo del proceso, los tribunales han admitido que el acusado que altera el orden en la sala, sea trasladado a una sala adyacente equipada con video-link. Esta solución no estaba explícitamente prevista por la legislación, pero fue adoptada por los tribunales por su propia iniciativa, y más tarde fue declarada constitucional por el Tribunal Constitucional español.

5. (3) ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (por ejemplo, asesinatos, accidentes de tráfico)?

Todos los rapports nacionales indican que las técnicas digitales y virtuales pueden ser empleadas para reconstruir hechos, aunque en muchos países esta posibilidad no es objeto de una regulación precisa. Es el caso de, por ejemplo, Argentina, Brasil, Croacia, España, Finlandia, Italia, Japón, Suecia y Turquía, donde no existe regulación expresa, pero la reconstrucción virtual de los hechos se permite en la medida en que no esté prohibida, o dependiendo de que las normas tradicionales sobre reconstrucción de hechos no establezcan cuáles son los instrumentos o aparatos que han de ser utilizados, o excluidos, en un concreto medio de investigación o prueba (como, por ejemplo, la regulación de la *Tatenrekonstruktion* en Austria, arts. 149-150 CPC). Varios rapports nacionales señalan que la regulación de la reconstrucción de hechos no se contiene en el CPC sino en las normas sobre la actuación de los peritos judiciales (p. ej., Croacia y Turquía).

5. (4) ¿Pueden utilizarse medios audiovisuales para presentar pruebas en el juicio (en su forma más básica: imágenes y sonido)?

Esta cuestión ya se respondió en parte en el apartado correspondiente a la cuestión (5)1, al abordar el tema de la presentación en juicio de la prueba relacionada con las TIC. Aquellos informes nacionales que contestaban que dichas pruebas pueden presentarse mediante la reproducción del la filmación o la escucha de la grabación de audio, también responden esta cuestión de manera afirmativa. No obstante, la presente cuestión va más allá de lo que plantea la cuestión (5)1, pues se refiere concretamente al uso de técnicas audiovisuales para presentar pruebas en general, y no sólo pruebas relacionadas con TIC.

De la lectura de los rapports nacionales se extrae la conclusión de que las técnicas audiovisuales pueden emplearse para presentar pruebas en el juicio, ya sea porque no está prohibido —es la mayoría de los casos— o porque está expresamente previsto por la ley. En la práctica, la utilización de estas técnicas difiere mucho de un país a otro, así como dentro de un mismo país la praxis varía dependiendo de los tribunales. La mayor parte de los rapporteurs observan que su uso depende, en última instancia, de la existencia de equipos adecuados (p. ej., España o Japón), del tipo de prueba (si la técnica audiovisual es necesaria o no), y de la complejidad del caso. En los países de Europa continental, a menos que la clase de prueba requiera estrictamente la reproducción de una filmación, la escucha de una grabación de audio o la presentación de sistemas, programas o datos informáticos, los abogados no suelen recurrir a técnicas audiovisuales o a presentaciones de tipo PowerPoint en su actividad de defensa del acusado. En este ámbito, la práctica forense de los Estados Unidos parece más adaptada al uso de modernas tecnologías en la sala de juicio. El número de salas de juicio que han sido certificadas como *high technology courtrooms* ha aumentado con rapidez, y, para 2003, la tecnología de video bidireccional se encontraba autorizada en 29 estados. Además, los abogados frecuentemente utilizan TIC y presentaciones de diapositivas tipo PowerPoint no sólo para sus alegaciones o para explicar la prueba, sino también para exponer y resumir sus conclusiones finales.

5. (5) ¿Pueden sustituirse los expedientes procesales penales en "papel" por los electrónicos? ¿Se ha avanzado hacia la digitalización de los procesos judiciales?

En el momento de escribir este rapport general, ninguno de los países cubiertos de los que disponemos informes nacionales había avanzado en la implementación de la justicia electrónica o *e-justice* lo suficiente como para sustituir completamente los expedientes en papel por archivos electrónicos. Al mismo tiempo, con la excepción de Japón, todos los rapports nacionales señalan que se han aprobado programas de digitalización que deberían llevar progresivamente a una transición gradual hacia los archivos judiciales electrónicos; sin embargo, no se ofrecen muchos datos sobre la efectiva implementación o progreso de esos programas. Bélgica reguló los procedimientos electrónicos por Ley de 10 julio 2006, junto con el proyecto "Phenix", con vistas a realizar la transición hacia la justicia digitalizada. Dicha ley establecía un principio peculiar: cada expediente debería ser íntegramente electrónico o íntegramente en papel, sin admitir la digitalización por partes del expediente, y rechazando también la posibilidad de tener una versión del expediente en papel junto a la versión electrónica. El proyecto no sólo era complicado, sino que exigía una enorme inversión económica, de ahí que terminara por resultar fallido. Pese a todo, el Ministerio de Justicia aprobó otro proyecto que debería ser implementado para

2015. Otros rapports nacionales dan cuenta de problemas análogos en la digitalización de la administración de justicia.

Los Estados Unidos, de nuevo, parecen más avanzados en el uso de TIC y modernas tecnologías en el sistema judicial. El rapport norteamericano indica que los abogados usan de manera habitual programas de archivo y gestión de casos electrónicos, registro electrónico de los plazos, las audiencias, vistas, etc., además de sistemas de gestión de casos *on line*. La comunicación entre el tribunal y los abogados también suele realizarse de manera general por correo electrónico. Actualmente se discute sobre la conveniencia de introducir los juicios virtuales, pero sin que ello conlleve una restricción del derecho a un juicio contradictorio y del derecho a confrontar a los testigos. Hasta el momento, por lo que nos consta, este asunto ha sido solamente objeto de debate, y será el futuro el que muestre si llega a hacerse realidad.

En cuanto a la digitalización parcial, la mayoría de los rapports nacionales indica que se camina decididamente hacia una administración de justicia digitalizada o *e-justice,* al menos en algunas áreas, ciertos actos judiciales o algunas fases del proceso. Muchos han comenzado por digitalizar algunos documentos e información (a nivel de la UE, puede verse el portal *e-justice*). Otros países ya han avanzado en la digitalización de las decisiones del Tribunal Supremo o de Tribunales Superiores, mientras que otros cuentan ya con todas las sentencias en formato digital. Este es, sin duda, un importantísimo avance, pero no es aún suficiente para hablar de justicia electrónica, sino más bien un modo de mejorar el acceso a la información mediante el recurso a bases de datos electrónicas.

El rapport de Austria relata que la digitalización se ha implementado a nivel de la policía y también en relación con los casos de la Corte Constitucional. Holanda ya contempla la posibilidad de presentar electrónicamente denuncias de delitos de menor importancia ante la policía. En España también se pueden denunciar electrónicamente algunos delitos. Italia ha digitalizado un gran número de documentos, y en España los abogados disponen de la posibilidad de presentar documentos y recibir notificaciones electrónicamente, ya sea directamente o mediante un representante ante el tribunal (procurador). A nivel de la UE, hay un reciente proyecto piloto dirigido a digitalizar ciertos procedimientos de cooperación internacional, en concreto los relativos a los mandamientos de detención y arresto europeos, que comprende inicialmente a Francia, Alemania y España[83].

En definitiva, puede decirse que hay muchos programas y planes de actuaciones que tienen por objeto la digitalización de los procedimientos judiciales, pero la realidad muestra que la administración de justicia electrónica, el expediente judicial electrónico y los procedimientos electrónicos son todavía una realidad lejana. Este débil y lento progreso contrasta notablemente con la digitalización que ha tenido lugar en otras administraciones públicas, como en las agencias tributarias o en los procedimientos administrativos. Frecuentemente se alude a cuestiones relativas a la seguridad informática y a peligros para la confidencialidad como argumento para no avanzar de manera firme hacia la completa digitalización de los archivos judiciales que contienen no sólo datos personales, sino datos que son a menudo sensibles y confidenciales. Desde la perspectiva de la defensa, la digitalización de los procesos podría facilitar el acceso al expediente[84], especialmente en casos complejos y voluminosos en los que ha de manejarse una enorme cantidad de documentos. También beneficiaría una gestión más eficiente de los casos, pues permitiría también reducir visitas al tribunal, por parte de los abogados o sus representantes, con el consiguiente ahorro de trabajo y de tiempo.

[83] Este proyecto piloto se denomina e-CODEX y comenzó a finales de 2013. Vid. el citado rapport de D. Brodowski sobre la UE, p. 8.

[84] Vid. M. Simonato, p. 32, citando a K. Strutin, "Databases, E-Discovery and Criminal Law", en *Richmond Journal of Law & Technology*, vol. XV, issue 3, p. 1 ss.; y D.B. Garrie – D.K. Gelb Garrie D.B. – Gelb D.K., "E-Discovery in Criminal Cases: A Need for Specific Rules", en *Suffolk University Law Review*, 2010, vol. 43, p. 393 ss.