REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

NÚMERO 1 - AGOSTO, 2016

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

SUMARIO

PRESENTACIÓN

Este número inicial de la *"Revista Uruguaya de Protección de Datos Personales"* expresa la iniciativa de la Unidad Reguladora y de Control de Datos Personales de encarar una nueva vía de difundir los derechos que garantiza el régimen de la ley Nº 18.331 de 11 de agosto de 2008 e incentivar su conocimiento y debida aplicación.

Con anterioridad se efectuó la publicación en soporte papel o en línea de guías sectoriales (sobre Educación, Salud, Administración y Telecomunicaciones), las Memorias con un balance de la actividad cumplida en el respectivo año así como Libros con resoluciones, dictámenes e informes.

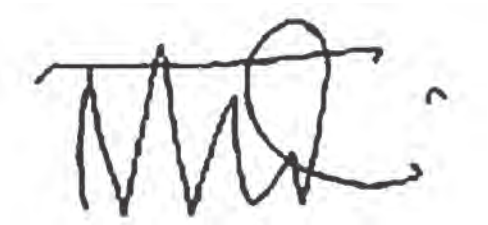
Estas modalidades proseguirán. El camino que se inicia con la Revista no le sustituye sino que procura propiciar, como antes se señaló, un diverso enfoque abierto a los aportes y contribuciones de expertos y conocedores, teóricos y prácticos, sean nacionales o extranjeros, en materia de datos personales y su protección.

También se pretende recoger planteamientos de interés de nuevos estudiosos así como informaciones sobre jurisprudencia, práctica administrativa, comentarios o iniciativas de diverso origen.

Se trata, pues, de una Revista que, sin provenir obviamente de un ámbito científico o académico, pretende abrirse a la comunidad de esa naturaleza y a los sectores sociales en general. Ello comprende los trabajos de estudiantes de distintos niveles educativos, incluso los que la Unidad premia con motivo del concurso *"Tus datos valen"* a nivel de Educación Primaria o Media y de quienes participen, con éxito, en el proyectado concurso académico sobre Protección de Datos Personales.

El Plan de la Revista que se indica a continuación revela lo antes expuesto y se estima que su Número 1 lo hace acabadamente.

En ese sentido, las Secciones serán: Doctrina, Jurisprudencia, Dictámenes de la Unidad, notas de interés y entrevistas.



Dr. Felipe Rotondo Tornaría

Presidente

Consejo Ejecutivo – URCDP

DOCTRINA


CHANTAL
BERNIER


GIOVANNI
BUTTARELLI


CARLOS
DELPIAZZO


MAR
ESPAÑA MARTÍ


PABLO
PALAZZI


XIMENA
PUENTE
DE LA MORA


AHTI
SAARENPÄÄ

EL FUTURO HA LLEGADO

Desafíos de aplicación del derecho a la privacidad a Internet de las Cosas

CHANTAL
BERNIER

Es abogada y se sumó a la práctica de Privacidad y Ciberseguridad de Dentons Canada LLP el 6 de octubre de 2014. Llegó a Dentons luego de 6 años liderando la Oficina del Comisionado de Privacidad de Canada (OPC) como Comisionado de Privacidad Interino así como Comisionado Adjunto. Tuvo a su cargo operaciones del OPC, incluyendo investigaciones nacionales e internacionales en los sectores público y privado, auditorías privadas, revisiones de valoraciones de impacto de privacidad así como análisis tecnológicos, desarrollo de políticas de privacidad e investigación.

SUMARIO

RESUMEN

El desarrollo rápido de la tecnología de la información impone a gobiernos, empresas y juristas una mirada al futuro. Es un desafío especial para los juristas que funden toda interpretación de la ley en precedentes. El derecho de la privacidad presente ese desafío de manera singular: por una parte, la mirada atrás es esencial a la preservación de los principios del derecho a la privacidad establecidos, fundamentales a la libertad y la dignidad humana; por otra parte, la mirada al futuro, con un pensamiento innovador, es esencial para aplicar esos principios inmutables a modalidades de riesgo en constante mutación. La solución reside en una adaptación insertada en la continuidad.

El reto de ese artículo es de proponer unas pistas de adaptación de los principios establecidos del derecho a la privacidad a Internet de las Cosas. En un esfuerzo de clarificación jurídica, aunque en rasgos básicos, de un marco de protección de la privacidad frente al desarrollo de Internet de las Cosas, ese artículo se divide en cuatros partes:

1. la natura general de las transformaciones de las nuevas tecnologías de la información y su impacto jurídico,
2. las características distintas del impacto de Internet de las Cosas,
3. el papel de las autoridades de protección de datos frente a ese impacto,
4. finalmente, interrogaciones sobre la declaración de invalidez de "Safe Harbor" en relación a Internet de las Cosas.

1. LA NATURA DE LAS TRANSFORMACIONES Y SU IMPACTO JURÍDICO

En general, en modernizando el marco jurídico de protección de la privacidad, tenemos que considerar tres fenómenos llaves:

i. El carácter inmutable del derecho a la privacidad contrastando con la mutación profunda de las modalidades de su ejercicio,

ii. El impacto de la abstracción de Internet sobre la noción de autonomía individual, que es la base del derecho a la privacidad, y

iii. La asimetría creciente entre el poder de los individuos frente al poder de las organizaciones que recogen sus datos personales, debida a la capacidad de recopilación, como a la complexidad y opacidad de Internet.

1. 1. Principios y modalidades

La definición del derecho a la privacidad en la jurisprudencia canadiense, quien corresponde a la definición universal, es la "autonomía de una persona a determinar la comunicación de sus datos personales"[1]. El elemento llave, en consecuencia, es el respeto de la autonomía, del control, individual.

Los principios vinculados a ese derecho no han cambiado y no pueden cambiar. Son inmutables como todo derecho humano. Corresponden a una necesidad visceral de proteger la integridad personal y gestionar la supervivencia en sociedad. Esa necesidad es muy anterior e independiente de las específicas leyes codificando el derecho a la privacidad. Es así que el European Data Protection Supervisor (EDPS) impulsa un pensamiento novador basado en la ética y la dignidad humana en su Opinión *Towards a New Digital Ethics ' Data Dignity and Technology.*[2]

En esa Opinión, el EDPS define la base ética de la modernización del marco jurídico de protección de la privacidad. En vinculando dignidad y datos, el EDPS propone un marco jurídico de privacidad que prohíbe la "objetivación de una persona como herramienta al servicio de intereses de un otra".[3] Eso incluye el daño moral de colección y uso excesivo de datos personales.

Con el tiempo, esa base ética ha sido articulada alrededor de los principios jurídicos que conocemos:

- la necesidad de obtener el consentimiento, individual en contratos privados, y colectivo frente al Estado en una sociedad democrática;
- la obligación de las organizaciones de minimizar la colección y el uso de los datos personales a lo necesario, de permitir acceso, y mantener la exactitud de esos datos,
- la obligación de transparencia de las organizaciones en el uso de los datos y,
- la obligación de protección de los datos recogidos.

Eso no cambia porque corresponde a una necesidad humana, entonces intemporal y universal.

Lo que cambia, con el tiempo, entre las culturas y ahora, radicalmente con las nuevas tecnologías de información, son las modalidades de ejercicio, y,

1 *R. v. Duarte, (1990) 1 Supreme Court of Canada, Cour Suprême du Canada, 30.*

2 *Opinion 4/2015*

3 *Supra p. 12*

en consecuencia los riesgos, del derecho a la privacidad.

Esa distinción entre principios y modalidades es nuestra guía en la modernización del marco jurídico de la protección de la privacidad: frente al Internet de la cosas, eso significa preservar el principio de autonomía individual en un contexto de modalidades de automatización de recopilación y de uso de datos personales.

1. 2. La abstracción de internet

El Profesor Alessandro Acquisti[4], economista y gran explorador de la transformación socio-económica del ejercicio del derecho a la privacidad, atribuye, de manera global, los desafíos actuales de ejercicio de la autonomía esencial al derecho de la privacidad a la "abstracción de Internet": el hecho que hemos pasado del mundo físico de modalidades de comunicación donde la privacidad es controlada por los cinco sentidos - con la vista, sabemos que somos vistos; con el oído, sabemos que somos oídos, etc...- a un mundo virtual donde no tenemos esas modalidades tradicionales de control, reduce nuestro control al punto de afectar el ejercicio del derecho a la privacidad.

El carácter virtual y la complexidad del internet tienen principalmente dos impactos jurídicos: forman obstáculos en el ejercicio y la validez del consentimiento y, como resultado, aumentan las exigencias de transparencia y responsabilidad de las organizaciones. Eso exige una adaptación correspondiente del marco jurídico.

1. 3. La asimetría de poder entre las organizaciones y los individuos

La abstracción de Internet, con la complejidad tecnológica y la pérdida de autonomía que cree, resulta en una asimetría creciente entre las organizaciones recopilando y utilizando datos personales y los individuos. En su Opinión, el EDPS resume la dinámica distinta de la nuevas tecnológicas en ubicuidad y poder. Ese tercer fenómeno es consecuencia del segundo: como consecuencia de la complejidad y opacidad de internet, el individuo pierde de su capacidad a determinar cuál datos personales comparte y a qué condiciones. Así, es a la merced de las organizaciones, en una relación de poder asimétrica.

Para re-establecer la simetría, y entonces la equidad en el uso de datos personales, es necesario aumentar las exigencias en obtención del consentimiento, los criterios de transparencia, así que las medidas de responsabilidad, sean códigos de conducta, "audits" o inspecciones por los reguladores.

El internet de las cosas es una ilustración concreta de esos tres fenómenos.

2. CARACTERÍSTICAS DISTINTAS DEL INTERNET DE LAS COSAS

El internet de las cosas es definido, en el informe de la Federal Trade Commission (FTC) de enero 2015 "Internet of things" como "la conexión de cosas físicas a Internet y entre ellas, a través pequeños, incrustados sensores, creando un ecosistema de ubicuo computing."[5] Que la clarificación del marco jurídico entorno al Internet de las cosas sea una preocupación de cierta urgencia es demostrado, entre otros ejemplos, por las actividades de varias agencias del Gobierno de los Estados Unidos. El *National Security Telecommunications Advisory Committee* del Presidente de los Estados Unidos describe la incertidumbre jurídica entorno al Internet de la cosas y sus riesgos como ¨una oportunidad pequeña y que se está cerrando, por asegurar la manera de maximizar la seguridad y minimizar los riesgos".[6]

El 5 de abril 2016, la National Telecommunications and Information Administration (NTIA) solicitó comentarios sobre los desafíos presentados por el Internet de las Cosas. El 3 de junio, la FTC respondía con su análisis de los riesgos y sus recomendaciones para el desarrollo del Internet de la Cosas en la preservación de la privacidad. En resumen, la FTC identifica los riesgos siguientes:

- la posibilidad de acceso no autorizado y mal uso de los datos personales;
- la facilitación de ataques sobre otros sistemas conectados;
- la creación de riesgos a la seguridad con la diseminación de datos sensibles como los datos relativos a la salud.

Una compilación de análisis de expertos resume el impacto del Internet de las cosas sobre el derecho a la privacidad en principalmente cinco puntos en torno a la pérdida de autonomía y el riesgo a la seguridad:

1. La colección autónoma de datos personales es problemática frente a los principios de consentimiento, el control, y la transpa-

4 *Alessandro ACQUISTI, Awareness, Information and Privacy Decision-Making , Presentation to the OECD Jerusalem Privacy Roundtable, 2010*

5 *Internet of things – Privacy & Security in a Connected World , FTC Staff Report, January 2015, p.5*

6 *Informe de Diciembre 2014*

rencia sobre la colección, las finalidades, la comunicación y la protección de los datos personales;

2. La mediación de la colección a través dispositivos no permite, en general, la distinción sobre la sensibilidad de los datos y, por consecuencia, las medidas de protección adecuadas;
3. La colección masiva de datos personales
   a. Es excesiva en relación a los fines
   b. Permite desarrollar perfiles personales que se convierten en datos personales sensibles;
4. La relación contractual limitada a la venta de cosas se convierte en una relación de servicios, que significa una relación continúa con el usuario sin su consentimiento; además, la colección continúa de datos puede revelar comportamientos e intereses, incluyendo la posibilidad de colección de datos personales de terceros.
5. Las posibilidades de acceso por las autoridades de la policía a esos datos sensibles han aumentado.

Las vulnerabilidades de seguridad son también reales:

1. La transferencia a diferentes nubes informáticas, o clouds, de confiabilidad relativa.
2. La transferencia de los datos a redes sociales, a veces automática, con el riesgo de difusión pública; y
3. La facilitación de ataques de sistemas vinculados a las cosas.

La FTC en su comentario del 3 de junio a la NTIA, ya mencionado, recomienda que las empresas,

- Enfatizan la seguridad y la minimización de los datos de manera especial en Internet de las Cosas;
- Permiten notificación y elección significativas en la recopilación y utilización de datos personales;
- Aplican medidas de seguridad aumentadas como: i) la integración de la seguridad en el diseño y desarrollo de los dispositivos; ii) la formación especial de los empleados; iii) la negociación de cláusulas contractuales que permiten supervisión de la protección de datos personales por los vendedores; iv) protecciones tecnológicas correspondientes al riesgo particular de Internet de las cosas; v) establecimiento de un control riguroso de acceso y vi) de un proceso de destrucción de los datos de manera segura al momento que no son necesarias para el servicio contratado.

En resumen, del punto de vista ético y jurídico, para preservar el derecho a la privacidad y acoger los beneficios del internet de las cosas, tenemos que:

desarrollar una nueva forma de consentimiento y transparencia en el contexto de colección autónoma de datos personales;

imponer normas de seguridad correspondientes al riesgo especifico; y

restaurar el equilibrio, la simetría, entre los individuos y las organizaciones.

Esas tres orientaciones forman la base de una proposición por un marco jurídico modernizado de aplicación a Internet de las Cosas.

3. MODERNIZACIÓN DEL MARCO JURÍDICO

El llamo de la Opinión del EDPS a las autoridades de protección de datos personales por un pensamiento innovador propone medidas específicas que son pertinentes a la protección de la privacidad en el contexto del Internet de las Cosas:

1. La simplificación de las reglas del tratamiento de los datos personales de manera que sean todavía pertinentes para una generación.
2. El reconocimiento del riesgo y prejuicio moral de la colección y uso excesivo de datos personales.
3. La colaboración más estrecha entre los reguladores de datos personales y reguladores conexos; por ejemplo, la exigencia de transparencia en la colección y finalidades de datos personales sirve también en contra a la prohibición de discriminación en los precios, a base de datos personales.
4. La creación entre reguladores de protección de datos y reguladores conexos, de un foro de publicación de estadísticas e información pública para alertar los usuarios a la realidad de la colección de datos personales.
5. El aumento de la responsabilidad de las organizaciones con códices de conducta, « audits » certificaciones y nuevas cláusulas contractuales;
6. Como la FTC en sus comentarios del 3 de junio a la NTIA, el desarrollo de ingeniería que es protectora de la privacidad y que permite

a los usuarios un real control de varias opciones.

7. La responsabilidad de los usuarios frente a su participación en la explotación de datos personales. El EDPS usa la palabra "prosumedores" para hacer sobresalir la noción de usuario del internet como agente activo de colección, explotación y diseminación de datos personales sobre Internet. El EDPS recomienda regulación de actividades individuales sobre internet y educación pública.
8. Exigir más que el consentimiento para legitimar la colección y uso de datos personales visto que puede ser precario. Por ejemplo, las organizaciones tienen que ser verificadas para asegurar la conformidad a la ley.
9. La constitución de "data vaults" o "bóvedas de datos" que impedirían el acceso a los datos a otras organizaciones que las que tienen la autorización del individuo.

La FTC también hace recomendaciones para adaptar el marco jurídico a internet de las cosas, más tradicionales pero pertinentes:

- Adoptar leyes generales sobre la seguridad de datos personales
- Clarificar las obligaciones de transparencia de las empresas con opciones por individuos en la elección de modalidades de transacción de datos personales y
- Imponer la obligación de alerta de intrusión.

Concretamente, a base de mi experiencia como regulador de la protección de datos personales por seis años en Canada, y ahora como abogada trabajando con empresas y gobiernos en protección de datos personales en la tecnología de la información, endoso las recomendaciones del EDPS y de la FTC. Además, propongo algunas medidas prácticas para la implementación de los principios de protección de la privacidad en el contexto específico de internet de las cosas:

1. Transparencia: Al punto de venta de un dispositivo conectado, o de suscripción a un servicio público conectado, la organización tiene la obligación de comunicar información clara, completa y accesible al individuo, sobre la colección autónoma – y automática- de datos personales, sobre sus finalidades, y sobre la protección de esos datos;
2. Consentimiento: Esa comunicación seria confirmada por la expresión de consentimiento expreso con firma – de la misma manera que consumidores firman formas de garantía- o con la activación de un appli especifica;
3. Opciones de rechazo:
   a. en el sector privado: una opción de rechazo, aunque perdiendo los ventajas de la conexión a internet, podría todavía permitir la compra del dispositivo;
   b. en el sector público, por ejemplo en la implementación de contadores inteligentes por servicio de electricidad con fines de mejorar la eficiencia energética, la imposición de internet de las cosas tiene que ser
      i. regulada por los estrictos criterios de necesidad, de proporcionalidad, de eficacia y de ausencia de una alternativa menos intrusiva,
      ii. aplicada con "Privacy Impact Assessments" (PIAs) para evaluar el impacto sobre la privacidad de cada iniciativa pertinente,
      iii. acompañada de información pública sobre los detalles de la colección de datos y sus finalidades, de manera proactiva como campañas de información, y receptiva con acceso de los ciudadanos a la Información,
      iv. supervisada por organismos de control internos y externos para asegurar la conformidad de manera proactiva,
      v. incluyendo remedios para obtener acceso a sus datos personales y corrección, llegado el caso.
4. Una vez los datos recogidos, las medidas de seguridad tienen que incluir, además de la protección apropiada al nivel de sensibilidad:
   a. Anonimización inmediata y efectiva de los datos personales non necesarios al funcionamiento del servicio; y
   b. Segregación y protección de los datos personales necesarios con acceso estrecho y controlado.

Esos parámetros de explotación de datos personales en internet de las cosas reflejan solamente una modernización de las reglas existentes:

- Consentimiento adaptado a los métodos de colección,
- Transparencia correspondiente a la ubicuidad y opacidad del uso, y

- Protección al nivel de riesgos y de sensibilidad de los datos, no solamente como recogidos, pero también en su aglomeración en un perfil.

Más radical es la transformación necesaria del poder de los reguladores para corregir la asimetría que se está desarrollando entre los individuos y las organizaciones.

4. EL PAPEL DE LOS REGULADORES

La proposición del aumento de los poderes y recursos de los reguladores no es popular. Sin embrago, es inevitable y se puede manifestar de forma positiva.

Es inevitable en base a esas constataciones:

- La economía numérica ofrece a las empresas beneficios comerciales y prácticos monumentales. Por el gobierno, el análisis de datos apoye decisiones más exactamente que nunca antes.
- Esa economía y esa riqueza de datos no se pueden desarrollar sin confianza de los individuos.
- La confianza de los individuos necesita que ejercen un poder de control inherente al derecho a la privacidad.
- Ese poder de control individual esta siempre más limitado frente a la capacidad tecnológica de las organizaciones.

La Opinión del EDPS[7] propone que los reguladores necesitan más poderes y recursos para aumentar

- Colaboración entre ellos y con reguladores conexos,
- Verificación e inspecciones de la organizaciones considerando los desafíos de complexidad y opacidad del internet para entender los verdaderos límites de colección, finalidades y protección de datos personales,
- Impuesto de penalidades a los delincuentes y
- Identificación por nombre de las organizaciones cuando es de interés público hacerlo.

Ese aumento de la intervención de los reguladores puede realizarse de manera colegial y positiva a raíz de dos fenómenos: i) al mismo tiempo que las organizaciones delincuentes pierden en reputación, las empresas conformas ganan, y adquieren un ventaja competitiva; ii) cuando los delincuentes pagan penalidades por no tener las practicas o las infraestructuras necesarias para ser conformes, son colocadas a nivel con las organizaciones que han invertido en la delantera. Eso parece económicamente más justo y conlleva un lado positivo.

5. INVALIDEZ DE SAFE HARBOR E INTERNET DE LAS COSAS

Finalmente, desde la decisión en el caso *Maximilian Schrems v. Data Protection Commissioner* de la Corte de Justicia de la Unión Europea (CJUE) del 6 de octubre 2015[8] tenemos que examinar cómo la anulación de Safe Harbor impacta la recopilación de datos personales trámite internet de las cosas.

En esa decisión, la CJUE ha declarado la invalidez de Safe Harbor. Safe Harbor era el acuerdo entre los Estados Unidos y la Comisión europea que tenía luego de adecuación para la transferencia de datos personales de Europa a empresas en los Estados Unidos.

Ahora, la transferencia a Estados Unidos, como a todo país que no ha sido reconocido como adecuado – solo Argentina y Uruguay tienen ese estatus en América Latina- necesita cláusulas modelos entre empresas, o "Binding Corporate Rules, BCRs" entre un empresa y sus filiales, o el consentimiento individual a la transferencia de los datos personales a los Estados Unidos. En el contexto del Internet de las cosas, ¿cómo se aplica?

En general, la opción del consentimiento individual para la transferencia de datos fuera de Europa parece un guion improbable y rechazado como impracticable por el número de usuarios. Pero, en varios contextos, incluido el de Internet de las cosas, el consentimiento individual puede ser una opción práctica: como ya mencionado, el consentimiento para la recopilación autónoma de datos personales, como el caso de Internet de las cosas, es recogido al punto de venta. En muchas aplicaciones eso podría incluir el consentimiento a la transferencia de los datos personales a los Estados Unidos. Esa opción vale para todas las empresas Latino-Americanas que no son establecidas en países que tienen la adecuación.

7 *Supra, nota 3, p. 10*

8 *Court of Justice of the European Union, Judgment in Case C-362/14*

CONCLUSIÓN

En resumen, el futuro ha llegado y la modernización del derecho la privacidad es urgente para su respecto en el contexto del Internet de las cosas.

Por qué en el futuro sea protegida la privacidad en el contexto de Internet de las cosas, tenemos que clarificar, específicamente en la relación a las características de esa nueva tecnología:

1. La forma de consentimiento valido en el contexto de colección autónoma, continua y mediante dispositivos.
2. Las exigencias de transparencia teniendo cuenta de la abstracción, la opacidad y la complexidad de internet.
3. Los poderes de control apropiados de las autoridades de protección de datos en esa situación de ubicuidad y capacidad masiva de colección y uso de los datos personales por las organizaciones, para defender los individuos de manera eficaz y rectificar la asimetría creciente con las organizaciones.

Lo que es seguro es que la protección continua de la privacidad exige, al mismo tiempo, un pensamiento fiel a los principios y novador en las modalidades de aplicación.

REFLEXIONES RESPECTO A LA GLOBALIZACIÓN Y LA PRIVACIDAD DE DATOS

Remitidas por el Supervisor Europeo de Protección de Datos

GIOVANNI
BUTTARELLI

Ha sido el Supervisor Europeo de Protección de Datos (EDPS) desde diciembre de 2014. Fue designado por decisión conjunta del Parlamento y el Consejo Europeo el 4 de diciembre de 2014 por el término de cinco años. Previamente se había desempeñado como EDPS Adjunto, desde enero de 2009 hasta diciembre de 2014. Antes de incorporarse al EDPS, trabajó como Secretario General de la Autoridad Italiana de Protección de Datos, posición que ocupó desde 1997 hasta 2009. Miembro del sistema judicial italiano con el rango de Juez de Casación, tuvo a su cargo múltiples iniciativas y comités en protección de datos y temas relacionados a nivel internacional.

SUMARIO

RESUMEN

El artículo analiza el impacto de la globalización y la conectividad en línea en la protección de datos. Reseña los distintos regímenes vinculados a los estándares internacionales que han influenciado a un gran número de países, y en particular a Uruguay.

Destaca la importancia de construir alianzas en materia de tratamiento responsable de datos basado en valores comunes, construyendo relaciones verdaderamente transatlánticas. Estas alianzas impactan en cuestiones tales como internet de las cosas, inteligencia artificial, big data, entre otras.

Reafirma la relevancia de un uso positivo de Big Data para cambiar el mundo sin afectar nuestros derechos fundamentales.

Finalmente, reseña las nuevas reglas europeas vinculadas con el Reglamento que entrará en vigencia el 25 de mayo de 2018, y su impacto en las decisiones de adecuación de países fuera de la Unión Europea.

REFLEXIONES

Globalisation is a daily reality for everyone. The labels on the food we eat and the clothes we wear give us a glimpse of the global value chain in the real world. There are plenty of international standards for the production and delivery of physical goods, to prevent harm occurring to individuals in the process. But for the online world, which has so quickly become so pervasive in our lives, we are only just beginning to understand the safeguards that are needed.

Both globalisation and its corollary of online connectivity depend on instantaneous, international flows of personal data. In Europe we are modernising our legal frameworks and preparing a new generation of rules which are fit for the digital age. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, the first and still the only legal data protection instrument with a global reach, is about to be modernised. Uruguay, by joining the Convention in 2013, established the remarkable precedent that these principles were not simply the preserve of the continent of Europe. With the adoption of its new law in April, Turkey became the 110th country with its own data protection legislation, and most of these 110 countries are outside Europe. Morocco, Senegal and Mauritius have expressed their intentions to become signatories of the Convention and they are in different stages of this process.

Meanwhile the European Union, in which the right to privacy and the right to the protection of personal data are fundamental rights, adopted in May this year a bold and comprehensive new framework for data protection: a Regulation with general application, and a Directive to be transposed by the 28 member states of the EU on data protection in the police and criminal justice sector.

So now is the opportunity for all democratic countries across the world to build partnerships on responsible data processing based on common values. We need to build a truly transatlantic relationship, embracing the shared culture and values of Europe and Latin America, as well as North America and even Africa.

This is not just about compliance with the law. We have to think about the long term implications for society of big data, the internet of things, artificial intelligence, self-driving cars and other frontier technologies. New laws like the EU's General Data Protection Regulation should start to reverse the recent trend towards secret tracking and decision-making on the basis of profiles hidden from the individual. Privacy is much more than the ability to avoid targeted advertising: individuals should be empowered and informed, with meaningful information about the algorithmic logic which develops these profiles.

There needs to be fuller transparency from controllers of personal data. The EU's new regulation establishes principles of data protection by design and by default and these should be a means of kick-starting market-driven solutions in the digital economy. Data portability – the ability of individuals to transfer data about them from one controller to another on the data subject's request and to receive a copy of the data which they themselves can transfer to another controller – is set to become a key component of 'big data protection' in the 21st century, a shift of control in favour of the individual.

Previous generations of data protection rules have addressed the transition from manual to automated processing, from analogue to digital networks, from the pioneering development of e-commerce to the Information Society, from silos to interconnected large-scale data systems.

Big Data - used well - can be used to change the world positively without compromising our fundamental rights. Technology has changed the na-

ture of personal data. It used to be a question of the data we gave controllers. But now, with profiling, companies have data about us which we never had as data subjects and which we do not know anything about. Big data allows all sorts of combinations from the 'digital breadcrumbs' we all leave, not just with credit cards but in social media, travelling around with contactless public transport smartcards and wearable devices. Social media reveals what sort of friends you have, perhaps your political views and sexual orientation, and how you spend your leisure time.

The new EU rules reinforces individual rights and how they are exercised and establishes the accountability of public bodies and companies to document how they will comply, with potential sanctions of up to 4% of annual global revenue for violations of the rules. The provisions on adequacy of a non-EU country for transfer of personal data and the wider scope of territorial application are of particular importance for Uruguay and its neighbours. Uruguay is among the small number of countries which have been assessed as 'adequate' – a term which the Court of Justice of the European Union, in its Schrems judgment in October 2016, affirmed to mean a country has safeguards which are 'essentially equivalent' to those applicable in the EU. Under the new regulation (Article 41), the European Commission must review at least every four years these individual adequacy decisions, and can decide whether to retain, repeal, amend or suspend those decisions. Furthermore, the regulation will apply (Article 3.2) to all organisations and companies that offer goods and services to individuals in the EU, irrespective of whether they require payment and irrespective of whether they are established on EU territory.

Uruguay is a true pioneer for data protection, and the natural partner for the European Union as we prepare for the 25 May 2018, the date the General Data Protection Regulation becomes fully applicable. I look forward to deepening our conversation and collaboration together in building a true transatlantic partnership.

TRATAMIENTO DE LA INFORMACIÓN PÚBLICA Y PERSONAL A LA LUZ DE LAS NUEVAS TECNOLOGÍAS

CARLOS DELPIAZZO

Es Doctor en Derecho y Ciencias Sociales por la Universidad Mayor de la República Oriental del Uruguay. Decano de la Facultad de Derecho de la Universidad Católica del Uruguay Dámaso Antonio Larrañaga. Catedrático de Derecho Administrativo en la Facultad de Derecho de la Universidad de Montevideo. Ex Catedrático de Derecho Administrativo, de Derecho Informático y de Derecho Telemático en la Facultad de Derecho de la Universidad de la República. Autor de 71 libros y más de 500 trabajos publicados en el país y en el exterior. Presidente del Capítulo Uruguay de la Federación Iberoamericana de Asociaciones de Derecho e Informática. Profesor Invitado del Instituto Nacional de Administración Pública (España). Profesor Visitante de la Especialización en Derecho Administrativo de la Universidad de Belgrano (Argentina). Profesor Extraordinario Visitante de la Universidad Católica de Salta (Argentina). Miembro del Comité Académico de la Maestría de Derecho Administrativo de la Facultad de Derecho de la Universidad Austral (Argentina) y de la Comisión Académica del Programa de Doctorado de Derecho Administrativo Iberoamericano liderado por la Universidad de La Coruña (España). Ex Director del Instituto de Derecho Administrativo y del Instituto de Derecho Informático de la Universidad de la República. Miembro del Instituto de Derecho Administrativo de la Universidad Notarial Argentina, de la Asociación Argentina de Derecho Administrativo, de la Asociación de Derecho Público del Mercosur, de la Academia Internacional de Derecho Comparado, y de la Asociación Iberoamericana de Derecho Administrativo. Miembro fundador y Vicepresidente para América del Sur de la Asociación Internacional de Derecho Administrativo. Secretario General del Foro Iberoamericano de Derecho Administrativo.

SUMARIO

PROPÓSITO

Asistimos en nuestros días a lo que el Papa Francisco ha calificado como la "globalización del paradigma tecnocrático", a consecuencia del cual "Hay que reconocer que los objetos producto de la técnica no son neutros, porque crean un entramado que termina condicionando los estilos de vida y orientan las posibilidades sociales en la línea de los intereses de determinados grupos de poder. Ciertas elecciones, que parecen puramente instrumentales, en realidad son elecciones acerca de la vida social que se quiere desarrollar" [1].

Agrega el Papa, con acierto, que "La especialización propia de la tecnología implica una gran dificultad para mirar el conjunto. La fragmentación de los saberes cumple su función a la hora de lograr aplicaciones concretas, pero suele llevar a perder el sentido de la totalidad, de las relaciones que existen entre las cosas, del horizonte amplio, que se vuelve irrelevante" [2].

Es lo que ocurre con la información -tanto la privada como la pública, no siempre adecuadamente distinguidas- ante las posibilidades que abren la interoperabilidad [3] y las redes sociales [4].

Por eso, se impone superar el referido paradigma tecnocrático, estableciendo bases firmes para quebrar el antagonismo -más aparente que real- entre información pública e información personal o privada, previniéndolo y evitándolo [5].

LOS TÉRMINOS DE LA CUESTIÓN

1. INFORMACIÓN PÚBLICA Y DERECHO DE ACCESO

Una de las características sobresalientes de la sociedad de nuestros días es que la información se ha convertido en una nueva forma de energía, de poder y de producción[6]. Ya nadie duda que, junto al poder de las armas y del dinero, hoy la información es un elemento central, incluso para el poder militar y el poder económico, constituyéndose en sí misma en una novedosa forma de bien valorable económicamente[7].

Es que "en la sociedad contemporánea la información se presenta con caracteres hasta ahora desconocidos en la historia de la civilización humana en lo concerniente a su cantidad, su variedad, su rapidez, su persistencia y, finalmente, y este es el carácter decisivo y condicionante de todos los demás, a su automatización"[8].

En ese contexto, se considera **información pública** aquella que se encuentra en poder de las Administraciones, siempre que la misma no se encuentre limitada mediante ley dictada por razones de interés general.

Frente a la misma, cualquiera sea el soporte en que se encuentre registrada como consecuencia del desarrollo tecnológico, opera el derecho de acceso a la información pública[9] como moderno desprendimiento del clásico derecho humano a la información[10], que implica hacerla accesible a todos[11], es decir, democratizarla y acortar la distancia entre el Estado y la sociedad[12]. No es casual que los

1 *Papa FRANCISCO – Carta Enciclica Laudato Si', Nº 107.*

2 *Papa FRANCISCO – Carta Enciclica Laudato Si', Nº 110.*

3 *Carlos E. DELPIAZZO - "A propósito de la reglamentación de la interoperabilidad", en Anuario "Derecho Informático" (F.C.U., Montevideo, 2014), tomo XIV, pág. 262 y sigtes.; y "Criterios para la ponderación entre interoperabilidad y privacidad en las Administraciones públicas", en CD del XV Congreso Iberoamericano de Derecho e Informática (Buenos Aires, 2011).*

4 *Carlos E. DELPIAZZO - "Las redes sociales en clave jurídica", en Anuario "Derecho Informático" (F.C.U., Montevideo, 2011), tomo XI, pág. 153 y sigtes.; y "Enfoque jurídico de las redes sociales", en CD del XIV Congreso Iberoamericano de Derecho e Informática (Monterrey, 2010).*

5 *Carlos E. DELPIAZZO - "A la búsqueda del equilibrio entre privacidad y acceso", en Carlos E. DELPIAZZO (Coordinador) - "Protección de datos y acceso a la información pública" (F.C.U., Montevideo, 2009), pág. 11 y sigtes.*

6 *Vittorio FROSINI - "Cibernética, Derecho y Sociedad" (Tecnos, Madrid, 1982), pág. 173 y sigtes.*

7 *Carlos E. DELPIAZZO – "Información, Informática y Derecho" (A.M.F., Montevideo, 1989), pág. 10 y sigtes.*

8 *Vittorio FROSINI - "Informática y Derecho" (Temis, Bogotá, 1988), pág. 29.*

9 *Marcela I. BASTERRA - "El derecho fundamental de acceso a la información pública" (Lexis Nexis, Buenos Aires, 2006), pág. 10.*

10 *José María DESANTES – "La información como derecho" (Madrid, 1973), pág. 36 y sigtes.; Miguel Angel EKMEKDJIAN – "Derecho a la información" (Depalma, Buenos Aires, 1992), pág. 25 y sigtes.; y Fernando URIOSTE BRAGA – "El derecho a la información", en Rev. Prisma (Montevideo, 1994), Nº 2, pág. 143 y sigtes.*

11 *Emilio GUICHOT (Coordinador) – "Transparencia, acceso a la información pública y buen gobierno" cit., pág. 199 y sigtes.*

12 *Dolores LAVALLE COBO – "Derecho de acceso a la información*

países pioneros en el reconocimiento y regulación del derecho de acceso a la información pública sean los más desarrollados desde una perspectiva democrática[13].

Además del principio de juridicidad, que es pilar fundamental del Estado de Derecho[14], tres principios generales convocan a la accesibilidad a la información de los entes públicos, siempre que la misma no se encuentre limitada mediante ley dictada por razones de interés general en atención a fines específicos (tal como ocurre con el secreto militar, el secreto estadístico o el secreto tributario, entre otros).

En primer lugar, corresponde mencionar el *principio de publicidad* del obrar administrativo, el cual deriva de la forma republicana de gobierno[15], por lo que "las restricciones a la publicidad deben atender a dos criterios: por un lado, deben ser más débiles cuanto mayor sea el interés individual del que pide información; por otro lado, deben ser más débiles cuanto mayor sea la responsabilidad del solicitante por el buen funcionamiento del ente administrativo requerido. Y en ambos casos, la restricción debe ser motivada en una razón que sea suficientemente importante como para compensar la razón genérica que aconseja la publicidad como resorte esencial del sistema republicano. No hay que olvidar que la restricción debe tener siempre un motivo legítimo, derivar de un acto inspirado en alguna razón atendible... Pero si no hay razones para la restricción, aunque tampoco existan motivos especiales para la publicidad, ésta procede; precisamente porque ésta es la solución de principio bajo el sistema republicano" [16].

En segundo lugar, íntimamente asociado al principio de publicidad, el *principio de transparencia* supone algo más. Cuando se habla de transparencia de la gestión administrativa, "se quiere dar un paso más respecto a la publicidad... como que la publicidad implica mostrar pero la transparencia implica algo más que mostrar, implica dejar ver; simplemente que el actuar de la Administración se deje ver como a través de un cristal" [17].

Más allá de la publicidad, la transparencia refiere a la diafanidad del obrar público, permitiendo ver con claridad el actuar de la Administración en la disposición y uso de los fondos públicos y en el obrar de sus funcionarios, por lo que "constituye una consecuencia de la muy elemental presunción de que el gobierno pertenece al pueblo, quien tiene derecho a saber qué hacen los servidores públicos, por qué y cómo lo hacen" [18].

Según se ha destacado[19], la transparencia se asocia a lo que es visible y accesible, a lo que puede ser conocido y comprendido, por contraposición a lo cerrado, misterioso, inaccesible o inexplicable. Igualmente, la transparencia se asocia a una carga afectiva ligada a la tranquilidad y serenidad provocada por todo aquello que se domina y racionaliza, por oposición a la angustia y perturbación de lo misterioso y desconocido. Además, del contraste entre las sombras y la luz, entre opacidad y transparencia, nacen nuevos métodos que tratan de referir el principio de legalidad, como límite y fundamento de la acción administrativa, al principio de consecución del interés público y del respeto por los derechos de los ciudadanos en el marco del bien común, métodos que tratan de promover los principios de colaboración ciudadana, de participación y de promoción de una nueva y diferente forma de concebir el poder administrativo más próximo a los ciudadanos.

En tercer lugar, desde la perspectiva tecnológica, interesa destacar que la accesibilidad por todos a la información pública y, más aún, al quehacer de las Administraciones públicas está impuesta por el *principio de participación* [20].

---

pública" (Astrea, Buenos Aires, 2009), pág. 3.

13 *Emilio GUICHOT – "Transparencia y acceso a la información pública en el Derecho europeo" (Global Law Press, Sevilla, 2011), pág. 77 y sigtes.*

14 *Carlos E. DELPIAZZO - "Afirmación y evolución del principio de juridicidad", en Jaime Orlando SANTOFIMIO, Héctor SANTAELLA y Andry MATILLA (Coordinadores) - "Ensayos de Derecho Público en memoria de Maurice Hauriou" (Universidad Externado de Colombia, Bogotá, 2013), pág. 197 y sigtes.*

15 *Felipe ROTONDO TORNARIA - "Aproximación a la participación del administrado a la luz de los principios generales", en Rev. de la Facultad de Derecho y C.S., Año XXVI, Nº 1, pág. 63.*

16 *Horacio CASSINELLI MUÑOZ - "El principio de publicidad de la gestión administrativa" cit., tomo 58, págs. 165 y 166; y Elbio J. LOPEZ ROCCA - "Publicidad y secreto en la Administración Pública", en Rev. de Derecho Público, Año 2003, Nº 24, pág. 39 y sigtes.*

17 *Carlos E. DELPIAZZO - "De la publicidad a la transparencia en la gestión administrativa", en Rev. de Derecho de la Universidad de Montevideo (Montevideo, 2003), Año II, Nº 3, pág. 113 y sigtes.; "La regulación legal del control social y transparencia", en Rev. de Antiguos Alumnos del IEEM, Año 5, Nº 1, pág. 29 y sigtes.; "Control social de la Administración y transparencia", en Rev. Ius Publicum (Santiago de Chile, 2003), Nº 11, pág. 43 y sigtes.; y "Transparencia en la contratación administrativa", en "Liber Amicorum Discipulorumque José Aníbal Cagnoni" (F.C.U., Montevideo, 2005), pág. 138 y sigtes.*

18 *Richard S WERKSMAN y Carlos MAMFRONI - "La transparencia y la Convención Interamericana contra la Corrupción", en Rev. de Derecho Administrativo (Buenos Aires, 1996), Año 8, Nº 21-23, pág. 346.*

19 *Jaime RODRIGUEZ-ARANA MUÑOZ - "La dimensión ética" (Dykinson, Madrid, 2001), pág. 312.*

20 *Carlos E. DELPIAZZO - "Dimensión tecnológica de la participación del administrado en el Derecho uruguayo", en Rev. Iberoamericana de Derecho Público y Administrativo*

En rigor, transparencia y participación se retoalimentan [21], por lo que, existiendo accesibilidad real, se abre un ancho cauce de participación ciudadana a través de la red, siempre que los habitantes sean informados y consultados en los asuntos que les conciernen [22].

Ahora bien: según se ha destacado con acierto, el derecho de acceso a los archivos y registros administrativos constituye un "derecho encrucijada" [23], habida cuenta del cúmulo de datos personales en poder de las Administraciones públicas, obtenidos a través del ejercicio de sus diversos cometidos.

Por lo tanto, es preciso preservar que, por la vía del intercambio de información entre las Administraciones que posibilita la interoperabilidad y del consiguiente acceso por los habitantes a esa información, no pueda verse herida la privacidad de las personas.

2. INFORMACIÓN PERSONAL Y DERECHO A LA PRIVACIDAD

Como ya he tenido oportunidad de destacarlo [24], desde que Samuel WARREN y Luis BRANDEIS perfilaron el clásico "right to be alone" (1890) hasta el presente, ha discurrido mucha agua debajo de los puentes respecto al *derecho a la intimidad*, transitándose -al impulso de las nuevas tecnologías de la información y las comunicaciones- hacia la libertad informática, la autodeterminación informativa y el derecho a la protección de los datos personales.

La globalización de la información privada ha adicionado una nueva tonalidad a la cuestión, que exorbita el concepto clásico de intimidad, abriendo cauce a su distinción del *derecho a la privacidad* (derivada de la expresión inglesa "privacy"), concebida como más amplia que aquélla al aludir a datos no íntimos pero que la persona no quiere que sean difundidos.

Si bien muchos autores identifican intimidad y privacidad, es posible diferenciarlas desde una perspectiva perfeccionadora de la tutela de la persona humana en su eminente dignidad [25].

Así, se ha dicho que: "La protección de los datos personales -entre los que debemos encuadrar aquellos que, unidos al individuo, se pueden considerar como características que definen a la persona y a su entorno, en su convivencia social- está suficientemente protegida en las nuevas legislaciones, mediante el derecho a la intimidad. Es cuando surge la Informática y la posibilidad de tratamiento automatizado de la información y su trasmisión telemática -que proporciona unas características especiales a la información, añadiendo posibilidades de tratamiento en tiempos pequeños, de volúmenes grandes, con las particularidades informáticas de procesamiento de la misma que, en principio, tienen una potencial agresividad contra la intimidad de la persona, en formas diferentes- cuando aparece una nueva relación entre datos y personas, que necesita que el individuo sea protegido más allá de las normas referentes a la intimidad. El derecho que se trata de proteger no es solamente el de la intimidad, sino algo con mayor profundidad, que en los ordenamientos de ámbito anglosajón, se ha dado en llamar "privacy" y que nosotros hemos castellanizado como privacidad" [26].

En esa línea, la antigua ley española de protección de datos Nº 5/1992 señalaba en su exposición de motivos que la intimidad "protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona", mientras que la privacidad "constituye un conjunto, más amplio,

(San José de Costa Rica, 2005), Nº 5, pág. 63 y sigtes.; y en Rogerio GESTA LEAL (Organizador) - "Administraçao Pública e Participaçao Social na América Latina" (Edunisc, Santa Cruz do Sul, 2005), pág. 117 y sigtes.

21 *Laura NAHABETIAN BRUNET – "Acceso a la información pública: pilar fundamental del buen gobierno" (A.M.F., Montevideo, 2010), pág. 188.*

22 *Laura NAHABETIAN BRUNET - "Protagonistas del cambio. Derechos ciudadanos y nuevas tecnologías", en X Congreso Iberoamericano de Derecho e Informática (Santiago de Chile, 2004), pág. 120 y sigtes.*

23 *Manuel ALVAREZ RICO e Isabel ALVAREZ RICO - "Derecho de acceso a los archivos y registros administrativos en la nueva ley de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común", en Rev. de Administración Pública (Madrid, 1994), Nº 135, pág. 479 y sigtes.*

24 *Carlos E. DELPIAZZO y María José VIEGA - "Lecciones de Derecho Telemático" (F.C.U., Montevideo, 2009), tomo II, pág. 57.*

25 *Carlos E. DELPIAZZO - "Dignidad humana y Derecho" (U.M., Montevideo, 2001), pág. 123 y sigtes.; "Protección de los datos personales en tiempos de Internet. El nuevo rostro del derecho a la intimidad", en Rev. de Derecho de la Universidad Católica del Uruguay (Montevideo, 2002), Nº III, pág. 253 y sigtes.; "Nueva regulación de la tutela de los datos personales y habeas data en el Derecho uruguayo", en "El Derecho en Red. Estudios en homenaje al Prof. Mario G. Losano" (Dykinson, Madrid, 2006), pág. 241 y sigtes.; "El derecho a la intimidad en el nuevo horizonte telecomunicativo", en Mariliana RICO CARRILLO, Coordinadora - "Derecho de las nuevas tecnologías" (Edic. La Rocca, Buenos Aires, 2007), pág. 129 y sigtes.; "Marco actual de la protección de datos", en Rev. Derecho y Nuevas Tecnologías (Buenos Aires, 2006), Años 4-5, Nº 6-7-8, pág. 527 y sigtes.; y "El derecho a la intimidad en el ciberespacio", en Anales de las 30 Jornadas Argentinas de Informática e Investigación Operativa, Buenos Aires, 2001, pág. 51 y sigtes.*

26 *Miguel Angel DAVARA RODRIGUEZ - "Manual de Derecho Informático" (Thomson - Aranzadi, Navarra, 2004), 6ª edición, págs. 53 y 54.*

más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

Si se admite tal diferenciación, los aludidos derechos podrían representarse en círculos concéntricos, en cuyo marco el derecho a la protección de datos personales comprende los datos que afectan a la vida íntima de la persona, pero también a todos aquellos que la identifiquen o puedan identificarla y, al hacerlo, puedan ser susceptibles de producir, en determinadas circunstancias, una amenaza para el individuo. Consecuentemente, faculta a la persona a decidir cuáles proporciona a un tercero y para saber quién los posee y para qué finalidad concreta. El ejercicio de ese poder se manifiesta en la posibilidad de consentir la colecta, tratamiento y uso de los datos, así como en el derecho de acceso, rectificación, cancelación y oposición [27].

De este modo, la reserva de la **información personal** o de carácter privado se opone a la publicidad que, por principio, tiene la información pública, distinción que, desde el punto de vista práctico, se ve diluida por el avance de las nuevas tecnologías e Internet [28] sin que ello alcance para desnaturalizar su esencia.

Abonan la confidencialidad de la información de carácter personal -erigida ella misma como principio general, regla de Derecho [29]- un conjunto de otros principios generales de Derecho que, con distintos grados de explicitación, son reconocidos a nivel comparado[30].

En primer lugar, corresponde mencionar el *principio de justificación*, según el cual la recolección de datos personales deberá tener un propósito general y usos específicos socialmente aceptables.

En segundo lugar, reviste vital importancia el *principio de limitación de la recolección*, según el cual los datos deberán ser recolectados por medios lícitos y con conocimiento y consentimiento del interesado, acotándose al mínimo necesario para alcanzar el fin perseguido.

En tercer lugar, conforme al *principio de veracidad* o fidelidad de la información, los datos personales que se registren deberán ser exactos, completos y actuales, rectificándose o cancelándose en su caso.

En cuarto lugar, el *principio de especificación* del propósito obliga a que en el momento de recolectarse los datos se informe con qué objetivo ello se hace, no pudiendo luego usarse para fines diferentes.

En quinto lugar, el *principio de seguridad* obliga a que todo responsable del registro de datos personales deba adoptar las medidas de reserva y cautela adecuadas para protegerlos contra posibles pérdidas, destrucciones o acceso no autorizado.

En sexto lugar, el *principio de limitación temporal* determina que los datos personales no puedan conservarse más allá del tiempo requerido para alcanzar el objetivo para el cual fueron recolectados.

PROCURA DEL DEBIDO EQUILIBRIO

A partir de la diferenciación entre información pública y privada y de los consiguientes derechos humanos de acceso a la primera y de protección de la segunda, es posible alcanzar la debida ponderación entre ambos, especialmente respecto a los grandes volúmenes de información que manejan las Administraciones públicas.

Al respecto, debe tenerse presente que la circulación de la información pública entre las Administraciones no es una libertad de éstas -la libertad se predica de las personas y no de las Administraciones como instrumentos de servicio a la sociedad y sus integrantes- sino un deber de servicialidad inherente a su naturaleza vicarial para el bien común [31] tendiente a hacer más eficaz su obrar y a garantizar el ejercicio del derecho de acceso por parte de todos los habitantes.

Distinta es la situación de la información privada, la cual no puede considerarse comprendida dentro

27 *Alvaro CANALES GIL - "La protección de datos personales como derecho fundamental", en anuario "Derecho Informático" (F.C.U., Montevideo, 2004), tomo IV, pág. 265.*

28 *José Julio FERNANDEZ RODRIGUEZ - "Secreto e intervención de las comunicaciones en Internet" (Thomson Civitas, Madrid, 2004), pág. 56 y sigtes.*

29 *Carlos E. DELPIAZZO - "Recepción de los principios generales de Derecho por el Derecho positivo uruguayo", en Actas del VII Foro Iberoamericano de Derecho Administrativo (Netbiblo, La Coruña, 2008), pág. 607 y sigtes., y en A.A.V.V. - "Los principios en el Derecho Administrativo Uruguayo" (A.M.F., Montevideo, 2009), pág. 31 y sigtes.*

30 *Carlos E. DELPIAZZO y María José VIEGA - "Lecciones de Derecho Telemático" (F.C.U., Montevideo, 2004), tomo I, págs. 75 y 76.*

31 *Carlos E. DELPIAZZO - "Bien común, sociedad y Estado", en Rev. de Derecho de la Universidad de Montevideo (Montevideo, 2012), Año XI Nº 21, pág. 81 y sigtes.*

de ese amplio flujo interadministrativo de datos, que no puede referir a los personales sino tan sólo a los públicos.

Bajo una perspectiva general, la cuestión no es novedosa sino que plantea -en nuevos términos [32]- el viejo dilema de si los derechos humanos entran o no en colisión, temática que enfrenta al menos dos visiones [33]: la de quienes sostienen el "conflictivismo" entre los derechos [34] y la de quienes, en cambio, postulan el "coherentismo" o compatibilidad de los derechos, procurando su armonización [35].

El punto de partida no puede ser otro que la propia noción de Estado de Derecho, caracterizada no sólo por el respeto y la garantía del conjunto de los derechos fundamentales, sino por el armónico relacionamiento de éstos, en atención a la centralidad de la persona y en orden a su realización [36].

En efecto, los derechos humanos no admiten ser considerados exclusivamente como *limitación al poder estatal*, erigiéndose también frente a los demás particulares. Como bien se ha señalado, "es claro que es el hombre, con su dignidad, con su naturaleza, con su personalidad, el que propone la materia de los derechos humanos, pero la proporciona porque es aquella misma naturaleza la que está inserta esencial y existencialmente en un orbe de relaciones sociales, en una sociedad" [37].

Tal circunstancia de la *limitación frente a los demás* no puede llevar a pensar en la inexistencia de la pretendida armonía entre derechos, afirmando la constante colisión de los mismos, en el marco de las relaciones sociales en que está inserto el hombre.

Es que, "los derechos, a diferencia de los intereses de las personas, son armónicos (...). Los seres humanos tenemos pretensiones y somos capaces de advertir que los demás también las tienen, y que para cada uno la propia pretensión constituye una verdad incontestable. Un orden jurídico se construye al advertir esta igualdad de los diferentes individuos, que es precisamente lo que origina la concurrencia o el conflicto potencial. Si el otro es tratado como un obstáculo, como una cosa, no hay orden jurídico, sino violencia; pero si es reconocido como un igual, se podrá tratar de armonizar la propia aspiración con las ajenas y, sobre la base de una verdad común, construir una regla de convivencia, esto es, un orden jurídico" [38].

La armonización de los derechos se impone asimismo como consecuencia de una adecuada hermenéutica constitucional, que parte de la necesaria unidad de la Constitución, haciendo compatible internamente su contenido, y evitando la supresión recíproca de disposiciones, al menos en los casos concretos.

Lo antedicho conduce a la constatación de que salvo respecto a la vida -supuesto de todos los demás derechos humanos- no hay jerarquías rígidas entre los derechos ya que no hay fundamento alguno de Derecho positivo para atribuir diferente peso a los derechos, pretendiendo dar solución, por esta vía, a los supuestos casos de conflictos o colisiones entre ellos.

Según se ha destacado, "las diferentes jerarquizaciones propuestas suelen depender de criterios y baremos que, aunque gozan de cierta justificabilidad en términos constitucionales, se encuentran fuertemente marcados por condicionamientos ideológicos" [39].

Para superarlos, hay quienes postulan como un método idóneo de interpretación constitucional para la resolución de los supuestos conflictos entre derechos, el denominado "balancing test" o ponderación de los derechos aparentemente enfrentados.

Según se ha dicho, "Los expositores de esta tesis procuran sopesar los derechos en juego. El punto de partida radica en considerar que todos los derechos y bienes son iguales y equivalentes entre sí, por lo que se impone una necesaria y casuística ponderación. Por regla general, los partidarios de esta tesis no proporcionan criterios para realizar la ponderación" [40].

32 *María del Camino VIDAL FUEYO - "Libertades públicas y nuevas tecnologías", en Fernando GALINDO (Coordinador) - "Gobierno, Derecho y Tecnología: las actividades de los Poderes públicos" (Thomson Civitas, Madrid, 2006), pág. 315 y sigtes.*

33 *Carlos E. GUARIGLIA - "El conflicto entre los derechos fundamentales" (A.M.F., Montevideo, 2007), pág. 310 y sigtes.*

34 *Juan CIANCIARDO - "El conflictivismo en los derechos fundamentales" (Eunsa, Pamplona, 2000).*

35 *Luis PRIETO SANCHIS - "Constitucionalismo y garantismo", en Miguel CARBONELL y Pedro SALAZAR (Editores) - "Garantismo" (Trotta, Madrid, 2005), pág. 48 y sigtes.*

36 *Carlos E. DELPIAZZO – "Derecho Administrativo General" (A.M.F., Montevideo, 2015), volumen 1, segunda edición actualizada y ampliada, pág. 38 y sigtes.*

37 *Germán BIDART CAMPOS - "Teoría General de los Derechos Humanos" (UNAM, México, 1989), pág. 147.*

38 *Pedro SERNA y Fernando TOLLER - "Interpretación Constitucional de los Derechos Fundamentales" (La Ley, Buenos Aires, 2000), págs. 38 y 39.*

39 *Pedro SERNA y Fernando TOLLER - "Interpretación Constitucional de los Derechos Fundamentales" cit., pág. 7.*

40 *Eduardo ESTEVA GALLICCHIO - "Los conflictos entre el derecho a la información y el derecho al honor en el Derecho comparado", en Revista de Derecho de la Universidad de Montevideo (Montevideo, 2002), Año I, Nº 1, pág. 92.*

El problema de los métodos referidos -de la jerarquización y de la ponderación- es que llevan implícito que los dos derechos alegados existen en el caso concreto, pero uno de ellos debe sacrificarse en aras de un contrincante superior en abstracto y a priori -tal es el caso de la jerarquización- o superior en concreto -como ocurre con el método del balance- lo que elimina matices y multiplica las falsas oposiciones: derecho de información o derecho al honor, libertad de la mujer o vida del concebido o nacido, libertad de empresa o justicia social, ecología o desarrollo, ocupación o propiedad.

Por eso, partiendo de la necesaria interpretación armónica de los derechos, impuesta no sólo por la unidad del sujeto humano, sino también por la regla general de interpretación constitucional sistemática, en casos de concurrencia de derechos, la labor del intérprete debe centrarse en pensar cada uno de los derechos en juego desde su *contenido esencial*, a efectos de determinar, no el "peso" concreto de los mismos para apreciar cuál es más importante o cuál debe rendirse, sino cuál de ellos comparece y cuál no en el caso concreto.

Determinar el contenido esencial de un derecho implica mirar hacia los límites internos de cada derecho en litigio, hacia su naturaleza, hacia el bien que protegen, hacia su finalidad y su ejercicio funcional; es atender a sus respectivos contornos y a sus esferas de funcionamiento razonable. El contenido esencial no es la última valla, que defiende un pequeño reducto inexpugnable para que aún pueda decirse que existe el derecho, sino que implica el amplio ámbito de ejercicio razonable de un derecho que, una vez definido en general y determinado en las circunstancias concretas, es absoluto, inexcepcionable, y no puede ser dejado de lado por razones utilitarias [41].

Desde un enfoque particular, el equilibrio entre el derecho a la información (y su desprendimiento, el derecho de acceso a la información pública) por una parte, y el derecho a la protección de datos personales (ubicado concéntricamente con los derechos a la intimidad y a la privacidad) por otra parte, aboga a favor de este último cuando existen datos personales en poder de la Administración susceptibles de ser accedidos no sólo por el titular sino por terceros[42].

Varias razones respaldan tal afirmación, que se sustenta en consideraciones que hacen a la diversa naturaleza de la información en juego, a los bienes jurídicos a ponderar, a los fines y, en definitiva, al contenido esencial de cada uno de ambos derechos.

En primer lugar, debe atenderse a la *diferente naturaleza de la información* de que se trata en uno y otro caso; no puede confundirse la información pública con los datos personales que puedan formar parte de expedientes o registros administrativos. Ello significa que el derecho de acceso por cualquier ciudadano a la información en poder de las Administraciones públicas no alcanza a toda la información sino específicamente a la calificable como pública [43], la cual no comprende a la de carácter privado o personal ni a las secretas por imperio de la ley dictada en razón del interés general.

En segundo lugar, coadyuva con lo anterior la determinación del *bien jurídico tutelado*, el cual impone la reserva sobre lo íntimo de cada persona. El que los datos personales se encuentren en poder de la Administración no implica que su tratamiento esté liberado de la observancia del régimen protector ni mucho menos que puedan procesarse con cualquier propósito distinto al que motivó su colecta sin consentimiento del interesado [44].

En tercer lugar, no puede dejar de considerarse la *diversidad de fines* que persigue cada derecho en el conjunto de los demás derechos. Si el ejercicio de un derecho afecta la consecución de la finalidad de otro, entonces habrá que examinar si la finalidad que persigue el primero se encuentra en correspondencia con la finalidad que persigue el segundo [45]. En la especie, es evidente que el ejercicio del derecho de acceso a la información pública, si no respeta el límite de la información privada, desvirtúa su fin. A su vez, la reserva de los datos personales no afecta el contenido esencial del derecho de acceso a los documentos administrativos.

En cuarto lugar, lo antedicho resulta corroborado porque la argumentación teleológica permite determinar el *contenido esencial* de cada derecho, impidiendo su desfiguración. En el caso, el núcleo duro determinante del derecho a la protección

41 *Carlos E. DELPIAZZO y Andrés ROBAINA RAGGIO - "Estado de Derecho y ocupaciones", en Rev. de Derecho de la Universidad de Montevideo (Montevideo, 2006), Año V, Nº 9, pág. 10.*

42 *Carlos E. DELPIAZZO - "Relaciones entre privacidad y transparencia. ¿Equilibrio o conflicto?", en Guillermo TENORIO (Coordinador) – "Los datos personales en México" (Porrúa – Universidad Panamericana, México, 2012), pág. 3 y sigtes.*

43 *Marcela I. BASTERRA - "El derecho fundamental de acceso a la información pública" cit., págs. 411 y sigtes. y 416 y sigtes.*

44 *Angel Daniel OLIVER-LALANA - "Internet como fuente de información accesible al público: pensando en el derecho de protección de datos en su contexto social y jurídico", en Rev. de Contratación Electrónica, Año 2006, Nº 77, pág. 24.*

45 *Carlos E. GUARIGLIA - "El conflicto entre los derechos fundamentales" cit., pág. 407.*

de los datos personales es la dignidad humana [46] mientras que el derecho de acceso a la información pública se sustenta en la transparencia connatural a la servicialidad de la Administración [47].

Finalmente, los principios generales antes referidos confirman el equilibrio que debe (teóricamente) y puede (prácticamente) reinar entre los derechos bajo examen. En especial, los principios de reserva y publicidad, que aparecen como opuestos entre sí, no lo son si se consideran los respectivos objetos informativos sobre los que aplican y la diferente naturaleza jurídica de los mismos: la información privada consistente en datos personales por un lado y la información pública por otro [48].

CONCLUSIÓN

Desde el punto de vista ético, volviendo a la enseñanza del Papa Francisco, cabe coincidir en que "es posible volver a ampliar la mirada, y la libertad humana es capaz de limitar la técnica, orientarla y colocarla al servicio de otro tipo de progreso más sano, más humano, más social, más integral" en la medida que se "tome conciencia de que el avance de la ciencia y de la técnica no equivale al avance de la humanidad y de la historia" [49].

Desde el punto de vista conceptual, en relación al tema específico que nos ocupa, es preciso afirmar el equilibrio como solución de principio, tanto desde el punto de vista sustancial como instrumental.

Sustancialmente, la circulación de información entre las Administraciones y su acceso amplio por los habitantes (en ejercicio de su derecho de acceso) debe referir a la ***información pública***, mientras que, al revés, la protección de la privacidad de las personas obligará a las Administraciones a cautelar la ***información privada*** referente a ellas. Ello es así porque, según ha quedado demostrado, los respectivos contenidos esenciales de ambos derechos abogan por la tutela de los distintos tipos de información: pública en un caso y privada en el otro.

Por otra parte, *instrumentalmente*, la interoperabilidad debe ser funcional a la ***información pública*** de que disponen las Administraciones pero puede conspirar contra la privacidad si se extiende sin más a la ***información privada*** de cada individuo que esté en poder de aquellas.

Desde el punto de vista jurídico, lo que subyace a la cuestión planteada es la calidad del Estado de Derecho, al que todos debemos aportar nuestro esfuerzo y sin cuya plena vigencia y perfeccionamiento cotidiano vano es pensar en la tutela de los derechos fundamentales de última generación.

En efecto, la proclamación del Estado constitucional de Derecho de nuestros días revaloriza y acentúa la centralidad de la persona humana, como lo reconoce el art. 1º de la Constitución alemana al proclamar que "La dignidad humana es intangible".

Como bien se ha puesto de manifiesto, asistimos a la instalación de nuevos paradigmas del Derecho público, entre los cuales el principio "pro homine", sustentado en la dignidad de la persona, refuerza la visión instrumental de las instituciones al servicio de los derechos fundamentales [50]

Por eso, "Hoy en día en el mundo occidental se afirma lo que se ha llamado el Estado constitucional de Derecho, basado en la primacía de la Constitución o, mejor dicho, del bloque de la constitucionalidad... Ese bloque de constitucionalidad reposa en la dignidad de la persona humana" [51].

Y tal dignidad no deriva de ningún tratado, Constitución o ley sino que es innata a la naturaleza humana [52], por lo que el aludido bloque de constitucionalidad comprende los derechos humanos reconocidos o no por la Constitución, contenidos o no en las convenciones internacionales [53].

Siendo así, en el marco de las relaciones de la Administración (servicial) con los administrados (cada persona y sus comunidades intermedias), éstos ostentan una posición de centralidad que, no obstante, no lo exonera de deberes y responsabilidades. Pero son mayores los de la Administración como consecuencia de su propia naturaleza instrumental, de su ser para cada uno de los integrantes del cuerpo social a los que se debe vicarialmente.

46 *Carlos E. DELPIAZZO – "Dignidad humana y Derecho" cit., pág. 27 y sigtes.; Héctor GROS ESPIELL – "La dignidad humana en los instrumentos internacionales de derechos humanos", en CATEDRA UNESCO DE DERECHOS HUMANOS – "Dignidad Humana" (Universidad de la República, Montevideo, 2003), pág. 9 y sigtes.; y José Aníbal CAGNONI – "La dignidad humana. Naturaleza y alcances", en Rev. de Derecho Público (Montevideo, 2003), Nº 23, pág. 11 y sigtes.*

47 *Carlos E. DELPIAZZO – "Derecho Administrativo Uruguayo" (Porrúa – UNAM, México, 2005), pág. 7 y sigtes.*

48 *Carlos E. DELPIAZZO – "¿Qué es el habeas data", en Rev. CADE de Doctrina y Jurisprudencia (Montevideo, 2009), tomo I, pág. 35 y sigtes.*

49 *Papa FRANCISCO – Carta Enciclica Laudato Si', Nº 112 y 113.*

50 *Juan Carlos CASSAGNE – "El acto administrativo. Teoría y régimen jurídico" cit., pág. 67 y sigtes.*

51 *Mariano R. BRITO – "La dignidad humana como fundamento de nuestro Derecho Administrativo" cit., pág. 164.*

52 *Jesús GONZALEZ PEREZ – "La dignidad de la persona humana y el Derecho Administrativo" cit., pág. 6.*

53 *Augusto DURAN MARTINEZ – "Neoconstitucionalismo y Derecho Administrativo" (La Ley Uruguay, Buenos Aires, 2012), pág. 845.*

RETOS DE LA PROTECCIÓN DE DATOS EN UN MUNDO GLOBALIZADO

MAR
ESPAÑA MARTÍ

Dirige la Agencia Española de Protección de Datos y ostenta su representación.
Es Licenciada en Derecho por la Universidad Pontificia Comillas, ICADE (1987) Madrid.
Previo a su designación se desempeñó como asesora en el Ministerio de Hacienda y Administraciones Públicas (hasta junio 2015), como Viceconsejera de Presidencia y Administraciones Públicas en la Junta de Comunidades de Castilla-La Mancha (desde 2012 a 2015) y como Secretaria General de la Consejería de Presidencia y Administraciones Públicas en la Junta de Comunidades en Castilla-La Mancha (desde 2011 hasta 2012), entre otras. Fue Profesora del Máster de Protección Internacional de Derechos Humanos de la Universidad de Alcalá (desde 2006 hasta 2010), Profesora del Master de Acción Política organizado por el Colegio de Abogados y la Universidad Rey Juan Carlos (desde 2005 hasta 2009) y Profesora Colaboradora de Derecho Administrativo en ICADE (en los años 1990-1991, 1991-1992).

SUMARIO

RESUMEN

El artículo analiza las iniciativas que en forma prioritaria ha llevado adelante la Agencia Española de Protección de Datos para responder a los desafíos que las nuevas tecnologías han traído a la vida cotidiana, y los riesgos que emanan de las mismas para la protección de datos personales.

Se hace expresa referencia al Plan Estratégico 2015-2019, siendo uno de sus pilares la prevención, con más de medio centenar de actuaciones para proteger de forma más eficaz a los ciudadanos. Se señala la concientización y sensibilización ciudadana como uno de los ejes principales de la actuación de la Agencia Española, buscando potenciar la cultura proactiva de los ciudadanos.

La gestión transparente de los datos, y vinculada a ésta la información clara y transparente por los responsables hacia los usuarios es uno de los grandes retos de la protección de datos.

La protección de los menores de edad -especialmente en internet-, la contratación irregular de servicios y la inclusión indebida en ficheros de morosidad, la evaluación de las implicancias de las nuevas tecnologías en la privacidad y la colaboración entre los distintos actores en la gestión de datos son temas especialmente tratados en el artículo, indicando las iniciativas realizadas en estas materias.

Finalmente, se detalla el impacto del nuevo marco europeo de la protección de datos reflejado en la entrada en vigor del nuevo Reglamento General de Protección de Datos de la Unión Europea.

INTRODUCCIÓN

Es para mí un honor haber sido invitada a participar en el primer número de la Revista Académica de Protección de Datos Personales de la Unidad Reguladora y de Control de Datos Personales de Uruguay. La protección de datos se enfrenta a retos decisivos derivados, en gran medida, del mundo hiperconectado en el que vivimos. El avance de las nuevas tecnologías ha aumentado las perspectivas de beneficios económicos para una gran variedad de empresas, que ven en fenómenos como el big data o el internet de las cosas posibilidades de negocio sin precedentes. La Agencia Española de Protección de Datos (AEPD) ha hecho una apuesta decidida por el fomento de la innovación, manteniendo a la vez que esta no puede desarrollarse de forma plena sin la confianza de los usuarios para los que han sido diseñados los productos y servicios. Para mantener esa confianza, se hace imprescindible que los usuarios mantengan el control sobre su propia información personal, que sean conscientes de quién y para qué se recogen sus datos, tras haberle proporcionado la información necesaria.

Existe un consenso generalizado sobre las ventajas y las posibilidades que aportan las nuevas tecnologías a la vida cotidiana de los ciudadanos, pero también sobre los riesgos que emanan de las mismas en relación a la protección de datos de carácter personal. En particular, la pérdida de control sobre el flujo de información que sobre nosotros se genera de forma continua, las limitaciones en el ejercicio de derechos derivadas de la falta de transparencia, las dificultades a la hora de gestionar el consentimiento y la complejidad de adaptar el tratamiento a las preferencias del usuario. Incluso, simplemente, el hecho de que no se ofrezca al ciudadano un entorno amigable en el que este pueda manifestar de forma sencilla y sin procedimientos enrevesados qué utilización quiere que se haga de su información personal.

Nos encontramos en un momento en el que las proyecciones a diez años hablan de un billón de objetos inteligentes interconectados y dotados de autonomía y en el que se transfiere la capacidad de decisión en entornos complejos hacia algoritmos capaces de procesar información procedente de un gran número de fuentes heterogéneas.

Estamos, por tanto, ante un panorama que genera preocupación entre las Autoridades de protección de datos. La Agencia Española de Protección de Datos se ha propuesto unas líneas de trabajo prioritarias para responder a los desafíos inmediatos, poniendo en marcha a la vez una serie de actuaciones que tratan de dar respuesta a los temas que más incidencia pueden llegar a tener en la vida de las personas. En la Agencia presentamos a finales del año pasado nuestro Plan Estratégico 2015-2019, que incluye actuaciones que han sido específicamente diseñadas para dar respuesta a los retos actuales. El Plan prevé entre otras actuaciones la elaboración o actualización más de una veintena de guías, e incluye más de 100 actuaciones que la Agencia pretende poner en marcha, y que pueden ser consultadas en detalle en nuestra página web.

Uno de los pilares del Plan Estratégico es la prevención. Para el desarrollo de este eje, se ha previsto la ejecución de medio centenar de actuaciones cuyo fin es una protección más eficaz de ciudadano. Entre ellas se encuentra, por ejemplo,

la de auditar las políticas de privacidad en la prestación de servicios en internet y ofrecer materiales útiles para el ciudadano que les ayuden a configurar adecuadamente sus perfiles en redes sociales, la puesta en marcha de un canal de comunicación dirigido a centros educativos, docentes, padres y menores, aspectos estos ya en funcionamiento. También trabajar en ámbitos con un gran impacto sobre la privacidad, como el tratamiento de datos en el sector sanitario o la contratación irregular, que implica en muchos casos la inclusión del ciudadano en un fichero de morosos. Para abordar estos temas, en la Agencia estamos trabajando con los diferentes colectivos y tenemos previsto realizar tanto actuaciones de concienciación como reuniones con los actores implicados. A estas actuaciones me referiré de manera más extensa a lo largo del artículo, ya que en la AEPD consideramos la prevención como uno de los elementos de mayor relevancia para garantizar una protección eficaz de los derechos de los ciudadanos, sin olvidar el ejercicio de la potestad sancionadora cuando haya quedado acreditado el incumplimiento de la normativa. Por otro lado, es preciso que la Agencia, como Autoridad de fiscalización y control, esté atenta a la evolución y el impacto de las nuevas tecnologías. En consecuencia, el desarrollo del Plan Estratégico 2015-2019 contempla la puesta en marcha de la Unidad de Evaluación y Estudios Tecnológicos para detectar y analizar tendencias, productos o servicios que puedan tener un impacto en la privacidad y la protección de datos de los ciudadanos, un área que se describirá con mayor detalle en otro de los espacios de este artículo. Por último, no es posible analizar los nuevos retos de la protección de datos sin tener presente el nuevo Reglamento europeo, el nuevo marco legal que se utilizará como referencia para hacer frente a los desafíos en materia de protección de datos.

CONCIENCIACIÓN Y SENSIBILIZACIÓN CIUDADANA

Uno de los ejes principales de actuación de la AEPD es apostar de forma decidida por la concienciación y la sensibilización de los ciudadanos. En este mundo globalizado se hace cada día más evidente la necesidad de ofrecerles sistemas que les permitan mantener el control sobre su información personal para que puedan, en cualquier momento, modificar sus preferencias de privacidad. Una gestión proactiva que, sin perder de vista las obligaciones que deben cumplir los responsables y que están definidas en el marco normativo, empodera a los ciudadanos para decidir, por ejemplo, qué información quieren compartir y con quién cuando utilizan determinados servicios de internet.

Para potenciar esta cultura proactiva de la privacidad entre los ciudadanos es fundamental que la AEPD, como organismo público encargado de velar por el conocimiento y la difusión de este derecho fundamental, les proporcione información clara y precisa sobre cuáles son los riesgos a los que se enfrentan cuando utilizan determinados servicios y cuál es la mejor manera de minimizarlos.

En este sentido, la Agencia está ultimando el proyecto "Privacidad y Seguridad en internet. Guía esencial" que, en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), proporciona a los usuarios de internet, en un lenguaje claro y sencillo, información práctica sobre cómo proteger los dispositivos portátiles; cómo generar y gestionar contraseñas; en qué consiste la verificación en dos pasos; cómo realizar copias de seguridad o proteger el correo electrónico; gestionar la información que se almacena en la nube; los riesgos en los servicios de mensajería instantánea; el phising; la protección de redes WiFi; el control parental o los wearables, así como la forma en la que pueden ejercerse los derechos en internet, en particular, el denominado derecho al olvido.

El proyecto, que incluye fichas y vídeos, ha sido realizado junto con el INCIBE, ya que la colaboración con otras entidades es importante para aglutinar esfuerzos y establecer sinergias. Consideramos que la colaboración con otros organismos es imprescindible para reforzar y ampliar la difusión de los proyectos y, en consecuencia, fortalecer las herramientas que se ponen a disposición de los ciudadanos. Ellos, los titulares de los datos, deben ser parte imprescindible de cualquier estrategia de protección, siendo conscientes de las múltiples situaciones en que sus datos pueden ser tratados, de cómo afectan esos tratamientos a sus derechos y de cómo pueden mantener el control sobre ellos.

El proyecto "Privacidad y Seguridad en internet. Guía esencial" se articula en torno a dieciocho fichas, que condensan información esencial en una página, con infografías y partiendo de las situaciones reales en las que se pueden encontrar los internautas; y seis vídeos que muestran cómo configurar las opciones de privacidad en seis de los servicios más populares de internet. Además, en los videotutoriales se muestra la forma en que se puede acceder a las configuraciones de privacidad y seguridad en servicios como Instagram, Facebook, Twitter, Whatsapp, Snapchat y YouTube para presentar a los ciudadanos cómo pueden elegir las opciones que les ofrecen una mayor protección en términos de acceso a los datos por terceros, quién puede buscarnos o ponerse en contacto con nosotros, etiquetado de nuestras fotos,

bloqueo de otros usuarios, aplicaciones vinculadas u opciones de geolocalización, entre otras.

El formato de esta guía, al estar sus contenidos diseñados en fichas independientes y autónomas, permite crecer de forma dinámica e incluir nuevos materiales de una manera sencilla. Esa misma filosofía acompaña a los videotutoriales, a los que se pueden unir distintos elementos si la aparición de nuevas herramientas y servicios de internet así lo aconsejan.

Además, la guía puede utilizarse de manera diferente por personas con intereses o necesidades distintas. En efecto, aquellos que deseen tener una visión global y completa la pueden leer de una manera secuencial de principio a fin. Pero otras, con interés en algún tema concreto, pueden consultar exclusivamente la ficha o fichas que les resulten de interés. Y lo mismo sucede con los vídeos. Desde la Agencia esperamos que estas herramientas resulten de interés a los ciudadanos, les ayuden a gestionar de una manera más adecuada su privacidad y les inviten a un uso responsable de las grandes oportunidades que ofrece la tecnología minimizando los riesgos para su privacidad.

HACIA UNA GESTIÓN TRANSPARENTE DE LOS DATOS

Anteriormente he mencionado que los responsables, aquellos que tratan datos, tienen unas obligaciones que deben cumplir. Uno de los grandes retos a los que se enfrenta la protección de datos personales es conseguir que los responsables de tratamiento y, en particular, todos aquellos que procesan datos de cientos de millones de usuarios y operan a escala mundial, informen a los ciudadanos de una manera clara y transparente.

En la Agencia hemos tenido importantes divergencias con grandes compañías tecnológicas que operan en internet, que llegaron a argumentar que, al ser empresas estadounidenses, no les era de aplicación la legislación española y europea de protección de datos, y que por tanto los ciudadanos debían reclamar sus derechos en EEUU. En el caso de Google vs. Agencia Española de Protección de Datos, fue necesario llegar al Tribunal de Justicia de la Unión Europea para defender los derechos de los ciudadanos y que este consagrase, en primer lugar, que los tratamientos que realiza la compañía están sometidos a las normas de protección de datos de la Unión Europea y, en segundo lugar, el denominado derecho al olvido, es decir, que las personas tienen derecho a solicitar del motor de búsqueda, con las condiciones establecidas en legislación de protección de datos, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación. De hecho, el Reglamento europeo de protección de datos recoge el "derecho al olvido" siguiendo el camino establecido por el Tribunal de Justicia, que lo señaló como una adaptación de los derechos de cancelación y oposición. Tras la sentencia del Tribunal, la situación ha mejorado de manera considerable no sólo en una materia como el derecho al olvido en la que el pronunciamiento es claro, sino también en otros ámbitos.

No es posible hablar de transparencia por parte de las compañías si no se habla de las políticas de privacidad, que se han convertido en el instrumento por antonomasia para proporcionar información a los usuarios de una manera sistemática y estructurada pero que, en demasiadas ocasiones, son complejas, extensas y casuísticas, dificultando la comprensión de las mismas. En otras ocasiones, servicios diferentes del mismo proveedor tienen políticas de privacidad distintas, lo que genera aún mayor confusión entre los ciudadanos.

En este ámbito, la Agencia Española de Protección de Datos, tras examinar las políticas de privacidad de Google y encontrar que no se ajustaban a lo exigido por la legislación española, además de las correspondientes actuaciones sancionadoras, instó a Google a adaptar las mismas a lo requerido por el ordenamiento jurídico.

Fruto de estas actuaciones, la Agencia ha promovido que Google introduzca modificaciones significativas a nivel mundial en materia de información, consentimiento y ejercicio de derechos, áreas sobre las que la AEPD le requirió que hiciese cambios. Además, la compañía se ha comprometido a adoptar medidas adicionales específicamente solicitadas por la Agencia y a mantener un diálogo constante tanto sobre la aplicación de nuevas medidas como a informar de futuros cambios que puedan producirse.

LA IMPRESCINDIBLE PROTECCIÓN DE LOS MENORES

Como se ha mencionado con anterioridad, los retos que para la protección de datos de carácter personal y la privacidad supone la espectacular evolución que están experimentado las tecnologías de la información y la comunicación (TIC), especialmente en internet, son difíciles de explorar. Internet y los servicios que se proporcionan a través de la Red han transformado profundamente nuestra sociedad, sin que estemos en condiciones de evaluar plenamente las consecuencias que implica para los derechos fundamentales y las libertades públicas de las personas, lo que resulta especial-

mente preocupante cuando se trata de menores de edad (niños y adolescentes).

No se ha establecido una edad determinada para comenzar a navegar por internet, pero lo que resulta indudable es que cada vez es más temprana. La Comisión Europea en 2012 la fijó en una media de 7 años y algunos estudios la reducen aún más. Además, los menores son grandes consumidores de los servicios que proporciona internet, que manejan de modo natural porque desde su nacimiento forma parte de sus vidas. De los 10 a los 15 años el uso de internet se vuelve prácticamente universal y se realiza de manera intensiva.

Esta integración innata de la tecnología en las vidas de los menores no implica en modo alguno que estos sean conscientes de los riesgos que un uso inapropiado puede llegar a tener. Son personas en fase de formación, por lo que no conocen plenamente el valor de la privacidad y la importancia que para su salvaguarda supone el buen uso de la información de carácter personal. Ello, a su vez, les lleva en numerosas ocasiones a actuar con cierta despreocupación y a una sobreexposición de sus propias vidas, pudiendo llegar a facilitar la comisión de conductas no deseadas, de las que tanto pueden ser víctimas como autores.

Que sean "nativos digitales" no implica que estén dotados de un alto grado de madurez. De hecho, ya se habla del término "huérfanos digitales" cuando, como ocurre con cierta frecuencia, padres y profesores carecen de las competencias digitales necesarias para guiarles y aconsejarles.

Partiendo de esta evidencia, la Agencia Española de Protección de Datos, en apuesta por la prevención como método para garantizar y reforzar la protección de las personas, ha estableciendo una línea prioritaria dirigida a la "Protección a los menores y educación", que incluye un conjunto de medidas y acciones destinadas a informar, formar y sensibilizar a los menores, así como a padres y profesores, para dotarles de conocimientos y herramientas con las que afrontar la tarea de educar a las nuevas generaciones. En este sentido, también hay que destacar la labor realizada por la Unidad Reguladora y de Control de Datos Personales de Uruguay en el ámbito educativo, con iniciativas como la capacitación de docentes o el concurso anual para niños de 11 y 12 años, además de la elaboración de diversos materiales.

La protección de los menores en la Red es compleja y afecta a muchos y variados actores, pues se plantea desde diferentes perspectivas. Por ello, uno de los principios en los que se basa la línea de actuación de la AEPD es la colaboración con aquellas instituciones y agentes involucrados en la protección de los menores. Aunar esfuerzos y disponer de recursos en común resulta esencial para afrontar un asunto tan polifacético.

La Agencia ha establecido una colaboración con el Ministerio de Educación, Cultura y Deporte, que se plasmó en la suscripción de un convenio, con el objetivo final de formar y sensibilizar a los menores en materia de privacidad y protección de datos en el uso de las TIC a través de un conjunto de actuaciones que, además de los propios menores, tienen como destinatarios también a los padres y los profesores, y que sirve de cauce para la comunicación con las Administraciones educativas de las distintas Comunidades Autónomas.

Profundizando en ese objetivo de facilitar la comunicación con los jóvenes, padres y profesores hay que destacar la reforma integral del portal de la Agencia dirigido tanto a concienciar a los menores como a facilitar materiales a padres y profesores, una página (www.tudecideseninternet.es) que integra todas las iniciativas, materiales educativos, juegos, enlaces e información de interés y ayuda en esta materia. A ello hay que sumar la reciente convocatoria de un premio dedicado a las buenas prácticas que los centros educativos hayan desarrollado en materia de privacidad y uso adecuado de internet, así como a la trayectoria profesional en este ámbito, dentro de la convocatoria anual de premios de la Agencia.

Además, la Agencia ha trabajado en el establecimiento de un canal específico de comunicación para todas aquellas cuestiones o dudas que se tengan relacionadas con la privacidad y el tratamiento de datos de menores de edad, así como los que ellos realizan. Este canal incorpora una línea telefónica, una dirección de correo electrónico y una línea de Whatsapp. Desde que entró en funcionamiento, a mediados de octubre de 2015, ha acumulado, junto con las consultas que llegan a través de la sede electrónica de la Agencia, más de 400 comunicaciones en su mayoría procedentes de padres y educadores.

En ese sentido, la Agencia también ha trabajado en la elaboración de varias guías destinadas a la formación y sensibilización de los menores de 10 a 14 años ('No te enredes en internet' y 'Sé legal'; y 'Guíales en internet' y 'Enséñales a ser legales'), que cuentan con una versión para padres y profesores. Son recursos educativos en formato de fichas para facilitar el aprendizaje sobre la privacidad, qué son los datos personales, qué pueden revelar, qué derechos se pueden ejercer, etc., así como para dar a conocer y concienciar sobre determinadas conductas en internet que causan daños a terceros y pueden llegar a ser constitutivas

de delitos, y que en ocasiones se realizan por mero desconocimiento y a veces por una sensación de falso anonimato e impunidad. Continuando con esa colaboración entre organismos públicos que ya se ha mencionado en otros apartados de este artículo, en la elaboración de estas guías también han colaborado aquellas instituciones y organismos con competencias en la materia. Además, en estos momentos se está trabajando en la elaboración de nuevos materiales en formato audiovisual que faciliten la labor del educador, ya sean padres o profesores, explicando cada uno de los contenidos de una forma sencilla y práctica.

En estrecha relación con el objetivo de reforzar la protección de los menores, se está trabajando en la elaboración de una guía para los centros educativos, sus equipos directivos y los profesores con la que dar respuesta a las distintas situaciones que en devenir habitual de la labor docente se les presenten y tengan que ver con el tratamiento de datos de carácter personal, así como en el diseño de talleres para que padres y familiares dispongan de los conocimientos necesarios para supervisar y guiar a sus hijos en internet.

En definitiva, se trata de una línea de actuación prioritaria y con vocación de continuidad que tiene como finalidad última que los menores puedan aprovechar todas las ventajas y oportunidades que las TIC les ofrecen con la máxima seguridad posible, y cuya estrategia para su consecución se apoya en la prevención y la colaboración.

CONTRATACIÓN IRREGULAR Y FICHEROS DE SOLVENCIA

La contratación irregular de servicios y la inclusión indebida en ficheros de morosidad constituye una de las principales fuentes de reclamaciones ante la Agencia Española de Protección de Datos y supone el mayor volumen de sanciones impuestas. En el año 2015 las sanciones declaradas en los sectores de telecomunicaciones y suministro y comercialización de energía ascendieron a un total de 8.295.006 euros, lo que supone el 60,49% de las impuestas por la AEPD. Los principales sectores afectados son los de telecomunicaciones y suministro de energía.

El incremento de la competencia en sectores de la actividad económica liberalizados como las telecomunicaciones o el suministro de energía en sus distintas modalidades ha generado el desarrollo de prácticas comerciales más agresivas por parte de los prestadores de servicios esenciales para los ciudadanos. La puesta en práctica de estas políticas comerciales se ha llevado a cabo en un entorno caracterizado, entre otras circunstancias, por el impulso de nuevos modelos de comercialización de productos y servicios a través de redes de distribución en las que se multiplican los puntos de contratación gestionados por terceras entidades vinculadas a los suministradores de estos servicios pero ajenas a su propia organización. A ello hay que sumar el fomento de modalidades de contratación a distancia a través de la telefonía e internet y el incremento de las opciones de portabilidad de la contratación de unas compañías a otras manteniendo la titularidad de las líneas de telecomunicaciones contratadas como instrumento que facilite la competencia entre las empresas.

El conjunto de circunstancias que se han descrito ha generado dificultades para la identificación inequívoca de los clientes que contratan estos servicios (contratación a distancia y portabilidad) y ha incentivado prácticas desleales por parte de los comercializadores con el fin de incrementar el número de clientes y las comisiones que perciben por su contratación.

Las debilidades en la identificación de los nuevos clientes ha generado prácticas ilícitas de suplantación de la identidad, con la consecuencia de que se facturan los servicios a personas que no los han contratado. Ello conlleva que las personas suplantadas rechazan el pago de los servicios y los impagos dan lugar tanto a intensas políticas de recobro por parte de los suministradores de servicios como a la inclusión de estos ciudadanos en los denominados ficheros comunes de morosidad. Esta inclusión ilícita en ficheros de morosidad se mantiene incluso en los casos en que los ciudadanos impugnan la deuda ante un órgano competente para resolver la reclamación (juzgados, juntas arbitrales de consumo o administración competente en la materia), cuestionando su existencia o cuantía.

El acceso generalizado a estos ficheros por todo tipo de entidades genera una importante lesión en los derechos de los afectados, que ven restringidas sus posibilidades de acceso a numerosos servicios que les son denegados o condicionados por figurar en dichos ficheros.

En el marco de la normativa de protección de datos personales estas conductas suponen la infracción de dos principios básicos: el tratamiento de datos de los ciudadanos suplantados sin consentimiento (art. 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el principio de calidad de datos por inclusión de información inexacta en los ficheros de morosidad (art. 4 LOPD).

La responsabilidad de estas prácticas se imputa tanto a las redes de comercialización como a los propios suministradores de estos servicios por la

falta de diligencia en la comprobación efectiva de la identidad de los clientes en los contratos que son tramitados por aquellos.

Ante esta situación, la Agencia concluyó en el año 2012 una inspección sectorial de carácter preventivo con el fin de auditar los principales incumplimientos de la LOPD y formular unas recomendaciones que permitieran evitarlas o, al menos, minimizarlas. Atendiendo a los problemas detectados, las principales recomendaciones fueron que en los contratos escritos y firmados es necesario recabar y conservar documentación acreditativa de la identidad del contratante (copia de DNI u otro documento acreditativo de la identidad). En las grabaciones donde consta el consentimiento para la contratación es obligatorio garantizar la autenticidad, la integridad y la identificación fiable de los manifestantes y la no alteración del contenido de lo manifestado, así como el momento de su emisión y recepción. Por último, en los casos de contratación por internet, sería recomendable habilitar la utilización de firma electrónica avanzada del contratante. En su defecto se deberán implantar medidas que garanticen la identidad del contratante.

La relevancia de la inserción indebida en ficheros de solvencia y su incidencia negativa en los derechos de los ciudadanos ha determinado la inclusión en el Plan Estratégico 2015-2019 de nuevas acciones proactivas dirigidas a garantizar el cumplimiento de la LOPD. Estas acciones se han concretado en la celebración de reuniones con las empresas que operan en los principales sectores afectados, así como con los responsables de los ficheros comunes de morosidad, para informarles de las deficiencias ya constatadas y requerirles iniciativas para su resolución.

La Agencia ha previsto completar estas iniciativas con la elaboración de un documento que describa las competencias propias de la AEPD, las Autoridades de consumo y las de la Secretaría de Estado de Telecomunicaciones y Servicios de la Sociedad de la Información (SETSI), de forma que los ciudadanos puedan conocer con claridad a quién deben acudir en defensa de sus derechos, en un entorno en que los límites de dichas competencias en ocasiones pueden resultar difusos. Además, la AEPD prevé actualizar el Plan sectorial de oficio sobre el tratamiento de datos en la contratación telefónica y a través de internet, por ser las actividades en las que se constata el mayor volumen de incumplimientos. A estos proyectos se va a sumar la elaboración de materiales prácticos y la creación de una sección online específica de preguntas frecuentes planteadas por los ciudadanos (FAQs).

CREACIÓN DE LA UNIDAD DE EVALUACIÓN Y ESTUDIOS TECNOLÓGICOS

La Agencia Española de Protección de Datos ha establecido como objetivo prioritario en su Plan Estratégico 2015-2019 el apoyo a aquellas iniciativas que contribuyan a generar un clima de confianza en el ámbito de la economía digital y en los usos de la tecnología por los sectores público y privado, favoreciendo la competitividad de las empresas, el desarrollo y la innovación de las industrias TIC y creando un ambiente propicio de cumplimiento normativo en materia de privacidad.

Además, otro de sus objetivos clave es impulsar una labor proactiva de la AEPD que permita detectar el impacto que los nuevos productos y servicios tecnológicos pueden tener en la privacidad de los ciudadanos, impulsando la introducción, desde las primeras fases de su desarrollo, de los requerimientos de la legislación de protección de datos.

Para dar cuenta de este interés de la Agencia por conjugar la necesidad de la promoción de la investigación y la innovación en España como motores de nuestra economía con el respeto a los derechos de las personas, uno de los ejes estratégicos se ocupa especialmente de este apartado.

Ese eje, denominado "Innovación y protección de datos: factor de confianza y garantía de calidad", engloba un total de once iniciativas encaminadas a impulsar una labor proactiva en la Agencia que permita detectar el impacto de los nuevos desarrollos tecnológicos en la privacidad de los ciudadanos, favoreciendo la introducción de políticas de protección de datos desde el diseño para garantizar que los derechos de los ciudadanos y de su privacidad está presente en todas las fases de concepción, análisis e implantación de dichos desarrollos tecnológicos.

Entre dichas iniciativas es necesario destacar la creación de la Unidad de Evaluación y Estudios Tecnológicos (UEET), que nace con la misión de evaluar las implicaciones para la privacidad de las nuevas tecnologías, realizando estudios prospectivos y análisis de los productos y servicios para conocer de primera mano sus funcionalidades y la forma en que almacenan, tratan y comunican los datos personales que recogen, así como la transparencia con la que se llevan a cabo estos tratamientos.

Estos estudios se centrarán en las tecnologías más actuales y que tengan un mayor impacto en la privacidad de las personas como los relativos a los diversos aspectos de la llamada sociedad conectada, que cubrirían temas como big data, internet de las cosas, device fingerprinting, el mundo smart

(smart cities, smart cars, smart homes, smart workplaces), aplicaciones móviles, datos biométricos, drones y otras tecnologías de vigilancia inteligente, etc.

En concreto, ya se está trabajando en dos estudios sobre big data. Uno se ocupa de este fenómeno con carácter general y centrado en las soluciones que se aplican en el entorno empresarial y comercial, ya que la Agencia es consciente de que la analítica de datos se está extendiendo a buen ritmo en áreas como la inteligencia de negocio, la gestión de la publicidad, el desarrollo de nuevas soluciones y productos ajustados a las necesidades de los clientes, la gestión de recursos humanos, la búsqueda de nuevos mercado, el control del fraude, etc.

Según todos los estudios y previsiones económicas, las nuevas tecnologías de análisis masivo de datos o big data tienen un gran potencial innovador y pueden ser un elemento esencial para potenciar el crecimiento económico y la creación de puestos de trabajo. Pero, por otro lado, por su propia naturaleza, los productos y servicios basados en big data tienen un tremendo potencial invasivo para la privacidad de las personas e, incluso, si no se toman las medidas adecuadas, pueden llevar aparejadas discriminaciones inaceptables.

En la realización de este estudio la Agencia colabora con ISMS Fórum, asociación empresarial sin ánimo de lucro cuyo objetivo principal es fomentar la seguridad de la información en España y que ha creado dentro de su estructura el Data Privacy Institute, que aglutina a personas y organizaciones españolas implicadas en el cumplimiento de la normativa sobre privacidad y la protección de datos de carácter personal.

Por otro lado, la Agencia está llevando a cabo un estudio sobre la reutilización de información clínica y análisis masivo de datos en el sector sanitario que pretende conocer la situación española en este campo en los ámbitos asistencial, de investigación, epidemiológico y de salud pública, tanto en el sector público como en el privado.

El objetivo del mismo es, a través de una caracterización de los proyectos de big data más relevantes que se estén desarrollando en estos momentos, identificar las líneas estratégicas y las tendencias principales en este campo, si bien partiendo de las iniciativas concretas que se están desarrollando en España.

Partiendo de los resultados del trabajo de campo, la AEPD realizará un análisis de sus implicaciones en la protección de datos personales con el fin de promover la adopción de buenas prácticas de protección de datos y realizar las recomendaciones oportunas para dotar de seguridad jurídica a estos tratamientos, ayudando tanto a las autoridades sanitarias como a los profesionales e investigadores sanitarios en la realización de estos proyectos.

Como ya se ha mencionado, este análisis y las recomendaciones se incardinan en la actuación preventiva y proactiva de la Agencia.

Por otro lado, también está ya en marcha la convocatoria de becas retribuidas dirigidas a postgraduados TIC en materias tales como matemáticas, física, ingeniería informática e ingeniería de telecomunicaciones, lo que redundará, en el futuro, en que existan profesionales TIC que conozcan estas materias y reconozcan la necesidad de que los desarrollos tecnológicos que realicen en su vida profesional respeten los derechos de los ciudadanos, además de promover la colaboración entre la Agencia y la Universidad.

Profundizando en esto último, está previsto poner en marcha a medio plazo un portal del desarrollador, en el que las personas que se dedican a construir y programar herramientas informáticas puedan encontrar, en un único lugar y en un lenguaje y un formato que les resulte accesible, todos los requisitos que deberían tener en cuenta para una correcta protección de los derechos de las personas que van a utilizar sus productos o cuyos datos van a ser tratados por los mismos, partiendo de la base de la integración de la protección de datos desde el diseño y por defecto en sus trabajos.

Del mismo modo, la Agencia prevé establecer contactos con grupos de investigación tecnológica que permitan una colaboración continuada de sus miembros, apoyando a la AEPD en las labores descritas en este apartado y, al mismo tiempo, poder tener un canal de comunicación para plantear a la Agencia las inquietudes que aparezcan en sus investigaciones en materia de protección de datos.

Otra línea que nos parece muy interesante es la realización de acciones y la creación de herramientas para que en los estudios universitarios de carácter técnico y científico pueda estar presente la protección de datos personales, de tal forma que los futuros científicos e ingenieros tengan al menos unos conocimientos básicos y esenciales sobre esta materia. De esta manera, serán conscientes de que han de tenerla en cuenta a lo largo de su vida profesional, tanto cuando desarrollen productos o servicios que entrañen el tratamiento de datos personales como cuando realizan labores de análisis de datos.

Otro aspecto importante que lleva a cabo la Unidad de Evaluación y Estudios Tecnológicos es la relación con empresas que desean presentar a la

Agencia proyectos tecnológicos innovadores para que sean evaluados por la Unidad y, de esta manera, hacerles llegar cuáles serían, en su caso, las garantías o procedimientos adicionales que se deberían implantar para cumplir con la legislación de protección de datos o, simplemente, para reducir los riesgos para la privacidad de los ciudadanos que podrían conllevar los mismos.

Finalmente, también hay que destacar que está previsto que esta Unidad sea la encargada de revisar y evaluar, tras la plena aplicabilidad de las disposiciones del Reglamento General de Protección de Datos, las evaluaciones de impacto en la protección de datos que muestren que el tratamiento al que se refieren entraña un alto riesgo si el responsable no adopta medidas para mitigarlo. La Unidad deberá, en un plazo de ocho semanas, detectar e indicar las medidas que deben adoptarse para que el tratamiento pueda llevarse a cabo para que sean comunicadas por la Agencia a los responsables del mismo.

COLABORACIÓN CON LOS RESPONSABLES Y PROFESIONALES DE LA PRIVACIDAD

La Agencia ha mantenido una política proactiva que facilite a los responsables del tratamiento de datos el cumplimiento de sus obligaciones. Con este fin se han editado guías generales y específicas sobre los criterios de aplicación de la LOPD y se han diseñado diversas herramientas para la inscripción de ficheros en el Registro General de Protección de datos o la implantación de medidas de seguridad, así como para que los sujetos obligados puedan autoevaluar de forma anónima su nivel de cumplimiento y las deficiencias detectadas respecto del mismo. A ello se añade la posibilidad de presentar consultas complejas que son resueltas por el Gabinete Jurídico de la Agencia. En el año 2015 se han mantenido reuniones con representantes de asociaciones empresariales, especialmente con las representativas de pymes y micropymes con el fin de contrastar la utilidad práctica de las guías y las herramientas de autoevaluación, constatando que su eficacia es susceptible de mejoras que incrementen su utilidad práctica.

Por otra parte, la evaluación del Servicio de Atención al Ciudadano a lo largo del tiempo permite concluir que se trata de un canal de información que no sólo es utilizado por los ciudadanos, sino también por los propios sujetos obligados y por los consultores que les asesoran. En 2015 este servicio atendió casi 220.000 consultas planteadas a través de diferentes canales (+10,6% respecto a 2014), de las que hay que destacar el aumento de las cuestiones planteadas a través de la Sede electrónica de la Agencia, con un incremento del 23,6% respecto al año anterior.

Partiendo de estas conclusiones, el Plan Estratégico ha incorporado la necesidad de establecer un canal específico para los responsables del tratamiento de datos que les permita obtener información y resolver las dudas sobre el cumplimiento de la LOPD, así como la de revisar las guías editadas de forma que ofrezcan una información más asequible para la solución de problemas concretos.

Por otra parte, la publicación del Reglamento General de Protección de Datos Personales el 25 de mayo de 2016, cuya aplicación efectiva se difiere dos años, establece un nuevo modelo de cumplimiento normativo en el que se acentúa la acreditación diligente de la responsabilidad de los sujetos obligados, planteando a la Agencia el reto de ofrecer criterios sobre el mismo.

El Reglamento, que se detalla posteriormente, parte de la necesidad de evaluar los niveles de riesgo que implicará el tratamiento de los datos personales en orden a que los responsables de su tratamiento adopten las medidas necesarias para garantizar los principios de protección de datos y permitir el ejercicio de los derechos que reconoce.

Entre estas medidas se incluyen nuevas obligaciones de información, la llevanza de un registro de los tratamientos y, en algunos casos, la realización de evaluaciones de impacto, la privacidad desde el diseño y por defecto y la designación de un delegado de protección de datos (DPD).

La creación de un canal especifico de atención a responsables, especialmente a pymes y micropymes, permitirá ofrecer información para facilitar el cumplimiento del Reglamento a lo largo del periodo transitorio para su aplicación efectiva.

La figura del DPD, en los casos en que sea exigible, ejercerá un papel destacado para garantizar la protección de datos por parte de los responsables y encargados del tratamiento, facilitará el ejercicio de los derechos a los interesados y será un cauce fluido de contacto con ellos y con la AEPD. Por ello el Plan Estratégico prevé promover la figura del DPD, elaborar una guía que incorpore las características específicas de esta figura y habilitará un canal específico para atender las cuestiones que planteen los delegados de protección de datos.

Asimismo la Agencia promoverá las evaluaciones de impacto en protección de datos, facilitando metodologías para realizarlas a partir de la guía que ya se encuentra disponible en la web de la Agencia, y orientaciones sobre la privacidad desde el diseño y por defecto.

Estas orientaciones deben dirigirse específicamente a los profesionales TIC encargados de diseñar y mantener los sistemas de información y de desarrollar nuevos productos y servicios que impliquen el tratamiento de datos personales.

Por otro lado, pero unido de forma intrínseca al apartado anterior, los profesionales de la privacidad desempeñan un relevante papel en la aplicación de la normativa de protección de datos mediante la labor de asesoramiento que prestan a responsables y encargados del tratamiento, ya que su experiencia en la materia constituye una fuente fundamental para conocer las inquietudes y dificultades que suscita la aplicación de la legislación.

En consecuencia, el Plan Estratégico destaca la necesidad de mantener políticas de colaboración fluida y ágil con las asociaciones de profesionales de la privacidad para conocer los problemas que se plantean y sus sugerencias sobre cómo resolverlos y transmitir los criterios y líneas de actuación de la Agencia. Ello redundará, sin duda, en la calidad de su asistencia profesional y, por tanto, en un mejor cumplimiento de la normativa y de las garantías de los ciudadanos.

La Agencia ha venido manteniendo reuniones con asociaciones de profesionales de la privacidad y ha iniciado una relación directa con ellas para conocer sus dudas y sugerencias en relación con el Reglamento recientemente publicado, una relación sobre la que vamos a seguir trabajando para profundizar en las líneas de colaboración.

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS COMO NUEVO MARCO

El 25 de mayo de 2016 ha entrado en vigor el nuevo Reglamento General de Protección de Datos de la Unión Europea, que sustituirá a la Directiva del año 95. El Reglamento pretende ser el instrumento con el que la Unión responde a los retos que plantean el uso generalizado de las modernas tecnologías de la información y la comunicación y la globalización.

El contenido del Reglamento puede considerarse, en sus planteamientos centrales, una evolución de la Directiva del 95, de la que recoge, reforzándolos, los principios básicos de la protección de datos y los derechos de los interesados. Sin embargo, desde el punto de vista de los procedimientos y mecanismos de protección, el Reglamento contiene importantes novedades.

La más evidente de ellas es su naturaleza dentro del marco de los actos jurídicos europeos. El Reglamento es una norma que se aplica directamente en los Estados Miembros. Estos pueden adoptar normas que faciliten o posibiliten su eficacia y directa aplicabilidad, y pueden también aprobar normas de desarrollo en los casos en que el Reglamento les habilite para ello. Pero no son precisas normas de trasposición. Desde el punto de vista de los ciudadanos, esta norma, que uniformiza el derecho europeo de protección de datos, supone la garantía de un nivel similar de protección en toda la Unión.

El control que los ciudadanos tienen de sus datos personales se refuerza desde varios frentes. Por una parte, se clarifica la noción de consentimiento, que deberá prestarse de forma inequívoca mediante declaraciones o acciones afirmativas claras. Por otra, se incorporan nuevos derechos, como el derecho a la portabilidad o el derecho a la limitación de los tratamientos. El Reglamento menciona también el "derecho al olvido". Sin embargo, ha renunciado a configurarlo como un derecho autónomo, siguiendo la línea marcada por el Tribunal de Justicia de la Unión Europea en la Sentencia sobre el caso Google Spain, donde señaló que este derecho no es sino una adaptación a la actividad de los motores de búsqueda de derechos clásicos como son el de cancelación y el de oposición.

El Reglamento también incluye una novedad en el caso del derecho de oposición, disponiendo que corresponderá al responsable demostrar que sus intereses prevalecen sobre los derechos, libertades e intereses del interesado en relación con sus circunstancias específicas.

Uno de los capítulos del Reglamento que introduce las principales novedades que, además, más directamente podrán afectar a la protección de que disfruten los interesados, es el dedicado a las obligaciones de los responsables y también de los encargados, ya que tiene en cuenta la influencia que actualmente ejercen éstos a la hora de determinar las condiciones de un tratamiento de datos.

En la Directiva se establecen una serie de objetivos de cumplimiento, pero se dice muy poco sobre el modo de alcanzarlos. Apenas hay algunas referencias a las obligaciones de notificación de ficheros y autorización previa de determinados tratamientos, a los delegados de protección de datos y a las medidas de seguridad.

El Reglamento, por su parte, apuesta por un enfoque preventivo, estableciendo la obligación para responsables y encargados de implantar medidas que les coloquen en posición de poder cumplir con las previsiones del Reglamento, y también la obligación de estar en condiciones de demostrar que han aplicado esas medidas.

Entre estas medidas se cuentan las de protección de datos desde el diseño y por defecto, el mantenimiento de un registro de tratamientos, la necesidad de aplicar medidas de seguridad adecuadas al riesgo derivado de los tratamientos, la realización de evaluaciones de impacto sobre la protección de datos de los tratamientos que a priori parezcan entrañar un alto riesgo para los derechos y libertades de los interesados y la también obligatoria implantación de un delegado de protección de datos en las organizaciones públicas y en las privadas que lleven a cabo determinados tratamientos.

Mención aparte merece el papel destacado que el Reglamento reserva a los códigos de conducta y a los esquemas de certificación. Ambos son instrumentos de co-regulación que reflejan plenamente el nuevo enfoque que el Reglamento propugna, ya que en los dos casos, aunque por diferentes vías, las organizaciones que se adhieren a ellos asumen un compromiso de cumplimiento y aceptan someterse a una supervisión reforzada de ese compromiso.

En el terreno de las transferencias internacionales el Reglamento mantiene el modelo seguido por la Directiva, aunque con algunos ajustes orientados a flexibilizarlo. Como principio general se establece que los datos no podrán ser exportados desde la Unión Europea a países que no ofrezcan un nivel equivalente ("adecuado") de protección. La constatación de ese nivel la seguirá realizando la Comisión, si bien el Reglamento contiene un listado de aspectos a valorar más largo, detallado y exigente que el recogido por la Directiva.

En los casos en que el país de destino no ofrezca ese nivel de protección, seguirá siendo posible transferir los datos siempre que el exportador, ya sea responsable o encargado, ofrezca garantías suficientes. También se amplía el catálogo de instrumentos para ofrecer esas garantías, dándose carta de naturaleza legal a las Normas Corporativas Vinculantes (BCR, en sus siglas inglesas) e incluyéndose por primera vez los códigos de conducta y los esquemas de certificación.

También podrán transferirse datos a países sin nivel adecuado de protección cuando concurra alguna de las causas de excepción que el Reglamento, en la misma línea que la Directiva, prevé. El Reglamento añade una nueva excepción, que sólo puede operar cuando no sea posible ofrecer garantías suficientes o invocar alguna de las otras excepciones, permitiendo la transferencia sobre la base del interés legítimo del responsable siempre que se trate de transferencias que no sean repetitivas y que afecten a un número limitado de titulares de datos.

El segundo gran grupo de disposiciones del Reglamento que marcan una clara diferencia con la Directiva es el que organiza el sistema de supervisión.

En primer lugar, el Reglamento confirma un modelo de supervisión basado en la intervención de autoridades administrativas especializadas e independientes. Para ello regula con detalle las condiciones para su establecimiento y funcionamiento, con especial hincapié en todos los elementos que contribuyen a garantizar su independencia y efectividad, sus funciones y sus poderes. Entre estos últimos se incluye específicamente la potestad para imponer sanciones económicas, algo no expresamente previsto en la Directiva del 95.

Al mismo tiempo, el Reglamento opta por un sistema de supervisión que podría calificarse como cooperativo. Teniendo en cuenta que se trata de una norma llamada a aplicarse en toda la Unión, que busca obtener niveles similares de protección para todos los ciudadanos y que se dirige, cada vez con más frecuencia, a responsables y encargados que operan en varios países, es lógico que las autoridades de supervisión hayan de coordinar su actividad y cooperar para evitar duplicaciones innecesarias, emitir decisiones consistentes y aumentar su eficacia.

El Reglamento establece expresamente una obligación de cooperación mutua, sometida a plazos y procedimientos específicos, que incluye la realización de acciones conjuntas llevadas a cabo por personal de las distintas autoridades afectadas por un determinado tratamiento.

Esa cooperación se extiende a los procesos de toma de decisiones. En los casos de tratamientos transnacionales, en que una empresa tiene establecimientos en varios Estados Miembros o realiza tratamientos que afectan significativamente a ciudadanos en varios Estados Miembros, la adopción de la decisión corresponde a la autoridad del Estado en que la empresa tenga su establecimiento principal o único en la Unión. Pero esa decisión debe adoptarla atendiendo a las propuestas de las demás autoridades afectadas (porque haya establecimientos o ciudadanos afectados en su territorio). Si alguna de estas autoridades discrepa de la propuesta de la autoridad principal, puede remitir el conflicto al Comité Europeo de Protección de Datos, que lo resolverá mediante una decisión vinculante para las autoridades implicadas.

Hay que subrayar que en todos estos casos, los interesados siguen manteniendo la posibilidad de dirigirse siempre a una única autoridad de supervisión, que en la mayoría de los casos será la del país en el que residan. Es ésta la que se ocupa de

todos los contactos con otras autoridades y de informar al interesado de la marcha y el resultado de sus posibles reclamaciones.

El citado Comité Europeo es el sucesor del actual Grupo del Artículo 29, pero con diferencias sustanciales. La primera, ya mencionada, es que puede adoptar determinadas decisiones vinculantes, para lo cual se le ha dotado de personalidad jurídica propia. Además, el Comité gestiona el llamado mecanismo de coherencia, en virtud del cual emitirá dictámenes no vinculantes (pero que de no aceptarse pueden ir seguidos de una decisión vinculante) sobre proyectos de decisiones de las autoridades, distintos de los tratados en el sistema de cooperación, que puedan tener efectos en la libre circulación de datos en la Unión. Aparte de ello, el Comité, de composición también paralela a la del GT29, hereda sus funciones consultivas y de emisión de recomendaciones, dictámenes o buenas prácticas.

El modelo de supervisión se completa con un régimen de sanciones. El Reglamento no tipifica con demasiado detalle las infracciones, limitándose a enumerar incumplimientos de varios de sus artículos, ni tampoco es demasiado preciso respecto a las cuantías de las sanciones. En este punto establece dos niveles, el primero con un máximo de 10 millones de euros o el 2 por ciento del volumen de negocio anual global, aplicándose el que resulte más elevado de los dos en el caso de compañías y, en los mismos términos, 20 millones de euros o el 4 por ciento del volumen de negocio anual global.

El efecto coordinado de estas medidas de refuerzo del control de sus datos para los ciudadanos, de prevención en las organizaciones y de mayor desarrollo del sistema de supervisión debe repercutir en una mejor protección de los derechos de los interesados.

Al mismo tiempo, cambiará de forma sustancial el modo en que las autoridades de supervisión desarrollan su actividad. Muchas de sus decisiones ya no podrán adoptarlas en solitario, sino que deberán consultarlas y negociarlas con otras autoridades implicadas. De igual forma, podrán beneficiarse de las actuaciones de inspección o control llevadas a cabo por otras autoridades. En último extremo, las autoridades deberán también ajustar su actividad al enfoque del Reglamento, intensificando sus actividades de sensibilización, apoyo a interesados, responsables y encargados y control preventivo.

El nuevo Reglamento ha sido llamado a profundizar en el sistema que diseñó la Directiva europea de Protección de Datos hace más de 20 años y que logró sentar las bases de un modelo de garantías avanzado y protector para sus ciudadanos. En paralelo, las Autoridades de Protección de Datos tenemos la obligación de dar respuesta a los retos de futuro escuchando a todos los implicados, llegando a soluciones sostenibles que permitan compatibilizar la innovación tecnológica con el cumplimiento de la normativa, ya que solo así se podrá garantizar de una forma efectiva el derecho fundamental a la protección de datos de los ciudadanos.

DIFUSIÓN NO AUTORIZADA DE IMÁGENES ÍNTIMAS

(Revenge Porn)

PABLO A.
PALAZZI

Es Abogado y LLM Fordham Law School. Socio del estudio Allende & Brea (Buenos Aires, Argentina). Profesor de Derecho Universidad de San Andrés, director del Programa de Derecho de Internet y Tecnología de las Comunicaciones (DITC) de la Universidad de San Andrés y del Centro de Tecnología y Sociedad de la Universidad de San Andrés (Buenos Aires, Argentina). Autor de varios libros y artículos en la materia.
Comentarios son bienvenidos a ppalazzi@udesa.edu.ar

SUMARIO

RESUMEN

En este artículo el autor analiza los desafíos para la protección de datos de las imágenes publicadas en internet, buscadores y redes sociales, las que aún no han encontrado su régimen jurídico.

Se destaca que en materia criminal no existen figuras penales que traten directamente a la imagen específicamente como bien jurídico, aunque sí ha sido categorizada como dato personal bajo los delitos previstos en las leyes de protección de datos personales.

Se define y delimita el alcance del concepto de "revenge porn" señalando que en general consiste en la publicación no autorizada de imágenes o videos privados, generalmente conteniendo imágenes íntimas, que una persona (generalmente la ex pareja por sí o a través de terceros) publica por venganza luego de terminar la relación. Realiza además un racconto de los distintos regímenes que han tratado el tema en el derecho comparado, para culminar con el análisis detallado de la normativa y jurisprudencia argentina en la materia.

Destaca los fundamentos para penalizar la difusión no autorizada de videos o imágenes íntimas, incluyendo entre éstos el derecho a la intimidad, la normativa de violencia de género contenida en la Convención de Belem do Pará, la libertad de expresión y la falta de interés público.

Finalmente, realiza una propuesta para amparar la imagen en la legislación penal argentina.

1. INTRODUCCIÓN

1.1. LA IMAGEN Y SU DIFUSIÓN EN INTERNET

Desde hace unos años la fotografía y el video se han instalado en Internet y en las redes sociales. El amplio uso de blogs, mensajería instantánea y redes sociales, la práctica de sacarse "selfies" y de subirlas online en cuestión con un sólo click de un teléfono móvil se ha expandido a límites inimaginables. Cada imagen subida puede ser "tagueada" en redes sociales, o se puede encontrar con un buscador de imágenes en segundos. Los buscadores y las redes sociales indexan estos contenidos y forman bibliotecas casi infinitas de datos personales online accesibles en forma gratuita. La emergente Sociedad de la Información tiene muchos elementos característicos, pero sin duda uno de ellos es la imagen y el video.

Muchas de estas fotos y videos no están destinados a ser difundidos pero finalmente terminan en Internet en contra de la voluntad del titular de la imagen. La regulación legal de la imagen es compleja puesto que el derecho a la imagen, como derecho personalísimo está definido como un derecho subjetivo sobre el cual el titular tiene ciertas prerrogativas, con contadísimas excepciones (las permitidas en la ley). Pero la tecnología permite múltiples usos de la imagen y del video cuyo único límite es que "se puede hacer".

En materia criminal en nuestro medio no hay figuras penales que traten directamente a la imagen específicamente como bien jurídico. Sin embargo cabe su categorización como dato personal bajo los delitos previstos en las leyes de protección de datos personales.

Por otra parte, la protección penal de la privacidad no es ni debe ser absoluta. Todo este mundo de la imagen requiere cautela al legislar que usos de la imagen serán delitos. Como sucede con numerosas acciones disvaliosas, solo ciertas conductas son delito y el resto de las acciones queda dentro del marco de libertad permitido que el Estado no puede sancionar criminalmente, sin perjuicio de la libertad de accionar civilmente que le queda a la víctima. En materia civil, por el contrario las cautelares se obtienen incluso contra buscadores[1].

Las imágenes publicadas en Internet, en buscadores y en redes sociales aún tienen que encontrar su régimen jurídico. La jurisprudencia ya sostuvo que un buscador de imágenes no es responsable de los contenidos indexados ni violenta el derecho a la imagen al reproducir una versión reducida de la misma, pese a que no existía una excepción expresa en la ley[2]. También que una persona que se ve envuelta en temas de interés público no puede impedir que se difundan imágenes de su persona con fines informativos previamente publica-

1 *Ver por ejemplo el caso "T. M. E. c/ Google Inc. s/ medida autosatisfactiva", del Juzgado de Primera Instancia de Familia de Rawson, de fecha 26 de noviembre de 2013 (MJ-JU-M-82809-AR | MJJ82809 - MJJ82809). Se ordena cautelarmente a la empresa demandada el inmediato y urgente bloqueo en su buscador de internet, en virtud de los diferentes enlaces que aparecen en el mismo vinculando a la actora con fotografías íntimas, datos personales, así como comentarios injuriantes sobre su persona e intimidad que fueron subidos por una ex pareja sin su consentimiento.*

2 *CSJN, "María Belen Rodriguez v. Google y otro", publicado en Revista Latinoamericana de Protección de Datos, Año I, No.1, págs. 352/384 (2015) y nuestro comentario El fallo de la Corte Suprema de Argentina en el caso Google, la creación pretoriana de un procedimiento de "notice & take down" y su impacto en la protección de datos personales, en pág. 385 de la misma publicación.*

das en redes sociales[3]. Finalmente se sostuvo en varios casos que la imagen libremente disponible en Internet o redes sociales es pública a los fines de reconocimiento judicial del autor de un hecho delictivo[4].

Además de la imagen voluntariamente subida a Internet, aparece el problema de las imágenes publicadas sin permiso. A comienzos del 2014 tomó estado público en la Argentina que un hacker logró infiltrarse en varios sistemas informáticos de famosos y difundió sus fotos íntimas por redes sociales[5]. El hacker habría tomado el control de la videocámara que tiene el ordenador y luego de activarla sin conocimiento del legítimo usuario captó imágenes íntimas.

Asimismo, desde hace un tiempo suelen aparecer en diversos sitios de Internet fotos o videos de escenas íntimas de famosos (y a veces no tan famosos). Estas imágenes son difundidas en medios periodísticos y sobre todo en el mundo online sin ningún límite. A veces estas imágenes se originan en una sesión fotográfica realizada en el pasado, sin destino a publicidad como ocurrió en un caso reciente con la novia del entonces vice presidente de la Nación[6]. Otras, son habidas en forma ilegal de algún ordenador o servidor en la nube[7] o se trata del típico caso del novio o novia que desea vengarse de su ex pareja (fenómeno conocido como *revenge porn*).

¿Qué amparo penal tiene la imagen captada *ab-initio* con autorización de la víctima pero luego difundida sin su consentimiento? Seguidamente analizamos la protección penal de este aspecto de la intimidad, las respuestas del derecho comparado y una propuesta para Argentina.

La ocurrencia de estos hechos es y será cada vez más frecuente. La Informática ha permitido a cualquiera acceder a poderosas herramientas para captar la imagen, grabar videos y difundirlos en Internet. La viralización de contenidos, un concepto inicialmente usado en marketing digital, y el morbo inagotable de los usuarios de Internet ayuda a difundir sin límites este tipo de imágenes. La consecuencia de ello es que una imagen íntima que estaba destinada a ser mantenida en la vida privada en brevísimo tiempo puede llegar a millones de personas.

1.2. CONCEPTO

El término "*revenge porn*" fue usado por primera vez en los Estados Unidos[8].

Consiste en la publicación no autorizada de imágenes o videos privados, generalmente conteniendo imágenes íntimas, que una persona (generalmente la ex pareja por sí o a través terceros) publica por venganza luego de terminar la relación. De allí el término *revenge porn*.

El término no es el más preciso para definir la cuestión pero es el más difundido. La palabra inglesa porn que se traduce como porno o pornografía, está asociado a lo obsceno, pero las imágenes íntimas o privadas no necesariamente deben ser calificadas como obscenas. La palabra revenge se traduce como venganza. Siguiendo estas ideas en España se lo ha denominado "porno por despecho".

El término *revenge porn* se popularizó en los Estados Unidos con un sitio web conocido bajo el nombre "Is Anyone Up?". Se trataba de un sitio de Internet dedicado a difundir sin permiso de las víctimas, imágenes de escenas íntimas de éstas. Como el contenido era subido por terceros, el sitio se amparaba en la inmunidad prevista en la sección *230 de la Communications Decency Act*.

También se ha propuesto usar el nombre de *involuntary porn* o *non consensual pornography*[9]. Al eliminar el término "revenge" del concepto, se logra ampliar la figura. Es que no se incluye sólo a aquellas situaciones donde el sujeto activo actúa por venganza o donde las partes tenían una relación previa sino que se lo expande a terceros no relacionados con el hecho en sí de la captación original de la imagen. Estas publicaciones o republicaciones por terceros tienen el mismo efecto que la publicación original.

---

3 *CNCiv, Sala H, 2/9/2015, D.P.Y.D c/Google, MJ-JU-M-95456-AR ("El interrogante que debe plantearse es hasta donde pueden considerarse íntimas las fotos que existen en una red social como la nombrada, donde justamente se trata de compartir eventos y fotos por una red masiva de comunicación y que casualmente se la define como una red social. El funcionamiento de Facebook es similar al de cualquier otra red social, aunque esta oración deberíamos formularla al revés, ya que es esta la red social que marca los antecedentes y las condiciones que deben cumplir las demás").*

4 *CNCrim., Sala VI, 2/6/2015 A., F. s/ Nulidad, (rechazo de planteo de nulidad por reconocimiento de imputado en foto en red social). Ver también RIQUERT, Las redes sociales como nuevo medio orientador de pesquisas criminales, LL 2015-E -432, con cita de numerosos fallos sobre la materia.*

5 *Cfr. la nota La modelo Noelia Marzol denunció a Camus Hacker ante la Justicia, La Nación, 28/1/2014.*

6 *Cfr. Los tatuajes confirman que es Agustina Kampfer, Clarín, 15/8/2014.*

7 *Andrea PETERSON, Emily YAHR y Joby WARRICK, Leaks of nude celebrity photos raise concerns about security of the cloud, Washington Post, 1/9/2014.*

8 *Ver http://en.wikipedia.org/wiki/Revenge_porn.*

9 *FRANKS, How to Defeat 'Revenge Porn': First, Recognize It's About Privacy, Not Revenge, 22/6/2015.*

2. EL "REVENGE PORN" EN EL DERECHO COMPARADO

2.1. ESTADOS UNIDOS

2.1. 1. Surgimiento del problema

Desde un comienzo, el problema para regular la circulación de este tipo de imágenes online en Estados Unidos fue doble: una fuerte libertad de expresión y una normativa fuertemente establecida –aunque cuestionada en esta clase de supuestos- respecto a la inmunidad de los intermediarios de Internet[10].

Es decir que, por una parte, el discurso auténtico y verdadero tiene una fuerte protección constitucional a través de la Primera Enmienda de la Constitución de los Estados Unidos y una foto verdadera de una persona captada libremente cabe dentro de ese concepto. Por otra parte, cualquier sitio de Internet que permite publicar contenido subido por terceros, tiene protección e inmunidad civil bajo una ley conocida como *Communications Decency Act*[11].

2.1. 2. Primeros casos judiciales

Numerosos casos de *revenge porn* han ocurrido en los Estados Unidos en los últimos años. En general estos casos pueden ser supuestos de subida online de imágenes o videos de escenas íntimas, pero muchos de ellos también van acompañados de insultos, amenazas, coacciones o casos de hostigamiento a largo plazo a la víctima.

Quienes han estudiado el tema en profundidad, han comprobado que las normas jurídicas y las fuerzas de seguridad no están preparadas para dar una respuesta rápida y efectiva a esta clase de ataques[12].

Sin perjuicio de ello, muchos de estos casos terminaron con penas de prisión a los culpables por aplicación de diversas normas penales. Varios casos fueron tapa de diarios o comentados ampliamente en Internet, impulsando así un debate sobre la seguridad en la nube y la necesidad de legislar en forma más adecuada el uso no autorizado de imágenes íntimas. Así ocurrió con el caso de las conocidas actrices Jennifer Lawrence[13], Kate Uptown o Kirsten Dunst[14]. Incluso en estos casos se precisó que las imágenes tenían metadatos[15] que indicaban la ubicación geográfica de donde habían sido tomadas[16].

Asimismo, todas estas publicaciones de imágenes íntimas y las lagunas legales existentes han llevado a replantear la inmunidad otorgada en forma general a los intermediarios de Internet con el fin de fomentar el desarrollo de la Red, sobre todo a aquellos sitios que se dedican a publicar este tipo de imágenes y abusan de las protecciones dadas a intermediarios neutros.

El caso más notorio ocurrió en el año 2014 con el operador del sitio de internet *Is anyoneup?* que permitía a cualquier usuario de Internet publicar fotos de escenas íntimas con fines de humillar a las mujeres participantes en las mismas. El dueño del sitio, Hunter Moore, fue arrestado por haberle pagado a un hacker para que obtuviera ciertas fotos de una cuenta de correo electrónico. Fue sometido a un proceso penal[17] y finalmente recibió la condena de dos años y seis meses de prisión[18]. Pero Moore solo fue condenado por ayudar al acceso ilegítimo. El sitio que creó y las miles de imágenes de víctimas que publicó no eran delito penal entonces en la mayoría de los Estados Unidos. A raíz de este caso, y de muchos otros que le siguieron, se inició una tendencia para llegar este vacío legal.

Otro caso notorio es el del hacker de *celebrities*, Christopher Chaney, quien accedió sin permiso a

10 *Paul LARKIN, 'Revenge Porn,' State Law, and Free Speech, Loyola of Los Angeles Law Review, Vol. 48, 2014.*

11 *Sobre el tema remitimos a los diversos artículos publicados en la obra colectiva bajo mi dirección Responsabilidad Civil de los intermediarios en Internet (Pablo Palazzi, director), Abeledo Perrot, 2012.*

12 *CITRON, Hate Crimes in cyberspace, Harvard, 2014, p. 35 a 119.*

13 *En su caso, este escándalo llevó a que el sitio Reddit cambiara su política de privacidad y prohibiera imágenes de desnudos. Ver Mike ISAAC, In Privacy Update, Reddit Tightens Restrictions on Nude Photos, New York Times, 24 de Febrero de 2015.*

14 *MCCOY, 4chan: The 'shock post' site that hosted the private Jennifer Lawrence photos, Washington Post, 2/9/2014; Andrea PETERSON, Emily YAHR y Joby WARRICK, Leaks of nude celebrity photos raise concerns about security of the cloud, Washington Post, 1/9/2014.*

15 *Por esta razón las redes sociales como Facebook eliminan los metadatos de las fotos que publican, a menos que el usuario opte positivamente por dar a conocer su ubicación.*

16 *Kashmir HILL, Leaked Nude Images Reveal Celebs' Location Information, Forbes, 9/2/2014, www.forbes.com/sites/kashmirhill/2014/09/02/leaked-nude-images-reveal-celebs-location-information .*

17 *Rusell BRANDOM, Revenge porn magnate Hunter Moore will face up to seven years in prison, The Verge 18/2/2015.*

18 *Abby OHLEISER, Revenge porn purveyor Hunter Moore is sentenced to prison, The Washington Post, 12/3/3015.*

numerosos ordenadores, incluyendo los archivos de varias actrices (Simone Harouche, Mila Kunis, Christina Aguilera, Scarlett Johansson, Renee Olstead). El hacker fue arrestado luego de un año de investigación en la Operation Hackerazzi[19]. En el caso se logró probar que luego de acceder a los ordenadores, el autor creaba una regla interna de desvío del correo y obtenía copias de toda la correspondencia digital en busca de fotos o correos íntimos, que luego usaba para extorsionar a sus víctimas. Esto le permitía leer el correo incluso, luego de que se cambiara la *password* de la víctima y seguir "sustrayendo" imágenes.

El autor fue juzgado[20] por 26 hechos diferentes, todos relacionados con acceso ilegítimo a sistemas informáticos sin autorización, daño a sistemas informáticos, interceptación de comunicaciones (*wiretapping*, por el acceso y desvío de correos) y robo de identidad agravado. Chaney fue sentenciado a la pena de 10 años de prisión[21].

Algo similar ocurrió con el caso de *Miss Teen USA*. Un hacker de 19 años, Jared James Abrahams, fue sometido a un proceso penal y se declaró culpable de (i) ingresar ilegalmente en el ordenador de la modelo (y de otra veintena de personas), (ii) copiar y captar fotos sin permiso y, (iii) amenazarlas con publicar esas fotos online en redes sociales si no le enviaban más fotos de desnudos[22].

En septiembre de 2014 un ataque de ingeniería social al sitio *icloud* de Apple permitió a un hacker obtener numerosas fotos de famosas[23], que fueron publicadas en varios sitios de la web[24]. Las fotos fueron publicadas durante un corto periodo de tiempo en sitios como 4chan y Reddit antes de que fueran retiradas, El autor del hecho avisó del acceso a imágenes y vídeos de decenas de famosos y habría pedido un "rescate" en bitcoins -la moneda virtual— para no publicarlas.

Estos casos demuestran la existencia de hechos típicos que se repiten cada vez más y consisten en difundir online fotografías de escenas intimas, o amenazar a sus titulares o extorsionarlos con difundirlas a cambio de algún beneficio económico o de otra clase.

2.1. 3. Normativa estadual estadounidense

En Estados Unidos comenzaron a presentarse en varias legislaturas estaduales proyectos de leyes para penalizar este tipo de prácticas. Estos proyectos están impulsados por la constante ocurrencia de casos, y la preocupación y demanda social que generó el vacío legislativo, sumado a las noticias en la prensa de la falta de cobertura legal de este fenómeno[25].

Recordamos que en Estados Unidos cada estado tiene competencia exclusiva en materia penal y pueden aprobar sus propias normas criminales. Los estados suelen ser los laboratorios legales donde se experimenta para el establecimiento posterior de una legislación federal. En agosto de 2013, cerca de 14 estados habían aprobado o estaban discutiendo normas especiales sobre este asunto[26]. En el año 2014 eran 17 y a fines del año 2015 había 26 estados con legislaciones especiales[27]. También en el año 2015 se comenzó a debatir sobre una posible legislación a nivel federal[28].

La mayoría de las leyes aprobadas cubren tanto la captación como la posterior difusión no autorizada de fotos de escenas íntimas. Pero cada norma local tiene variantes y es imposible analizarlas a todas.

En California está prevista en el *California Penal Code*[29] con seis meses de prisión y varios miles de dólares de multa. La norma regula otras situaciones vecinas como espiar a una persona en un cambiador en una loca, o con cámaras ocultas

El delito previsto en la ley de California consiste en distribuir con intención imágenes íntimas en circunstancias en la cual la persona debió enten-

19 *Ver Boletín del FBI, http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft*

20 *El juicio oral incluyó un video-testimonio de Scarlett Johansson donde –en medio de lágrimas- la actriz contaba como había sido humillada por la difusión en Internet de sus fotos íntimas, que estaban destinadas solamente a quien entonces era su marido.*

21 *Christopher Chaney sentenced to 10 years in jail for hacking into personal online accounts of celebs Scarlett Johansson, Mila Kunis, Christina Aguilera, http://www.nydailynews.com/entertainment/gossip/hollywood-hacker-10-years-jail-article-1.1222151*

22 *RISLING, Miss Teen USA sextortion case: Hacker pleads guilty, Associated Press, Noviembre 13 de 2013.*

23 *Entre las afectadas vuelven a estar Jennifer Lawrence y Kaley Cuoco (The Big Bang Theory), Kim Kardashian, Vanessa Hudgens, Rihanna, Mary-Kate Olsen, Avril Lavigne o la futbolista estadounidense Hope Solo.*

24 *Fotografías de famosas desnudas: El hacker vuelve a filtrar fotografías íntimas, Hufftington Post, 21 de septiembre de 2014.*

25 *Una editorial del diario New York Times dijo sobre el tema: "Revenge porn is one of those things that sounds as if it must be illegal but actually isn't. It's the term of art for publishing sexual photos of someone without his or her -- usually her -- permission, often after a breakup". Cfr. Editorial del diario New York Times del día 13 de octubre de 2013.*

26 *http://www.cagoldberglaw.com/states-with-revenge-porn-laws/*

27 *http://www.endrevengeporn.org/revenge-porn-laws/*

28 *O'HARA, A federal revenge-porn bill is expected next month, The Daily Dot, 21/6/2015.*

29 *California Penal Code, sección 647(j)(4).*

der que la imagen quedaría reservada y siempre que el sujeto activo sepa que la distribución causará un serio perjuicio y efectivamente la persona sufre ese perjuicio emocional. La norma tiene excepciones para fines informativos de la prensa ("distribution is made in the course of reporting an unlawful activity") o cuando tiene lugar en un proceso judicial.

El problema en California es que la ley de *revenge porn* sancionada no contemplaba las selfies, por la creencia de que quien se saca una autofoto o *selfie*, estaría consintiendo su difusión posterior por el riesgo de que la imagen caiga en manos de terceros. Esto es criticado por autores[30] que consideran que muchos de estos supuestos (como el caso de las *selfies*) deben también quedar incluidos en el concepto de *revenge porn* cuando son difundidos contra la voluntad de la persona retratada.

2.2. BRASIL

En el año 2014 Brasil aprobó la ley del Marco Civil de Internet[31]. La norma fue aprobada como reacción por parte de Brasil a las revelaciones hechas por Edward Snowden.

Esta norma otorga inmunidad a los intermediarios de Internet por el contenido generado por terceros y establece un sistema de *notice & take down* de contenido ilegal (arts. 18, 19 y 20, *Ley de Marco Civil de Internet*).

La sección III de la ley brasilera se titula "De la Responsabilidad por Daños que Surgieran del Contenido Generado por Terceros". El art. 18 de la ley del marco civil dispone que el proveedor de conexión a internet no será responsabilizado civilmente por daños surgidos por contenido generado por terceros.

Con el objetivo de asegurar la libertad de expresión e impedir la censura, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica, no toma las previsiones para, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, hace disponible el contenido especificado como infringiente, exceptuando las disposiciones legales que se opongan (art. 19).

Finalmente el art. 21 dispone que el proveedor de aplicaciones de internet que disponibilice contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, *de imágenes, videos u otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando*, posterior al recibimiento de la notificación por el participante o su representante legal, dejar de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la indisponibilización de ese contenido.

En síntesis, el art. 21 de esta ley dispone que serán responsables si no remueve contenido relacionado con lo que podría calificarse como casos típicos de "revenge porn".

Ese es el único caso de remoción obligatoria de contenidos sin la necesidad de autorización judicial bajo la ley brasilera[32]. Es una regla muy estricta que se incluyó para forzar a intermediarios a remover imágenes íntimas no consentidas de "revenge porn"[33].

El origen de esta norma no fue el video no autorizado de la modelo Ciccarelli y su cautelar contra Youtube[34], como se suele indicar erróneamente, sino el hecho que dos menores de edad (de 16 y 17 años) se suicidaran en Brasil después que sus fotos íntimas fueran ampliamente divulgadas en la red[35].

30 *Cfr. la exposición de Holly Jacobs, Revenge Pornography. Legal and Policy issues, en CPDP 2015, Bruselas, 22/1/2015.*

31 *Ver Ley de Marco Civil de Internet, ley 12.963 del 23 de abril de 2014, publicada en Revista Latinoamericana de Protección de Datos, Año I, No.1, págs. 187/202 (2015).*

32 *Para un desarrollo de esta ley y sus aspectos sobre privacidad ver D.DONEDA y M. MONTEIRO, O sistema brasilerio de privacidade e protecao de dados no Marco Civil da Internet, en Revista Latinoamericana de Protección de Datos, Año I, No.1, págs. 23/49 (2015).*

33 *Ley de Marco Civil de Internet, art. 21. El proveedor de aplicaciones de internet que disponibilice contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, de imágenes, videos u otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando, posterior al recibimiento de la notificación por el participante o su representante legal, dejare de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la indisponibilización de ese contenido. Parágrafo único. La notificación prevista en el artículo deberá contener, bajo pena de nulidad, elementos que permitan la identificación específica del material apuntado como violador de la intimidad del participante y la verificación de la legitimidad para presentación del pedido. Ver Revista Latinoamericana de Protección de Datos, Año I, No.1, págs. 187/202 (2015).*

34 *Brazil model wins YouTube battle , BBC News, January 5, 2007.*

35 *IRAHETA, Pornografia da vingança: Marco Civil da Internet facilita punição e obriga sites a tirar vídeos íntimos do ar, http://www.brasilpost.com.br/2014/03/28/pornografia-da-vinganca-marco-civil_n_5052468.html y la nota sin autor, Víctima de las redes sociales: una estudiante se suicida tras aparecer en un vídeo porno, http://www.elconfidencial.com/tecnologia/2014-05-24/victima-de-las-redes-sociales-una-estudiante-se-suicida-tras-aparecer-en-un-video-porno_135717/#lpu6oTNOXNnQcZAJ*

Es ilustrativo que Brasil no incluye en el Código Penal el delito de revenge porn, sino que regula solo una forma rápida de remover el contenido de la red invirtiendo la regla de inmunidad de los intermediarios de Internet.

2.3. ESPAÑA

2.3. 1. Jurisprudencia anterior a la reforma del año 2015

Entre los años 2011 y 2015 se produjeron innumerables casos de difusión o publicación no autorizada de imágenes íntimas y de datos personales en redes sociales, blogs y demás sitios de Internet. Por ello la jurisprudencia española tuvo que abordar el tratamiento de estos casos donde la imagen o un dato personal era distribuida sin permiso.

Numerosos casos juzgaban la revelación no autorizada de datos íntimos bajo una multitud de encuadres legales. Así los tribunales españoles fueron encontrando soluciones legales a esta problemática a través de diversas figuras penales.

Por ejemplo, el caso de un joven que accedió sin permiso al perfil de su primo en la red social Tuenti y cambió la clave del perfil y envió a sus contactos correos ofensivos al tiempo que indicaba en su perfil "reconozco que soy gay" para que fuera visto por todos los amigos del afectado. Al ser enjuiciado por un juzgado penal de Badajoz, la jueza acordó imponer al autor de la acción seis meses de prisión por el delito de descubrimiento y revelación de secretos, y por una falta de injurias[36].

Un juzgado de Pamplona condenó a un joven a una pena de seis meses de prisión y multa de 1080 euros como autor del delito de revelación de secretos por haber accedido sin consentimiento de una amiga a su cuenta de Tuenti. Al acceder al perfil colgó varias fotos mujeres desnudas e hizo público el perfil que hasta ese momento era reservado[37].

Un juzgado penal en Santander condenó a un año de cárcel a un hombre que colgó en la red social Tuenti catorce fotografías de su exnovia desnuda. La jueza consideró que estos hechos eran constitutivos del delito de violación de secretos[38].

Un caso de la Audiencia provincial de Alicante, condenó a una pena de cárcel de dos años a un joven que colgó en una red social fotos íntimas de su exnovia, en las que aparecía semidesnuda. La Audiencia consideró al joven culpable del delito de revelación de secretos por difundir imágenes que atentaban contra la intimidad de su ex pareja[39].

Se impuso pena de cuatro años, más 630 euros de multa y 7 mil euros de indemnizaciones para la persona que engañó a dos niñas de 12 y 11 años en la red Tuenti para que se desnudaran. La Audiencia de Cantabria impuso dicha pena al hombre que se hizo pasar por una chica de 14 años en Tuenti y convenció a estas dos niñas para que le enviasen fotografías de ellas desnudas.

En la SAP Lleida 25 febrero 2004[40] se condena por delito de injurias con publicidad a quien divulga la grabación consentida de una relación sexual. No se considera la existencia de un delito contra la intimidad pues la grabación se realizó con el consentimiento de la afectada, fue meses después, cuando, sin su consentimiento, se decide a divulgar la intimidad compartida. Un supuesto similar puede verse en SAP Huelva del 15 febrero de 2002[41].

La jurisprudencia civil española[42] considera intromisión en la vida privada a la publicación por la prensa de fotos de desnudos en una playa pública pero desierta.

Como puede apreciarse, existían en España numerosas condenas a personas por difundir imágenes de escenas íntimas aplicando entre otros el delito de revelación de secretos[43].

Durante el año 2014 comenzó a debatirse si el *revenge porn* era delito en España y si era necesario reformar la legislación entonces vigente. Pero ocurrió un caso específico que detonó el debate púbico y planteó la necesidad de legislar. Este caso llevó a que se incluyera la figura que analizamos en la reforma penal del año 2014. La inclusión de esta nueva figura se debió al caso de Olvido Hormigos, un concejal que pasó a la fama tras difundirse por Internet un vídeo íntimo que había grabado y enviado a su pareja[44].

36 *TOURIÑO, El derecho al olvido y la intimidad en Internet, Ed. Catarata, pág. 55, Madrid, 2104.*

37 *TOURIÑO, El derecho al olvido y la intimidad en Internet, pág. 54.*

38 *TOURIÑO, El derecho al olvido y la intimidad en Internet, pág. 54.*

39 *TOURIÑO, El derecho al olvido y la intimidad en Internet, pág. 54.*

40 *SAP Lleida 25 febrero 2004 (ARP 2002, 636).*

41 *SAP Huelva 15 febrero 2002 (JUR 2002, 115257).*

42 *STS español, (Sala 1ª) de 23 de junio de 2015, rec. nº 2409/2013.*

43 *En todos estos casos seguimos a TOURIÑO, Alejandro, El derecho al olvido y la intimidad en Internet, págs. 53/59.*

44 *No obstante haber formulado un reclamo por infracción a su privacidad por la situación en la que se vio envuelta, la víctima, aprovechando la notoriedad que le produjo el evento, terminó publicando un relato sobre el tema con nombres de ficción. Ver el libro de Olvido Hormigos, El Abrazo Infiel, Editorial RBA, Madrid, 2015. Todo lo cual lleva a cuestionar cuál es el efecto de las propias acciones de las víctimas del revenge porn y cómo debe ello incidir en sus reclamos civiles o penales.*

2.3. 2. Reforma del código penal español

A raíz de estos numerosos casos comenzaron a surgir propuestas de reforma de la normativa penal vigente, focalizadas en la necesidad de eliminar el *consentimiento de la víctima* como causal de exclusión de responsabilidad penal de la figura de publicación no autorizada de la imagen personal[45].

En octubre de 2012, el Ministerio de Justicia español incluyó esta figura en el anteproyecto de Código Penal. Con esta propuesta se buscaba castigar la "*divulgación no autorizada de imágenes o grabaciones íntimas, incluso si se han obtenido con consentimiento de la víctima*". En el informe oficial del proyecto se presenta esta nueva figura penal como una forma de protección especial de la mujer[46], aunque en realidad la figura ampara a víctimas de ambos sexos.

Hasta la introducción de esta propuesta de reforma, se contemplaba como delito en la figura básica del art. 197 del Código Penal español: (i) el apoderamiento de cartas, papeles, mensajes de correo electrónico u otros documentos de naturaleza personal de la víctima, y (ii) la interceptación de cualquier tipo de comunicación de la víctima, sea cual fuere la naturaleza y la vía de dicha comunicación interceptada. Ambas conductas exigen *la falta de consentimiento* de la víctima pues tutelan el secreto frente a su apoderamiento.

Con la reforma se propuso tutelar el caso de *las imágenes o grabaciones de otra persona obtenidas con su consentimiento pero que se divulgan contra su voluntad*, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad[47].

La reforma apuntaba claramente a la esencia del delito de revenge porn: la divulgación no autorizada de grabaciones o imágenes íntimas obtenidas con el consentimiento de la víctima, en situaciones claramente privadas, pero luego divulgadas sin su anuencia, cuando afecten gravemente a su intimidad.

El legislador español ubicó este nuevo delito dentro de la figura de descubrimiento y revelación de secretos prevista en el art. 197 del Código Penal. Esta reforma entró en vigencia en julio de 2015.

El proyecto ya aprobado modifica el art. 197 con un nuevo inciso séptimo que dice así "Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

El delito de *revenge porn* en el Código Penal español tiene los siguientes elementos:

"sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla": la acción principal consiste en difundir, revelar o ceder a terceros imágenes realizando este accionar sin autorización de la víctima.

"que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros": este es el típico supuesto de revenge porn, la imagen es generalmente captada con consentimiento del afectado y en un contexto de intimidad (ej. su domicilio o cualquier otro lugar privado: "*fuera del alcance de la mirada de terceros*") pero luego se usa o difunde contra su voluntad.

"cuando la divulgación menoscabe gravemente la intimidad personal de esa persona": este agregado es importante pues permite centrarse en los casos graves, esto es aquellos relativos a imágenes íntimas, generalmente de escenas sexuales.

Agravante: si (i) los hechos hubieran sido cometidos por el *cónyuge o por persona que esté o haya estado unida a él* por análoga relación de afectividad, aun sin convivencia, (ii) la víctima fuera *menor de edad* o una persona con discapacidad necesitada de especial protección, o (iii) los hechos se hubieran cometido con una *finalidad lucrativa*.

No se requiere en la figura básica una finalidad específica de lucro (es sí una agravante) ni ánimo

45 *COLAS TUREGANO, La importancia del consentimiento del sujeto pasivo en la protección penal del derecho a la propia imagen, en Rev. boliv. de derecho nº 15, enero 2013, pp. 160-179.*

46 *El informe que fundamenta la reforma dice: "El Código Penal ahonda, igualmente, en la protección de la mujer mediante la introducción de nuevas figuras delictivas, como el delito de matrimonio forzado, el de acoso u hostigamiento, la divulgación no autorizada de grabaciones o imágenes íntimas obtenidas con el consentimiento de la víctima y la alteración de los dispositivos telemáticos para controlar medidas cautelares".*

47 *Aprobado el Proyecto de Ley de Reforma del Código Penal, http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/200913Enlace_ReformaCodigoPenal.htm*

de venganza, aunque está implícito en el acto de difundir fotos íntimas de la ex pareja.

2.4. REINO UNIDO

En el Reino Unido también se legisló recientemente esta figura con una pena de dos años de prisión[48].

La reforma se aprobó a través de la *Criminal Justice and Courts Act 2015*[49], luego de una gran cantidad de casos[50] que tuvieron amplia repercusión por tratarse de personas famosas, tal el caso de Rihanna y de la cantante Tulisa Contostavlos. La sanción de la norma fue un avance pues con anterioridad a este fallo los fiscales requerían que se probara alguna suerte de acoso producido con las fotografías, o que se tuviera derecho de autor sobre las mismas.

En el caso Contostavlos v. Mendahun[51] un juez londinense otorgó una cautelar a la cantante Tulisa Contostavlos, quien se agraviaba del hecho que un video con escenas íntimas filmadas por su ex novio estaban circulando por Internet. La actora también demandó a varios sitios de Internet que habrían republicado los videos, logrando una indemnización de 42,500 libras esterlinas de uno de los demandados.

La nueva figura se denomina *Disclosing private sexual photographs and films with intent to cause distress*, y se diferencia de la versión española en que requiere la intención de causar malestar psicológico.

En febrero de 2016 Irlanda del Norte también se sumó a los países con legislación al aprobar una norma que penaliza la difusión de imágenes captadas con consentimiento[52].

2.5. CHILE

En Chile[53] se están discutiendo proyectos de leyes para criminalizar el *revenge porn*.

Las diputadas Andrea Molina y Claudia Nogueira presentaron un proyecto de ley que busca sancionar a quien publique imágenes de contenido sexual, ya sean fotos o videos, producidos en la privacidad de una pareja y difundidas sin consentimiento. El proyecto busca sancionar con multas e incluso cárcel a quienes publiquen y difundan este tipo de material, conocido como "porno venganza" o revenge porn. Las penas podrían alcanzar la reclusión menor en su grado medio a máximo (541 días a cinco años de cárcel) y multas de hasta 1.000 unidades tributarias mensuales (42 millones 220 mil pesos). Además, se buscan las mismas sanciones para los administradores de aquellos sitios de Internet que no bajen o eliminen de forma inmediata los contenidos de este tipo[54].

2.6. ALEMANIA

En octubre de 2015 Corte Federal alemana[55] dictó una sentencia en el cual dispuso que un ex novio debía borrar todas las imágenes íntimas de su novia, incluso para el caso que no pensara compartirlas o difundirlas a terceros. No se trata de un caso penal pero demuestra que los tribunales están dispuestos a amparar la privacidad sobre imágenes íntimas aunque fueron captadas con consentimiento de la víctima[56].

El argumento del tribunal fue que si bien la actora había consentido la captación de su imagen, el *consentimiento caduca cuando la relación de pareja finaliza*[57]. El tribunal fue más lejos y sostuvo que mantener las fotos almacenadas era violatorio de su derecho a la privacidad. Se hizo referencia al "poder manipulador" que generaba el tener estas fotos. La sentencia le ordena borrar todas las imágenes y videos.

---

48 *VINCENT, Sharing revenge porn in the UK now carries a two year jail sentence, The Verge, 13 de abril de 2015.*

49 *Ver http://www.legislation.gov.uk/ukpga/2015/2/introduction*

50 *En los ultimos dos años la policía había contabilizado 149 denuncias por casos de revenge porn. Ver la nota 'Revenge porn' illegal under new UK law, http://www.bbc.com/news/29596583*

51 *Contostavlos v. Mendahun [2012] EWHC 850 (QB) (29 de Marzo de 2012).*

52 *Revenge porn to become crime in Northern Ireland, Stormont rules, 11 de febrero de 2016.*

53 *Cfr. la nota "Diputadas UDI proponen sanción para difusión de fotos y videos íntimos", http://www.cooperativa.cl/noticias/pais/politica/udi/diputadas-udi-proponen-sancion-para-difusion-de-fotos-y-videos-intimos/2014-08-24/113255.html*

54 *Ver http://derechosdigitales.tumblr.com/post/95850658781/chile-presentan-proyecto-de-ley-contra-la-porno*

55 *Bundesgerichtshof (BGH), sentencia del 22/10/2015.*

56 *German court orders man to destroy naked images, BBC, 22 de diciembre de 2015.*

57 *El argumento es interesante y nos recuerda que en materia de protección de datos personales, el consentimiento se puede revocar, con lo cual sería posible invocar la norma que admite la revocación del "presunto consentimiento" para evitar el uso de sus datos personales, que incluye a las imágenes.*

Un caso anterior fallado en agosto de 2015 por un tribunal de Düsseldorf condenó a una persona que había difundido fotos íntimas de la actora a pagar la suma de 15,000 Euros[58].

2.7. NUEVA ZELANDA

En julio de 2015 Nueva Zelanda aprobó la ley *Harmful Digital Communications Act* mediante la cual se penaliza el *revenge porn*. Con anterioridad a esta reforma la *Privacy Act* (ley de protección de datos del año 1993) excluía de su aplicación el procesamiento de los datos personales creados o recolectados en el ámbito doméstico como sucede con muchas leyes de protección de datos personales[59].

Sin embargo, luego de la reforma, esta excepción a la Privacy Act no se aplica cuando se publica o se difunde material altamente ofensivo para el titular del dato personal. La reforma cubre solamente material que una persona ordinaria o ciudadano común considera ofensiva, según el estándar desarrollando por los tribunales de Nueva Zelanda en el caso *Hosking v. Runting*[60].

En el citado caso, la Corte de Apelaciones rechazó una demanda por violación a la privacidad de dos menores. Los hijos gemelos de una pareja famosa fueron fotografiados en un mercado, un lugar público, sin consentimiento de los padres. Los padres se habían negado a dar entrevistas y dejar que se publicaran fotos de sus hijos en la prensa con anterioridad. El tribunal reconoció la existencia de un tort por violación a la privacidad pero se negó a otorgar daños en el caso concreto pues entendió que las fotos no eran altamente ofensivas para el ciudadano común ("highly offensive and objectionable to a reasonable person of ordinary sensibilities"), aunque si lo fueran para sus padres. Con fundamento en este estándar la reforma requiere que las fotos sean altamente ofensivas[61].

2.8. CANADÁ

La provincia canadiense de Manitoba fue la primera jurisdicción en aprobar una norma (Intimate Image Protection Act,) para evitar el revenge porn. La norma entró en vigencia en enero de 2016. La norma penaliza la distribución no consentida de imágenes y videos sexuales y permite a las víctimas demandar a los autores y reclamar los daños ocasionados.

La norma se originó en una serie de casos famosos, pero también en la evidente necesidad de actuar frente a la gran cantidad de casos denunciados. El Canadian Centre for Child Protection (C3P), que presta ayuda a las víctimas de estos delitos tuvo 350 denuncias de casos de revenge por desde marzo de 2015 a enero de 2016. La mitad de esos casos eran menores de entre 15 y 17 años[62]

3. EL REVENGE PORN EN EL DERECHO ARGENTINO

3.1. PRIMEROS CASOS

En la Argentina, los primeros casos de *revenge porn* se intentaron canalizar penalmente -en forma infructuosa-, por la vía de los delitos contra los derechos intelectuales y de las injurias. Los hechos más típicos eran casos de ex novios o novias que difundían por Internet, en blogs o por medio de un correo electrónico una foto o video íntimo de su ex pareja. En algunos casos la foto no era real sino que se realizaba un fotomontaje, alterándola y agregando desnudos no presentes en la foto original.

Lo único que desea la víctima en estos casos es lograr retirar de Internet sus fotos íntimas. El castigo del culpable suele quedar en segundo lugar frente a esta urgente necesidad de lograr remover sus datos y contenidos privados de la web. Pero las cautelares suelen ser difíciles de obtener. Recordemos que en el fuero penal las soluciones se complican porque es sabido que la jurisprudencia no concede medidas cautelares a menos que exista un auto de procesamiento, lo cual sirve de verosimilitud del derecho para la cautelar, o por lo menos la convocatoria a indagatoria[63].

58 *http://www.dw.com/en/in-germany-your-ex-must-destroy-nude-photos-on-request/a-18934921*

59 *Ver por ej. arts. 21 y 24 de la ley de protección de datos de Argentina.*

60 *Hosking and Hosking v Runting & Pacific Magazines Nz Ltd, sentencia del 25 de marzo de 2004, [2004] NZCA 34; [2003] 3 NZLR 385 (New Zealand Court of Appeal).*

61 *https://opcwebsite.cwp.govt.nz/news-and-publications/guidance-resources/hdca-faqs/*

62 *Ver CBC News, Manitoba revenge porn law aims to empower victims, http://www.cbc.ca/news/canada/manitoba/manitoba-revenge-porn-law-aims-to-empower-victims-1.3408847*

63 *CNCrim y Correc, Sala VI, 9/12/2008, L., M.E. s/medida cautelares; CNFed.Crim y Correc. Sala I, 5/1/2015, D.A.R. s/ medida cautelar.*

3.2. DIFICULTADES PARA APLICAR EL DERECHO DE AUTOR

Entendemos que se recurrió al Derecho de Autor pues el derecho a la imagen estaba contenido en la ley de derechos intelectuales (ley 11.723). En estos casos se argumentó que la foto era una obra intelectual y que quien la reproducía sin autorización incurría en el delito de reproducción no autorizada de obra intelectual.

A nuestro entender, esta tesis tiene varios inconvenientes. El delito de reproducción no autorizada de obra intelectual no comprende a la imagen como objeto protegido sino a las obras intelectuales originales[64]. La imagen de una persona es un derecho personalísimo, no un derecho de propiedad intelectual. La ley 11.723 reprimía solo la reproducción no autorizada de obras intelectuales, no de imágenes[65].

Una fotografía puede calificar como obra intelectual bajo la ley 11.723. Esa fotografía puede contener la imagen de una persona, pero en ese caso el autor de la obra (la foto) es quien toma la fotografía con la cámara y no quien aparece retratada en ella. Por lo tanto, quien aparece en una fotografía no está legitimada para reclamar por el contenido de la obra[66], a menos que tenga una cesión escrita sobre los derechos de autor de la foto íntima (algo inusual en el contexto donde se toman este tipo de fotografías).

Asimismo, no toda imagen captada fotográficamente constituye una obra intelectual. Crear una obra intelectual implica dotar a la foto de originalidad, y la intención del sujeto que ello ocurra. Si bien la originalidad es un requisito muy fácil de obtener en Derecho de Autor, podría llegar a considerarse que la obra no es original.

Las instantáneas de escenas íntimas no parecen pretender llegar a la categoría de obras intelectuales, no existe el elemento volitivo de crear una obra intelectual[67], y en muchos casos carecen de originalidad para ser consideradas obras intelectuales.

Asimismo en el derecho argentino no existe la doctrina de las "meras fotografías", que ampara fotografías cuando no sean originales, pero, igualmente tienen valor comercial. Un ejemplo de esta protección lo encontramos en la legislación española[68]. Las meras fotografías son protegidas porque pese a no ser originales, constituyen el resultado de un trabajo que puede tener gran valor comercial, documental, científico e informativo. En España con esta norma incluso se amparan las fotografías realizadas automáticamente o mecánicamente por instalaciones de seguridad[69].

Está claro que la persona fotografiada en este tipo de imágenes no es la autora, y si se trata de una auto foto (conocidas como *selfies*), o de un video casero, menos aún suele ser la intención de hacer una obra.

Asimismo el art. 34 de la ley 11.723, en una de sus tantas contradicciones que nuestra ley autoral tiene con el Convenio de Berna, dispone que "*Debe inscribirse sobre la obra fotográfica o cinematográfica la fecha, el lugar de publicación, el nombre o la marca del autor o editor. El incumplimiento de este requisito no dará lugar a la acción penal prevista en esta ley para el caso de reproducción de dichas obras*". En las imágenes o videos que analizamos (videos caseros o selfies con escenas íntimas), es infrecuente su registro en la Dirección de Derechos de Autor o el agregado del nombre del autor. Podría argumentarse sin embargo que se trata de una obra inédita también amparada por el art. 72 inc. "a" de la ley 11.723[70].

Finalmente entendemos que no fue la intención del legislador transformar cualquier foto (o videos) de escenas íntimas en una obra intelectual y usar la ley 11.723 para perseguir penalmente a quien las difunde sin permiso. El Derecho Penal no admite ese razonamiento por analogía. No obstante lo dicho, no cabe descartar la calificación de obra intelectual en algunos casos, y poder usar los procedimientos de notice and take down don-

64 *Art. 72 inc a ley 11723 - Sin perjuicio de la disposición general del artículo precedente, se consideran casos especiales de defraudación y sufrirán la pena que él establece, además del secuestro de la edición ilícita: a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabientes.*

65 *En Argentina hasta agosto de 2015 el derecho a la imagen estaba tutelado por la ley 11723. Con la entrada en vigencia del nuevo Código Civil y Comercial el 1 de agosto de 2015, la imagen es un derecho autónomo tutelado por el art. 52 del nuevo Código.*

66 *Podría tratarse de una selfie, en cuyo caso la aplicación de la ley 11723 es más lógica o de una foto tomada de común acuerdo por todos los participantes de la foto, en cuyo caso se podría hablar de coautoría de la obra intelectual.*

67 *Sin perjuicio que en esto existe toda una industria que comercializa fotografías y la creación de obras audiovisuales les da derecho a amparar la obra dentro del régimen de la ley 11.723.*

68 *El art. 128 de la LPI española dice "Quien realice una fotografía u otra reproducción obtenida por procedimiento análogo a aquélla, cuando ni una ni otra tengan el carácter de obras protegidas en el Libro I, goza del derecho exclusivo de autorizar su reproducción, distribución y comunicación pública, en los mismos términos reconocidos en la presente Ley a los autores de obras fotográficas. Este derecho tendrá una duración de veinticinco años computados desde el día 1 de enero del año siguiente a la fecha de realización de la fotografía o reproducción".*

69 *BERCOVITZ RODRIGUEZ-CANO, Manual de Propiedad Intelectual, Tirant lo Blanch, Valencia 2015, pág. 280.*

70 *CNCasac. Penal, sala II, 2/4/2004, De Simone, Daniel E. y otro s/ rec. de casación, publicado en LL 05/11/2004 , p.7.*

de estén legislados para dar de baja esta clase de contenido[71].

Los casos hasta la fecha decididos en la Argentina siguen esta línea. La Cámara del Crimen[72] confirmó un fallo de primera instancia y desestimó una denuncia penal iniciada por una modelo a la que le publicaron fotos personales en Internet. La querella argumentó que su agravio se sustentaba en "la violación del derecho a la imagen" de la modelo ya que "en el sitio web se han publicado imágenes sin su autorización; ello, según la interpretación que formularon de los arts. 31 y 71 de la ley 11.723"[73].

Los jueces sostuvieron que "sin perjuicio de las acciones civiles que pudieren corresponder, dado que las imágenes publicadas, tal como se señaló en la denuncia, se corresponden con trabajos fotográficos y artísticos por los cuales la denunciante se encuentra vinculada contractualmente, al haber autorizado el uso de su imagen, corresponde confirmar la decisión en cuanto rechazó la petición de ser tenida por querellante".

La decisión se funda en que "... la legitimación se encuentra, en realidad, en cabeza de los autores y otros titulares de la propiedad intelectual y sus derechohabientes, expresión que debe entenderse referida a los adquirentes de la obra, o a los cesionarios parciales, o a las personas autorizadas por el autor a ejercer sus derechos". Es decir, entendieron que no era titular de obra intelectual alguna. Por todo ello, confirmaron lo decidido en primera instancia y desestimaron por inexistencia de delito la denuncia intentada por la modelo.

En el mismo sentido, otra decisión[74] desestimó una denuncia penal con fundamento en la ley 11.723. El caso versaba sobre la creación de una página web con datos filiatorios, domicilio y dos fotografías de una persona desnuda a la cual se le había agregado el rostro de la hija del denunciante. Este había tomado la fotografía original sobre la cual se realizó el fotomontaje.

El tribunal entendió que la imagen en cuestión "... no encuadraba en la ley 11.723 pues no se daban los requisitos de originalidad y creatividad que la misma reclama para otorgar protección legal a la simple fotografía con la cual se habría confeccionado el documento mencionado y además por no encontrarse registrada ante el organismo respectivo con el fin de resguardar la propiedad intelectual".

Respecto a las injurias, en estos supuestos (publicación no autorizada de fotos íntimas) las querellas presentadas se fundaron en el descrédito al honor que genera la difusión de imágenes íntimas destinadas a quedar en reserva. Los jueces también consideraron que la difusión de estas imágenes no encuadraban dentro del delito de injurias, y en estos casos se sumó el obstáculo adicional que requiere accionar por vía de querella por ser delito de acción privada y la mayoría de los casos se presentaron como simple denuncia.

3.3. TIPOLOGÍA DE CASOS Y CONCURRENCIA CON OTRAS FIGURAS PENALES

El fenómeno del *revenge porn* puede ser objeto de algunas clasificaciones en función de la voluntad de la publicación, de los motivos de la difusión, y de los participantes y su edad. Esta clasificación sirve para entender mejor qué está cubierto por la ley y que falta regular en la materia.

En el análisis de estos casos partimos de la base que la fotografía o video de la víctima contiene escenas intimas que en principio no estaban destinadas a ser difundidas, y por lo tanto los registros de esas imágenes están amparados por el derecho a la privacidad y el derecho a la imagen de quienes en ella aparecen (arts. 52 y 53 del nuevo Código Civil y Comercial).

En los casos que analizamos estas fotos o videos suelen ser captados *con permiso* de la víctima. Puede suceder que sean grabaciones caseras de escenas íntimas, sobre las que luego se pierde el control, ya sea por un acto de ingreso no autorizado al lugar donde se encuentran (generalmente un ordenador, disco rígido, pen drive o *smartphone* o incluso en un proveedor en la *nube*), o porque voluntariamente se comparte con la pareja durante la relación. Ha sucedido también que se lleva a reparar el *smartphone* y el personal del servicio técnico copia sin permiso el contenido, o bien que se extravía el mismo, y quien lo encuentra divulga su contenido o lo "vende" a la prensa amarilla al descubrir que su titular es una persona famosa.

Respecto a la *persona retratada*, ésta puede ser un mayor o un menor, lo cual es importante para diferenciar algunas situaciones delictuales más serias. La presencia de un menor de edad en esta clase de imágenes nos lleva al art. 128 del Cod. Penal, además del delito de amenazas coactivas o la extorsión si fueron obtenidas por la fuerza. La

71 *FITZPATRICK, Here's How Celebs Can Get Their Nude Selfies Taken Down, Revista Time, http://time.com/3256732/jennifer-lawrence-selfies-copyright/*

72 *CNCrim. sala VII, 13/2/2013, "N.A. s/querella".*

73 *Cfr. la nota sin autor, El modelo del delito inexistente, Diario Judicial, 17/5/2013.*

74 *CNCrim. sala I, 11/2/2000, "Fappiano, Guillermo".*

figura de revenge porn que analizamos se refiere siempre a adultos.

Respecto a la *persona que capta la imagen*, puede ser también un *mayor o un menor*. Este aspecto es indistinto a los fines del delito que analizamos.

El registro de la imagen puede haber tenido lugar *con o sin consentimiento* del registrado. El consentimiento también aparece en la difusión y es un consentimiento distinto del consentimiento dado para la captación, es decir, la imagen puede haber sido tomada con consentimiento pero luego difundida contra la voluntad de la víctima. Incluso aunque la víctima haya dado consentimiento para la difusión, cabe recordar que bajo la ley argentina en materia de derechos personalísimos -la imagen es uno de ellos-, el consentimiento no se presume, es de interpretación restrictiva, y libremente revocable[75].

La captación contra la voluntad del sujeto puede ocurrir mediante el uso de artefactos tecnológicos que permiten grabarla en forma subrepticia, a distancia, *hackeando* la seguridad, o porque está accesible públicamente de alguna manera. El ingreso sin permiso a un ordenador o sistema de correo donde se encuentre la foto puede constituir el delito de acceso no autorizado a sistemas informáticos (art. 153 bis Cod. Penal) o violación de correo electrónico (art. 153 del Cód. Penal).

Finalmente cabe definir la *finalidad de la captación*, reproducción o distribución de la imagen, lo cual será determinante para los distintos supuestos que analizamos. Esta puede ser:

hacer un video casero para uso privado, que luego es difundido por la ex pareja con ánimo de venganza: estos son los casos conocidos como *revenge porn*. La finalidad en estos casos suele ser usar las imágenes para humillar públicamente a la víctima, cuando tiene lugar entre adultos[76], pero no se requiere un ánimo de venganza.

Dar a publicidad las imágenes o videos con el fin de perjudicar, humillar o burlarse al sujeto[77]: son los casos recientes de celebrities, o también casos de bullying escolar.

usar las imágenes con fines de corromper a menores[78], lo cual también puede quedar dentro de la figura del delito de *grooming*,

usar las imágenes con fines de extorsión a la víctima, o para pedir más imágenes. En un caso de pedido constante de fotografías de imágenes pornográficas a menores, se calificó la conducta como constitutiva del delito de amenazas coactivas[79].

Finalmente sería posible aplicar en algunos casos la figura contravencional de hostigamiento, prevista en el art. 52 del Código Contravencional de la Ciudad Autónoma de Buenos Aires (Ley n. 1.472). La norma dispone que "Quien intimida u hostiga de modo amenazante o maltrata físicamente a otro, siempre que el hecho no constituya delito, es sancionado con uno (1) a cinco (5) días de trabajo de utilidad pública, multa de doscientos ($ 200) a un mil ($ 1.000) pesos o uno (1) a cinco (5) días de arresto".

En algunos supuestos, la constante publicación y difusión no autorizada de fotografías íntimas de una persona en la web podría calificar como una suerte de hostigamiento, si tiene como efecto intimidar o amenazar a la víctima en su vida en sociedad.

3.4. PRIMER PRECEDENTE

75 *Según el art. 55 del nuevo Código Civil y Comercial: " Disposición de derechos personalísimos. El consentimiento para la disposición de los derechos personalísimos es admitido si no es contrario a la ley, la moral o las buenas costumbres. Este consentimiento no se presume, es de interpretación restrictiva, y libremente revocable" Asimismo el decreto reglamentario de la ley de protección de datos personales dispone que: "El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos." (art. 5 decreto 1558/2001).*

76 *Si se tratan de menores que envían éstas imágenes puede catalogarse como un caso como distribución de pornografía infantil o delito de sexting. Ver PALAZZI, Los delitos informáticos en el Código Penal, segunda edición, 2012, Abeledo Perrot, pág. 46/47.*

77 *En algunos países está legislado penalmente el acoso o bulling escolar, y estas acciones también puede ser tipificadas como delitos de injurias, amenazas, coacciones, etc.*

78 *Para un caso de envío de imágenes pornográficas a menores catalogado como corrupción ver TOral. en lo Criminal Nro. 1 de Necochea, 5/6/2013, F., L. N. s/ corrupción de menores agravada, LL 2014-C, 60, DPYC 2014 (agosto), 185 con nota de Silvina Andrea Alonso y nuestra nota El grooming tipificado como corrupción de menores agravada, en Revista de Derecho Penal y Procesal Penal, Abeledo, Febrero 2014, pág. 315, (en autoría con Carla Delle Donne). Ver también el caso CNCrim, Sala IV, c. 1522/2011, C.F.N. s/corrupción de menor de trece años (remisión de fotos pornográficas a menor de 13 años con el fin de corromperla).*

79 *CNCasac Penal Sala I, Flamenco Saavedra Causa 16.238 Flamenco Saavedra Sala I reg. 22.319 24/10/2013. En el caso el imputado amedrentó y hostigó –vía internet- a una niña de trece años con la finalidad de obtener material fotográfico y fílmico de carácter pornográfico. Luego de calificar el acto como delitos de amenazas coactivas, el tribunal sostuvo que corresponde agotar los medios de investigación con el fin de determinar la posible comisión de un delito de acción pública, ya que la conducta imputada no se limitaría al menoscabo de la dignidad de la víctima y a una grave injerencia en su fuero íntimo por las amenazas perpetradas, sino que por el tenor pornográfico del material que se habría obtenido coactivamente y la minoridad de la damnificada, no puede descartarse la posible comisión de delitos vinculados con la difusión de pornografía infantil (ley 26.388).*

Un caso que tuvo mucha prensa en la Argentina es el caso conocido como "Camus hacker". El autor fue procesado en primera instancia por considerárselo responsable en los delitos de amenazas coactivas y extorsión en grado de tentativa. Se trató de una causa penal en la cual se investigaba la filtración en las redes sociales de fotos íntimas de famosos como Coki Ramírez, Diego Korol, Jorge Zonzini, Noelia Marzol, Sergio "Maravilla" Martinez, Fátima Florez, Iliana Calabró, Verónica Lozano y Annalisa Santi.

El procesamiento fue dictado por el Juzgado de Instrucción Penal N° 49, a cargo de la Doctora María Dolores Fontbona de Pombo. La acción penal se inició con una investigación preliminar de oficio del Fiscal Ricardo Saenz. Luego se inició la instrucción penal a través la Fiscalía N° 19[80]. La causa fue elevada a juicio oral y terminó con un juicio abreviado en el cual se acordó la pena de tres años de prisión en suspenso por el delito de coacción[81].

Como fue un juicio abreviado, no se dice nada cerca de la sustracción de imágenes y si éstas pueden ser objeto del delito de hurto. La querella se había iniciado por los delitos de coacción y amenazas coactivas[82].

3.5. PROPUESTAS DE REFORMA EN EL PROYECTO DE LA LEY 26.388

En el año 2008 se reformó el Código Penal en materia de delitos informáticos. La ley 26.388 introdujo nuevos delitos relacionados con la tecnología tales como la estafa informática, el daño informático, la creación y distribución de pornografía infantil, la violación del correo electrónico y el acceso ilegítimo a sistemas informáticos.

Ese proyecto de reforma[83] también había planteado incorporar el delito de captación y uso no autorizado de datos, imágenes y sonidos (proyectado como art. 153 ter), pero este tipo penal fue finalmente descartado en el debate parlamentario porque se entendió que podría alcanzar a las cámaras ocultas y por ende constituía una amenaza al periodismo de investigación[84]. Se consideró en definitiva que la protección civil era suficiente tutela para la imagen.

Fue así como en la reforma del Código Penal (ley 26.388) que incorporó ciertos delitos informáticos quedó un vacío respecto de la tutela penal de la imagen. Este vacío, generado por temor a avasallar a la prensa, deja sin embargo un problema en la materia pues las nuevas tecnologías han avanzado enormemente y hoy en día es muy fácil captar la imagen de diversas formas y reproducirla y ponerla a disposición de toda la web. Existen como hemos visto un sinnúmero de delitos que amparan conductas relacionadas con el uso que se da a la imagen pero ninguno que en forma concreta tutele la difusión no autorizada de imágenes captadas con consentimiento de la víctima.

3.6. EL ANTEPROYECTO DE CÓDIGO PENAL DEL AÑO 2014

La comisión para la elaboración del proyecto de reforma y actualización del Código Penal de la Nación creada por el Decreto 678/12 presentó un anteproyecto en febrero de 2014.

El art. 120 del anteproyecto bajo el epígrafe de "Violación de la privacidad" propone "Será reprimido con prisión de 6 meses a 2 años y multa de diez a ciento cincuenta días, el que vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se apoderare de registros no destinados a la publicidad".

La norma asimismo contiene una agravante que duplica la pena en casos de comisión de hechos mencionados en el párrafo primero mediando abuso de oficio o profesión, o de su condición de funcionario público.

Como puede apreciarse de la lectura de primer párrafo del art. 120 del anteproyecto se trata en general de registros de imagen captados sin consentimiento del titular, incluso sin conocimiento del mismo mediante el uso de dispositivos tecnológicos que ayudan a invadir la privacidad.

---

80 *Ver la nota Procesaron a Camus Hacker por amenazas y extorsión en el caso del robo de fotos íntimas a famosos, Infobae, 12 de febrero de 2015.*

81 *Ver Tribunal Oral n. 6, causa 4786, 2/12/2015, Ioselli, Emanuel Carlos. Del acta del juicio de abreviado surge que se pacta condena por coacción, por lo tanto el tribunal no se pronuncia sobre la sustracción de las imágenes.*

82 *Las amenazas coactivas alegadas eran contra la señorita Analisa Santi, una ex-estudiante de la Facultad de Derecho de la Pontificia Universidad Católica Argentina que prefirió dejar el Derecho luego de cursar un par de años en la UCA y ser modelo publicitaria.*

83 *El artículo propuesto por la Cámara de Diputados establecía como art. 153 ter del Código Penal era el siguiente: "Será reprimido con prisión de un mes a dos años, el que ilegítimamente y para vulnerar la privacidad de otro, utilizando mecanismos de escucha, intercepción, transmisión, grabación o reproducción de voces, sonidos o imágenes, obtuviere, difundiere, revelare o cediere a terceros los datos o hechos descubiertos o las imágenes captadas". La norma proyectada disponía en un segundo párrafo la exención de responsabilidad penal a quien realizara alguna de las conductas descriptas en el primer párrafo "cuando el único propósito sea garantizar el interés público".*

84 *PALAZZI, Los delitos informáticos en el Código Penal, pág. 148, 2da edición, Abeledo, 2012.*

Pero las fotos o videos sobre sus escenas íntimas captadas con consentimiento pero sin intención de difundirlas no parecen quedar dentro del primer párrafo. Por otra parte lo importante del supuesto que analizamos no es tanto la captación o apoderamiento (generalmente consentida) sino la difusión no autorizada de algo que debe quedar en la vida privada de las personas.

La norma proyectada tal vez debería incluir en un nuevo párrafo a la publicación o difusión de la imagen como una acción separada de la captación en sí misma, es decir una alternativa a la violación a la privacidad, como sucede con el delito de violación de correspondencia que separa el acceso de la publicación. Y además cabría diferenciar si es el mismo sujeto que la pública o un tercero.

Entendemos que en el proyecto de reforma el verbo *apoderarse* no es utilizado en el sentido de la acción del hurto sino en el sentido de copiar digitalmente el contenido. Es que no tiene otra interpretación en la edad actual dicho término cuando la mayoría de supuestos de captación de la imagen será en formato digital, y almacenada en medios electrónicos. Esto lleva a que el apoderamiento de la imagen muchas veces no implica desapoderar al titular del mismo, sino simplemente hacer una copia digital del archivo.

4. FUNDAMENTOS PARA PENALIZAR LA DIFUSIÓN NO AUTORIZADA DE VIDEOS O IMÁGENES ÍNTIMAS

4.1. LA PRIVACIDAD FRENTE A LAS NUEVAS TECNOLOGÍAS

El primer fundamento para penalizar los actos de revenge porn es el derecho a la intimidad de las personas cuya imagen es difundida sin permiso.

La viralización de Internet hace que estas imágenes privadas puedan llegar a millones de personas, humillando y estigmatizando a la víctima al darse a conocer aspectos de su vida íntima que deben quedar en reserva. Está en juego la tutela de la dignidad humana, punto central de los derechos personalísimos reconocido por la normativa de derecho privado[85].

En la Sociedad de la Información el individuo sigue teniendo el dominio sobre sus datos personales lo que incluye el control sobre su propia imagen, y ello le da derecho a decidir cuándo y dónde ésta puede ser publicada salvo las excepciones previstas en el Código Civil[86]. Difundir sin permiso escenas íntimas, dado el enorme daño que provocan, es una forma de dificultar este derecho a controlar la información personal sobre una persona y constituye una seria lesión a la intimidad que merece sanción penal. Esta sanción no es posible por las razones ya expuestas. La propuesta que aquí realizamos tiene por finalidad cumplir con tratados internacionales y cubrir el vacío en el Código Penal.

Legislar este aspecto de la imagen, como todo lo que ocurre con las nuevas tecnologías, no es tarea fácil. Dada la amplia difusión del uso de videocámaras, celulares, aplicaciones móviles, y redes sociales el uso de la imagen estática o en movimiento se ha expandido enormemente. Cualquier puede captar y subir una imagen online en segundos compartiéndola con millones de personas. Pero ello no implica que el derecho a la imagen deba quedar anulado o porque ahora resulta más fácil su infracción

La libertad de expresión no se extiende a divulgar la vida privada e íntima de las personas, y no existe ningún interés público que justifique publicar o dar a conocer escenas intimas de dos personas adultas manteniendo una relación sexual. De una exégesis de la ley 11.723 (art. 31) se extrae que el legislador ha prohibido como regla la reproducción de la imagen en resguardo del correlativo derecho a ella, que sólo cede si se dan circunstancias que tengan en mira un interés general que aconseje hacerlas prevalecer por sobre aquél derecho[87]. Este

85 *Art. 52 del Código Civil y Comercial. Afectaciones a la dignidad. La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1.*

86 *Artículo 53 del Código Civil y Comercial. Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos: a) que la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario; c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.*

87 *CSJN, 28/6/1988, Lambrechi, Norma Beatriz y otra c/ Wilton Palace Hotel y otro., Fallos 311:1171.*

interés general no estará presente en el supuesto que analizamos.

Creemos que resulta necesario sancionar penalmente la publicación en Internet de imágenes de connotación sexual sin el consentimiento del involucrado.

Los males sociales se verán siempre reflejados en la red y deben prevenirse las formas de combatirlos pues el efecto es mucho mayor que en el mundo offline.

4.2. LA NORMATIVA DE VIOLENCIA DE GÉNERO

Tal como sostuvimos en otra oportunidad[88], el principal fundamento para penalizar el revenge porn es la normativa de violencia de género contenida en la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (conocida como "Convención de Belem do Pará"). En Argentina, la Ley 24.632 aprobó esta Convención que forma parte del derecho interno argentino.

Entendemos que esta norma es relevante pues la mayoría de los casos de *revenge porn* tienen como víctimas a mujeres[89].

Según la definición dada por la Convención, la *violencia contra la mujer* incluye daño o *sufrimiento psicológico* a la mujer, lo que puede ocurrir sin lugar a dudas con la difusión no autorizada en Internet de imágenes íntimas que originalmente fueron captadas con su consentimiento[90] pero sin su autorización para la difusión posterior.

La Convención también dispone que toda mujer tiene derecho a una vida libre de violencia, tanto en el ámbito público como en el privado (art. 3).

Finalmente la Convención requiere a los Estados firmantes poseer recursos judiciales de protección[91] de estos derechos e incluso sanciones penales[92]. Nuestra opinión es que esta Convención debe ser la base para la figura penal que analizamos.

El intento y propuesta de penalizar los actos de "revenge porn" ha tenido fuerte respaldo en el movimiento que impulsa normas de género[93].

Es cierto que los tipos penales relacionados con la violencia de género han sido criticados en alguna oportunidad por su desigualdad, sin embargo entendemos que el justificativo de darles un tratamiento diferente reside en amparar estas situaciones que son más graves y reprochables socialmente y que en la práctica son las que más frecuentemente tienen lugar.

Otra justificación de la necesidad de penalizar esta conductas está dada por la ineficacia de las figuras civiles. La sanción civil es pecuniaria y llega tarde, junto con una cautelar que nunca va a lograr limpiar de Internet todas las imágenes, que podrán seguir apareciendo sin límite de tiempo alguno[94]. Por otra parte, la protección que en este ámbito de la privacidad otorga el derecho penal es más que necesaria, como claramente lo ha señalado la doctrina civilista[95].

---

88 *PALAZZI, Introducción al problema del Revenge porn, Working Paper No. 1 del Programa de Derecho de Internet de la Universidad de San Andrés, abril de 105, y nuestra nota Protección penal de la difusión no autorizada de la imagen íntima captada con consentimiento de su titular y el problema del "revenge porn, en Revista de Derecho Penal y Procesal Penal, No. 8, 2015, pp. 1587-1598.*

89 *CITRON, Are Men Really Harassed Online More Than Women?, FORBES, 9 de mayo de 2014. La columnista Jil Filipovic destacó en el diario inglés The Guardian: "No existen webs populares de porno vengativo con fotos de hombres desnudos porque como sociedad no pensamos que sea degradante o humillante que un hombre sea sexualmente activo [...] En el fondo, las webs de 'revenge porn' no son sobre chicas desnudas; para eso ya hay muchas en las que posan con su consentimiento. Todo esto trata sobre odiar a las mujeres, divertirse viendo cómo se viola su intimidad e hiriéndolas". Cfr. FILIPOVOC, 'Revenge porn' is about degrading women sexually and professionally, The Guardian, 28 de enero de 2013. Ver también la nota de VALENTI, What's Wrong With Checking Out Stolen Nude Photos of Celebrities, The Atlantic, 1/9/2014.*

90 *El artículo 2 de la Convención señala que se entenderá que violencia contra la mujer incluye la violencia física, sexual y psicológica: a. que tenga lugar dentro de la familia o unidad doméstica o en cualquier otra relación interpersonal, ya sea que el agresor comparta o haya compartido el mismo domicilio que la mujer, y que comprende, entre otros, violación, maltrato y abuso sexual.*

91 *El artículo 4 establece que "Toda mujer tiene derecho al reconocimiento, goce, ejercicio y protección de todos los derechos humanos y a las libertades consagradas por los instrumentos regionales e internacionales sobre derechos humanos. Estos derechos comprenden, entre otros:... b. el derecho a que se respete su integridad ... psíquica y moral, e. el derecho a que se respete la dignidad inherente a su persona y que se proteja a su familia; g. el derecho a un recurso sencillo y rápido ante los tribunales competentes, que la ampare contra actos que violen sus derechos.*

92 *Cfr. Artículo 7. Los Estados Partes condenan todas las formas de violencia contra la mujer y convienen en adoptar, por todos los medios apropiados y sin dilaciones, políticas, orientadas a prevenir, sancionar y erradicar dicha violencia y en llevar a cabo lo siguiente: c. incluir en su legislación interna normas penales, civiles y administrativas, así como las de otra naturaleza que sean necesarias para prevenir, sancionar y erradicar la violencia contra la mujer y adoptar las medidas administrativas apropiadas que sean del caso; d. adoptar medidas jurídicas para conminar al agresor a abstenerse de hostigar, intimidar, amenazar, dañar o poner en peligro la vida de la mujer de cualquier forma que atente contra su integridad o perjudique su propiedad.*

93 *RAMIREZ, La rebelión femenina contra el porno vengativo en internet, diario El País, 30 de enero de 2013 y la obra de Danielle Keats CITRON, Hate Crimes in cyberspace, Harvard, 2014, p. 143-166.*

94 *Ver los casos comentados por Danielle CITRON que incluyen acosos por años en la web. CITRON, Hate Crimes in cyberspace, págs. 35 a 72.*

95 *Borda, Una ley estéril, ED 67-581 (1976). El autor, al comentar la reforma del Código Civil que introdujo el art. 1071 bis –*

4.3. LIBERTAD DE EXPRESIÓN Y FALTA DE INTERÉS PÚBLICO

El tercer argumento es un argumento negativo, relativa a la falta de interés público en la publicación o difusión de estas imágenes que forman parte de la vida privada de las personas. Nadie puede argumentar interés legítimo alguno para difundirlas. La libertad de expresión en este caso debe ceder frente a la privacidad del contenido.

En Estados Unidos se ha escrito mucho sobre este conflicto con otros derechos. El problema se presenta porque en Estados Unidos el discurso verdadero tiene protección constitucional. La foto en un caso de revenge porn es verdadera, y no hay una excepción legal prevista para justificar su supresión o penalizar a quien la difunde. El mejor ejemplo es el caso del hate speech en Estados Unidos. Se suele argumentar que sin protección constitucional para el *hate speech*, no habría "mercado de las ideas" sobre, por ejemplo las ideas nazis. Se sostiene que para amparar el discurso que la sociedad encuentra aceptable también se debe amparar el discurso que la sociedad encuentra repugnante. Esto incluye el discurso sin valor tal como el hate speech o la pornografía[96].

Entendemos que no cabe *ab initio* tener una postura negativa a esta tipo de normas, que pueden convivir con la libertad de prensa si se logra encontrar un estándar adecuado para permitir que sobreviva.

Siempre ha existido y va a existir una tensión *natural* entre la libertad de información (y de prensa) y la protección de la vida privada. Pero encontramos que no hay contradicción pues estas escenas íntimas carecen de interés público alguno, salvo el morbo del público consumidor de esta clase de imágenes, que no podrá invocar derecho alguno de acceso a las mismas.

La falta de interés público de las imágenes relacionadas con actos de *revenge porn* se evidencia en los recientes cambios de las políticas de los principales intermediarios de Internet que prohíben expresamente escenas de desnudos.

Durante los años 2014 y 2015, ante el debate existente en la sociedad norteamericana, los intermediarios de Internet han dado un paso más. Así diversas empresas del mundo online como ser Reddit[97], Twitter[98] o Facebook[99] han prohibido en sus términos y condiciones en forma expresa las imágenes relacionadas con actos de *revenge porn*.

Los buscadores -por ejemplo Google[100]-, también tomaron la iniciativa de reconocer en forma expresa que aceptarían reclamos de remoción de imágenes de *revenge porn*, como ya viene haciendo con otra clase de información sensible tales como firmas, tarjetas de crédito, y otros datos que pueden causar perjuicio si permanecen en la red y son usados sin permiso[101]. En el blog de Políticas Públicas de Google[102] se puede leer que, luego de reconocer que el ideal de Google es incluir todo el contenido de la web sin limitaciones en las búsquedas, el fundamento de esta remoción se centró "*en el daño que causa la difusión de éstas imágenes*".

Es más, el caso de "*revenge porn*" es uno de los pocos supuestos en los cuales los buscadores han dejado de lado su rol pasivo de intermediarios y han comenzado activamente a remover resultados[103].

Estas conclusiones son aplicables en nuestro medio. Recordamos que el considerando n. 18 del fallo de la Corte Suprema en el caso "María Belén Rodríguez v. Google"[104] reconoce la libertad de ex-

reconocimiento expreso del derecho a la privacidad–, sostuvo: "La turbación de la intimidad debería ser incriminada como delito. Sólo así es posible concebir la esperanza de que la protección legal sea efectiva".

96 *DELGADO y STEFANIC, Must We Defend Nazis?: Hate Speech, Pornography, and the New First Amendment, NYU Press, pág. 153; HEINS, Banning Words: A Comment on "Words That Wound, 18 Harv. C.R.-C.L. L. Rev. págs. 585-592 (1983) y STROSSEN, Hate Speech and Pornography: Do We Have to Choose Between Freedom of Speech and Equality?, 46 Case W. Res. 449, 458 (1996).*

97 *SNYDER, Twitter and Reddit ban 'revenge porn,' but what took so long?, http://www.cio.com/article/2896213/social-media/twitter-reddit-ban-revenge-porn-first-amendment.html*

98 *TSUKAYAMA, Twitter updates its rules to specifically ban 'revenge porn', Washington Post, 11 de marzo de 2015.*

99 *PRICE, Facebook bans revenge porn in new Community Guidelines - Business Insider, 16/3/2015.*

100 *GRANDONI, Google to Remove 'Revenge Porn' Images From Search Results, New York Times, 19 de junio de 2015.*

101 *SINGHAL, "Revenge porn" and Search, http://googlepublicpolicy.blogspot.com.ar/2015/06/revenge-porn-and-search.html, post del 19 de junio de 2015.*

102 *En el post citado en la nota anterior se dice: "Our philosophy has always been that Search should reflect the whole web. But revenge porn images are intensely personal and emotionally damaging, and serve only to degrade the victims—predominantly women. So going forward, we'll honor requests from people to remove nude or sexually explicit images shared without their consent from Google Search results. This is a narrow and limited policy, similar to how we treat removal requests for other highly sensitive personal information, such as bank account numbers and signatures, that may surface in our search results".*

103 *GIBBS, Google removes results linking to stolen photos of Jennifer Lawrence nude, en The Guardian, 20 de octubre de 2014.*

104 *Corte Suprema de Justicia de la Nación, caso "María Belen Rodriguez v. Google y otro", publicado en Revista Latinoamericana de Protección de Datos, Año I, No.1, págs. 352/384 (2015) y nuestro comentario El fallo de la Corte Suprema de Argentina en el caso Google, la creación pretoriana*

presión en Internet y la falta de responsabilidad objetiva de los buscadores, y menciona a los casos de *pornografa infantil y los de publicación de imágenes de escenas íntimas* como claros supuestos donde no es necesario esperar una orden judicial frente a un pedido de remoción de la persona afectada.

La Corte Suprema de Justicia de la Nación explicó -a manera de *obiter*- que estos casos son supuestos donde el mero análisis de la imagen permite comprender que es ilegal su publicación. Por ende se debe dar de baja en forma inmediata el contenido en cuestión sin esperar una orden judicial.

Desde una perspectiva de *lege ferenda*, también podría ser posible pensar en una excepción para supuestos de interés público como la que fue prevista por la ley 26.388 para el caso de publicación de correspondencia digital relacionada con asuntos de interés público[105]. Creo que los casos serían excepcionales pero deberían estar presentes.

La norma que se redacte debería aclarar de alguna forma algo obvio: el hecho que los intermediarios de Internet no son responsables pues actúan en forma automatizada y sin posibilidad de control previo del contenido que se sube online, cuestión que ya los jueces están aplicando correctamente en materia de denuncias penales en casos de derecho de autor[106].

También cabe la posibilidad de optar por la solución de Brasil en la Ley del Marco Civil de Internet.

El problema de la regulación brasilera es que se parte de la base que los intermediarios son responsables a menos que remuevan el contenido, cuando en realidad nunca deberían ser responsables del contenido subido por terceros.

La ley brasilera ya citada[107] les quita la inmunidad si no remueven el contenido en forma sumaria, creando así un incentivo para actuar con rapidez. Si bien nos referimos exclusivamente a la responsabilidad penal, lo cierto es que no puede ponerse en cabeza del intermediario la posible sanción penal a menos que "actúe rápidamente y remueva el contenido", pues ello plantea serios problemas interpretativos respecto al dolo propio de la figura que estudiamos.

4.4. NUESTRA PROPUESTA

Somos de la idea que la legislación penal debe amparar la imagen, a través de dos figuras distintas que ya están contempladas en el Derecho Comparado.

La primera es la captación no autorizada de la imagen mediante dispositivos tecnológicos en lugares privados y *sin consentimiento* del titular de la imagen[108].

La segunda figura debe apuntar a amparar al sujeto contra la difusión no autorizada de la imagen que originalmente se captó *con su consentimiento* pero en un lugar privado y donde el contesto daba a entender que no deben difundirse, pues son escenas íntimas y el titular se verá gravemente afectado en caso de su difusión[109].

Los elementos del delito de revelación no autorizada de imágenes intimas (*revenge porn*) son los siguientes: (i) se difunden o revelan imágenes captadas con consentimiento, (ii) son imágenes o videos íntimos, de contenido sexual o de poses, pero donde el propio contenido de la imagen da a entender que su difusión afecta gravemente la privacidad de la víctima, (iii) la difusión es sin autorización del sujeto pasivo, (iv) esa divulgación afecta gravemente su privacidad, (v) no se requiere una intención especial ni un ánimo de venganza (lo cual sería muy difícil de probar pero por otra parte está implícito en la mayoría de los casos), (vi) la existencia de lucro puede funcionar como agravante pero no debe integrar la figura básica.

Numerosos autores coinciden en que la necesidad de un video íntimo de una persona además de po-

de un procedimiento de "notice & take down" y su impacto en la protección de datos personales, en pág. 385 de la misma publicación.

105 *Para un listado de indicios para determinar cuando puede haber interés público en casos de tutela de la vida privada ver PALAZZI, Publicación de un correo electrónico con contenido de interés público: el conflicto entre privacidad y la libertad de expresión en Internet, ED 257-203 (2014).*

106 *Ver por ejemplo CNCrim., sala V, P., L., 28/10/2013, LL 2013-F-452 y LL 2014-C-63, y en similar sentido el caso que involucró a Kodama vs. Taringa, CNCrim, Sala I, 5/5/2015, DJ 30/09/2015, p.63, cita online La Ley AR/JUR/8607/2015.*

107 *Art. 21. El proveedor de aplicaciones de internet que disponibilice contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, de imágenes, videos u otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando, posterior al recibimiento de la notificación por el participante o su representante legal, dejar de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la indisponibilización de ese contenido. Parágrafo único. La notificación prevista en el artículo deberá contener, bajo pena de nulidad, elementos que permitan la identificación específica del material apuntado como violador de la intimidad del participante y la verificación de la legitimidad para presentación del pedido.*

108 *Receptada en numerosas legislaciones, por ejemplo: art. 226-1 del Código Penal Francés.*

109 *Receptada en numerosas legislaciones, por ejemplo: cerca de una veintena de estados en los Estados Unidos de Norteamérica; sección 33-35 de la Criminal Justice and Courts Act 2015 del Reino Unido; art. 56 de la ley de privacidad de Nueva Zelanda, art. 197 del Código Penal español.*

der vulnerar el derecho a la propia imagen supondría una vulneración del derecho a la intimidad de la persona si no se cuenta con consentimiento de la misma[110].

En función de todo lo expuesto proponemos agregar como art. 153 ter del Código Penal la siguiente figura: "***Será castigado con una pena de prisión de tres meses a dos años el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones de audio o audiovisuales de aquélla, que hubiera obtenido con o sin su consentimiento en un lugar privado, cuando la divulgación menoscabe gravemente la privacidad de esa persona***".

5. CONCLUSIONES

La difusión de imágenes íntimas en internet constituye una grave afectación del derecho a la privacidad.

De todas las imágenes que puedan existir de una persona, este clase de datos son los más íntimos. Lo único que desea la víctima en estos casos es lograr retirar de Internet sus fotos íntimas. El castigo del culpable suele quedar en segundo lugar frente a esta urgente necesidad de limpiar la web de sus datos y contenidos privados. Pero las cautelares suelen ser difíciles de obtener e implican involucrar a intermediarios de Internet que no tienen relación alguna con el hecho ilícito. Por otra parte, la legislación civil ya cubre adecuadamente este tipo de hechos ilícitos, no así la penal, lo cual es un vacío que debe ser remediado con la modificación de los códigos penales.

110 *CITRON y FRANKS, Criminalizing Revenge Porn, Wake Forest Law Review, Vol. 49, 2014, p. 345; LARKIN, Revenge Porn, State Law, and Free Speech, Loyola of Los Angeles Law Review, Vol. 48, 2014; LEVENDOWSKI, Using Copyright to Combat Revenge Porn, NYU Journal of Intellectual Property & Entertainment Law, Vol. 3, 2014; BAMBAUER, Exposed, 98 Minnesota Law Review 2025 (2014) Arizona Legal Studies Discussion Paper No. 13-39; VARGAS DE BREA, La regulación de la pornografía no consentida en la Argentina, Paper del CELE, Diciembre 2015; PALAZZI, Protección penal de la difusión no autorizada de la imagen íntima captada con consentimiento de su titular y el problema del "revenge porn, en Revista de Derecho Penal y Procesal Penal, No. 8, 2015, pp. 1587-1598; y TOURIÑO, obra citada, pág. 53.*

EL ROBO DE IDENTIDAD Y LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

XIMENA
PUENTE DE LA MORA

Es abogada, académica e investigadora mexicana especialista en temas de transparencia y rendición de cuentas desde hace más de 10 años. Licenciada en Derecho por la Universidad de Colima, Maestra en Ciencias Jurídicas por la Universidad de Navarra; y Doctora en Derecho por la Universidad de Guadalajara.
Fue Comisionada del Instituto de Transparencia, Acceso a la Información y Protección de Datos del Estado de Colima (INFOCOL), donde ocupó la presidencia en 2014.
Actualmente preside el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI); el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales; y la Red Iberoamericana de Protección de Datos.
Es integrante del Secretariado Tripartita de la Alianza para el Gobierno Abierto; del Comité Coordinador del Sistema Nacional Anticorrupción; y del Sistema Nacional de Investigadores del Conacyt.

SUMARIO

RESUMEN

El robo o suplantación de identidad afecta a un gran número de personas en todo el mundo, sus consecuencias son en su mayoría devastadoras y de diversa índole: económicas, jurídicas, fiscales, sociales e incluso familiares.

El robo de identidad se encuentra íntimamente ligado a la protección de datos personales, ya que es a través del acceso a la información personal que se obtienen los datos necesarios para suplantar la identidad, por lo que la labor preventiva de concientización acerca de la importancia de proteger nuestros datos personales, constituye una herramienta valiosa para combatir este tipo de conductas ilícitas.

En consecuencia las autoridades encargadas de la protección de datos personales, juegan un papel importante en lo que respecta a la labor preventiva y de concientización entre la población para proteger su información personal y de esa manera evitar la comisión de este delito.

El presente artículo advierte sobre el aumento del robo de identidad, particularmente en México; plantea algunas de las consecuencias e implicaciones que se generan con motivo del robo de identidad; su vinculación con la protección de datos personales y describe como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI, a través de diversas acciones de carácter preventivo como la publicación de la Guía para Prevenir el Robo de Identidad, así como otros mecanismos de coordinación entre autoridades, está promoviendo una estrategia integral para que a través de la concientización a la población respecto a la debida protección de sus datos personales, se evite la usurpación de identidad.

1. INTRODUCCIÓN

En la actualidad, uno de los delitos que más afectan a nuestros países es el robo o suplantación de identidad, el cual consiste en la usurpación de la identidad de una persona para hacerse pasar por ella, asumir su identidad frente a terceros, con la finalidad, en algunos casos, de obtener recursos o beneficios a su nombre.

Hoy en día, los mecanismos que son utilizados en la comisión de delitos resultan ser cada vez más sofisticados, la tecnología está siendo usada para fines delictivos por quienes cometen este tipo de ilícitos y en consecuencia el *modus operandi* resulta ser complejo, en su comisión es posible inferir que intervienen una pluralidad de personas con conocimientos multidisciplinarios, principalmente del ramo informático, cibernético, financiero o de carácter contable.

El Robo de identidad tiene una conexión importante con la privacidad y el derecho a la protección de los datos personales, ya que el mecanismo a través del cual surge la usurpación o robo de la identidad de una persona por parte de un tercero, es el acceso a su información de carácter personal, ya sea números de cuenta bancarios, domicilios, números de teléfono, registros de población, identificaciones , direcciones electrónicas, contraseñas y otros datos que se encuentran asociados a las personas y a través de los cuales es posible realizar conductas asumiendo indebidamente la identidad de otra persona.

En razón de ello, las acciones de carácter preventivo que se realicen con la finalidad de proteger nuestros datos personales, son fundamentales para impedir la comisión del delito de robo de identidad, ya que en la medida en que se impida el acceso a ellos, no será posible la realización de este tipo de conductas.

En el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, conscientes de la gravedad de este delito se ha diseñado una estrategia para combatirlo, desde su ámbito de competencia, a través de acciones que tienen como objetivo por un lado, alertar a la población y concientizarla acerca de la importancia y los mecanismos que existen para proteger debidamente sus datos personales; y por otro lado concertar mecanismos de coordinación entre autoridades con atribuciones en la materia, para sumar esfuerzos y diseñar una estrategia integral que ataque de manera frontal y desde diversas trincheras este tipo de conductas delictivas.

2. ALGUNAS CONSECUENCIAS DEL ROBO DE IDENTIDAD

El robo de identidad tiene consecuencias graves que pueden requerir de tiempo y recursos para resolverse. Algunos posibles daños son:

- La adquisición de deudas a nombre de la víctima, dañar su historial crediticio y afectar su patrimonio;
- Dañar de forma temporal o permanente su imagen pública y su reputación, lo que puede propiciar la pérdida de empleo, expulsión de círculos personales, profesionales o académicos, divorcios o separaciones y litigios entre otras.

2.1. IMPLICACIONES DEL ROBO DE IDENTIDAD POR SECTORES

a) Personas mayores[1]

Los adultos mayores son más vulnerables a ser víctimas de este delito pues su información es accesible para muchas instituciones y organizaciones.

La información personal de los adultos mayores está expuesta a varias personas ya sea asesores financieros, personal de salud y otros profesionales que dan servicios de asistencia a este grupo de personas.

Las autoridades de Estados Unidos de América, como la *Federal Trade Commission* (FTC), están recibiendo cada vez más quejas sobre el robo de identidad en este grupo de edad, relacionado con impuestos. Ahora los beneficios del gobierno van a pagarse por medio de tarjetas de débito recargables.

b) Redes sociales[2]

Internet ha revolucionado nuestra forma de comunicarnos con la gente que nos rodea y, en muchos casos, nos permite establecer nuevos vínculos profesionales o mantener contacto con personas que tienen aficiones o inquietudes comunes. Las redes sociales son un instrumento que vincula a muchas personas entre sí, ya sea entre amigos, o bien entre gente desconocida; a través de las redes las personas buscan empleo, esparcimiento o nuevas amistades e inclusive comparten sus fotos o videos. Frente a este gran número de datos personales que viajan por la red, encontramos que existen personas, que intentan acceder a ellos para comercializarlos o, en algunos casos, suplantar la identidad de las personas.

c) Adolescentes en riesgo[3]

Los adolescentes en la actualidad son ***nativos digitales*** se encuentran familiarizados con el internet y las redes sociales; y en consecuencia, se ha identificado que son más arriesgados para compartir su información personal en internet, lo que provoca que sean muchos y diversos los riesgos a los cuales se encuentran expuestos en el mundo virtual.

La forma de comunicación de este grupo se da a través de las redes sociales, por lo que se convierten en un sector vulnerable frente a los ataques cibernéticos, entre ellos el robo de identidad. La facilidad con la que puede ser creado un perfil falso en Facebook, Instagram, Twitter, y un sinfín de redes sociales es alarmante.

Diversas encuestas advierten que hoy en día va en aumento el número de adolescentes que utilizan redes sociales, la convivencia que se da en este grupo de edad, es a través de estas redes, resultando abrumadora la cantidad de interacciones que se llegan a dar a través de aplicaciones, redes sociales, videollamadas, etcétera, así lo revela el Estudio de la CEPAL denominado *"La Nueva Revolución Digital, de la Internet del Consumo a la Internet de la Producción"*[4], en el que destacan las siguientes cifras: "En un segundo, en Internet se descargan más de 1.700 aplicaciones, lo que ha llevado a que a finales de 2014, el usuario promedio contara con alrededor de 60 aplicaciones. En el mismo lapso, se realizan más de 44.000 búsquedas en Google y más de 1.700 llamadas por Skype, se envían más de 2 millones de correos electrónicos, más de 300.000 mensajes por protocolo IP a través de WhatsApp y más de 8.500 tuiteos, se efectúan más de 1.800 publicaciones en Tumblr y 50.000 en Facebook, se suben más de 1.900 fotos y se ven más de 98.000 videos en YouTube y 655 horas de video en Netflix."

Las cifras anteriores, dan cuenta de la intensa y acelerada comunicación que se da a través de

1 *Lisa SHIFFLER. (2013). Foro sobre personas mayores y robo de identidad. Comisión Federal de Comercio. Consultado el 28 de junio de 2016 en: https://www.consumidor.ftc.gov/blog/foro-sobre-personas-mayores-y-robo-de-identidad*

2 *JJ VELASCO. (2011). Robo de Identidad en redes sociales, ¿qué hacer? Hipertextual.com. Consultado el 28 de junio de 2016 en: http://hipertextual.com/archivo/2011/09/robos-de-identidad-que-hacer/*

3 *Lina ORNELAS y G. GREGORIO., Carlos Compiladores. (2011). Protección de Datos Personales en las Redes Sociales Digitales: En particular de niños y adolescentes. Memorándum de Montevideo, México IIJusticia-IFAI. Consultado el 28 de junio de 2016 en: http://inicio.ifai.org.mx/Publicaciones/ProteccionRedesSociales.pdf*

4 *Comisión Económica para América Latina, CEPAL. (2015). La Nueva Revolución Digital. De la Internet del Consumo a la Internet de la Producción. Chile, pág. 20. Consultado el 28 de junio de 2016 en: http://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-internet-consumo-la-internet-la-produccion*

la red y en consecuencia, la exposición a diversos riesgos, entre ellos el robo de identidad entre quienes comparten su información en la red.

d) Robo de identidad Infantil[5]

El robo de identidad infantil es una tendencia en aumento ya que los registros de niños representan un alto valor para los delincuentes y generalmente pasan años antes de que se descubra el robo. Cuando se roba la identidad de un menor, el ladrón la puede usar durante años hasta que se descubra el delito. El niño y los padres del menor a quien le ha sido robada la identidad, pueden ignorar este hecho, hasta el momento en que el niño crezca y presente una solicitud para una tarjeta de crédito, un empleo, para alquilar un departamento o tramitar un préstamo.

e) Robo de Identidad Médica[6]

Se presenta cuando otra persona utiliza información personal de otra para obtener servicios o bienes médicos, o para obtener una ganancia económica. El usurpador de identidad puede utilizar una identidad falsa para ir a una consulta médica. Puede obtener medicamentos bajo receta o presentar reclamos a la compañía de seguros en nombre de otra persona.

En consecuencia, si se confunde el tratamiento o diagnóstico médico de quien roba la identidad con el tratamiento o diagnóstico del titular de los datos, la salud de éste último puede correr peligro. Ante este panorama, se considera necesario confrontar experiencias, buenas prácticas y analizar qué medidas se están tomando para garantizar la seguridad en lo que refiere a los datos de salud, considerados datos personales de carácter sensible, debido a que afectan la esfera más íntima de su titular o su utilización indebida puede dar origen a discriminación o traer consigo algún riesgo grave para éste.

2.2. EL ROBO DE IDENTIDAD VA EN AUMENTO

En México, el Robo de identidad va en aumento, y es que este ilícito no sólo se presenta por el uso de redes sociales y trámites en la red, también es muy común el extravío de documentos personales, lo cual genera un alto índice de riesgo de suplantación de identidad.

Según datos del Banco de México[7] y firmas especializadas[8], nuestro país ocupa el 8° lugar en este delito en el mundo. 67% es por pérdida de documentos, 63% por robo de una cartera y portafolios y 53% es información tomada de una tarjeta bancaria.

Según el *Estudio sobre los hábitos de los usuarios de internet en México 2014* de la Asociación Mexicana de Internet (AMIPCI), 9 de cada 10 internautas acceden a una red social[9]. En ellas, dejan sus datos personales, situación que eventualmente podría permitir a los atacantes inferir contraseñas, preguntas de seguridad u otras credenciales de autenticación.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, CONDUSEF, informó que[10] durante el primer semestre de 2015, las reclamaciones imputables a un posible robo de identidad se incrementaron 40% con respecto al mismo período de 2014, al pasar de 20 mil 168 a 28 mil 258.

Cabe destacar que de cada 100 reclamaciones imputables a un fraude, 2 corresponden a posible robo de identidad.

Sobre el monto reclamado por los usuarios, en el primer semestre del año ascendió a 118 millones de pesos, 19% más a lo reclamado en el mismo período de 2014 y de este monto el saldo abonado fue de 69 millones de pesos, es decir 58%.

---

5 *Álvaro PUIG. (2012). Cómo proteger a su hijo contra el robo de identidad infantil. AlertaenLínea.gov. Consultado el 28 de junio de 2016 en: https://www.alertaenlinea.gov/blog/como-proteger-su-hijo-contra-el-robo-de-identidad-infantil*

6 *Departamento de Justicia de California. (2013). Primeros auxilios para el robo de identidad médica. Consejos para consumidores. Hoja informativa para el consumidor 16. Consultado el 28 de junio de 2016 en: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft_sp.pdf*

7 *Edgar AMIGÓN. (2015). Robo de Identidad, un delito en aumento. Revista proteja su dinero. Año 16, N°186. CONDUSEF. Consultado el 28 de junio de 2016 en: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad y http://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf*

8 *Ilse SANTA RITA. (2013). Evite llevar toda su identidad en la cartera. El Economista. Consultado el 28 de junio de 2016 en: http://eleconomista.com.mx/finanzas-personales/2013/02/07/evite-llevar-toda-su-identidad-cartera*

9 *Asociación Mexicana de Internet, AMIPCI. (2014). Estudio sobre los hábitos de los usuarios de internet en México 2014. Consultado el 28 de junio de 2016 en: https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf*

10 *Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, CONDUSEF. (2016). Aumentan 40% reclamaciones imputables a posible robo de identidad en primer semestre de 2015, Comunicado de prensa. Consultado el 28 de junio de 2016 en: http://www.condusef.gob.mx/index.php/comunicados-de-prensa/1239-aumentan-40-reclamaciones-imputables-a-posible-robo-de-identidad-en-primer-semestre-de-2015*

3. EL ROBO DE IDENTIDAD Y SU VÍNCULO CON LA PROTECCIÓN DE DATOS PERSONALES

Para la suplantación o robo de identidad una persona obtiene, transfiere, utiliza o se apropia de manera indebida de los datos personales de otra, usualmente para cometer un fraude o delito. En ese sentido, *el robo de identidad implica la obtención y uso no autorizado e ilegal de datos personales,* por lo que, sin duda, es un fenómeno de interés del INAI, principalmente desde el punto de vista preventivo, para evitarlo.

Adicionalmente, el robo de identidad puede estar vinculado a una vulneración a las bases de datos personales de organizaciones privadas o públicas, quienes, en cumplimiento a la legislación que les aplique deben prever medidas de seguridad para la protección de los datos personales, y evitar su robo y uso no autorizado.

Por otra parte, de acuerdo con el *principio de calidad*, el cual establece, entre otros aspectos, la obligación del responsable para prever mecanismos para que los datos personales que posee sean correctos y estén actualizados. Aunque se presume que los datos personales que posee una organización pública o privada son correctos cuando los proporciona directamente el titular de los mismos, estas organizaciones están obligadas a tomar las medidas necesarias para procurar que los datos personales que traten sean correctos. Esta obligación en algunos casos está directamente relacionada con el robo de identidad, pues el responsable, al obtener los datos personales, tendría que llevar a cabo ciertas medidas de comprobación, para procurar que los datos personales que está obteniendo sean reales y pertenecen a la persona que los proporciona.

Por ello, el INAI publicó a inicios del presente año, la *Guía para Prevenir el Robo de Identidad*, disponible en la página del INAI http://inicio.inai.org.mx/DocumentosdeInteres/Guía_Prevenir_RI.pdf cuyo objeto es proporcionar información relevante con relación al robo de identidad, con la finalidad de que las personas cuenten con herramientas para conocer cómo proteger sus datos personales y así reducir el riesgo de que su identidad sea robada. De igual forma, se incluyen referencias para saber qué hacer y ante quién acudir en caso de haber sido víctimas de robo de identidad.

4. GUÍA PARA PREVENIR EL ROBO DE IDENTIDAD PUBLICADA POR EL INAI

La ***Guía para Prevenir el Robo de Identidad***, publicada por el INAI en su sitio de Internet, brinda a los titulares de los datos personales recomendaciones para proteger sus datos personales y evitar que sean víctimas del robo de identidad. Estas recomendaciones varían dependiendo del contexto y si se trata del mundo físico o del Internet. La Guía contiene, entre otras cosas, 10 consejos útiles para proteger la información de las personas:

1) Mantener seguros los documentos personales en casa y cuando haya un viaje;
2) Destruir los documentos personales cuando hayan dejado de ser necesarios;
3) Pensar antes de publicar o compartir información personal. No enviar claves, ni contraseñas por correo electrónico, ni compartirlos;
4) Proteger nuestra computadora, teléfono inteligente o tableta con un programa de seguridad (antivirus) y contraseñas seguras;
5) Limitar el número de documentos personales que traemos con nosotros;
6) Tener cuidado cuando nos soliciten información en persona, por internet o teléfono. Hay que verificar la identidad de quien la solicita;
7) Investigar si recibimos tarjetas de crédito, servicios o artículos que no hayamos solicitado, y estar pendiente de la correspondencia que nos haga falta;
8) Mantenernos alertas ante cualquier transacción bancaria inusual;

9) Tener siempre a la vista nuestras tarjetas de crédito o débito (solicitar que nos traigan la terminal), y

10) Realizar transacciones seguras, en computadoras que no sean públicas y asegurándonos que el sitio de Internet al que ingresamos es seguro.

La ***Guía para Prevenir el Robo de Identidad*** también proporciona a las víctimas del robo de identidad, algunas acciones para enfrentar ese delito. Es importante considerar que entre más rápido actúa la víctima, se podrá disminuir en mayor medida el daño causado. El plan de acción que presenta es el siguiente:

- ACCIÓN 1. Presentar denuncia ante las autoridades penales correspondientes (Procuradurías de los Estados y los ministerios públicos). Si no existe el delito en el Estado, puede haber delitos similares como usurpación o suplantación de la identidad o robo;
- ACCIÓN 2. Reportar la pérdida de los documentos a quien corresponda;
- ACCIÓN 3. Contactar y reportar a la institución financiera las afectaciones en tus cuentas o de cuentas que hayan sido abiertas a tu nombre, sin tu consentimiento. De igual forma, podemos acudir a la CONDUSEF, para presentar una queja en caso de que tengamos algún inconveniente en el trámite con la institución financiera que corresponda;
- ACCIÓN 4. Cancelar cuentas o servicios no autorizados que se hayan contratado en nuestro nombre. Si tenemos problemas con relación a la cancelación de nuestros servicios, podemos acudir a la Profeco;
- ACCIÓN 5. Solicitar una copia de nuestro reporte de crédito;
- ACCIÓN 6. Reportar a las redes sociales las vulneraciones que hayan sido identificadas en nuestras cuentas, y
- ACCIÓN 7. Contactar al INAI por el mal uso de tus datos personales. Cabe señalar que el INAI no investiga de manera directa el robo de identidad, pues la investigación y persecución de este delito corresponde a las autoridades de carácter penal. Sin embargo, el INAI puede investigar el indebido tratamiento de datos personales vinculado con el robo de identidad.

El alarmante aumento de la comisión del delito de robo de identidad a nivel nacional e internacional, demanda la creación de un frente común entre los sectores público y privado; particularmente por parte de quienes nos encontramos frente a la responsabilidad de velar por el cumplimiento de la legislación en materia de protección de datos personales.

Demanda también el involucramiento de los padres de familia para crear conciencia entre niños y jóvenes respecto al hecho de que, si bien el uso de la tecnología puede ser un gran aliado, conlleva también riesgos importantes como la suplantación de la identidad.

Pero sobre todo, demanda ser conscientes de que garantizar la privacidad en la era digital en la que vivimos, requiere contar con una nueva cultura de autoprotección de nuestros datos personales en Internet.

5. ESTRATEGIA DE COLABORACIÓN INSTITUCIONAL PARA HACER UN FRENTE COMÚN CONTRA EL ROBO DE IDENTIDAD

A principios de este año, el INAI y seis instituciones del sector financiero, bancario, hacendario, electoral y de procuración de justicia, suscribieron las *Bases de Colaboración en materia de Suplantación o Usurpación de Identidad*[11], considerando que la población en general requiere de información eficiente que le ayude a evitar la suplantación o usurpación de su identidad y, en específico, los usuarios de los servicios financieros afectados por la suplantación o usurpación de identidad, deben contar con la orientación oportuna y acción eficaz por parte de las diversas instancias relacionadas directa o indirectamente con la protección de sus intereses, para lo cual se consideró indispensable unir esfuerzos y coordinar acciones dentro del

11 *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI. (2016). INAI y seis instituciones forman frente común para combatir suplantación o usurpación de identidad. Comunicado de prensa INAI/040/16. Consultado el 28 de junio de 2016 disponible en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-040-16.pdf*

ámbito de las respectivas competencias de cada una de las instituciones involucradas.

Asimismo, la suscripción de las Bases se da en el contexto de la creciente importancia del robo de identidad a nivel nacional, que demanda la creación de un frente común entre los entes públicos y privados quienes, debido a sus respectivos ámbitos de competencia, se encuentran relacionados con el manejo, protección del patrimonio y salvaguarda de los datos personales de las y los mexicanos.

El objeto de las Bases es definir el marco de colaboración y coordinación entre las instituciones que las suscriben, así como realizar diversas acciones a fin de inhibir la utilización del sistema financiero mexicano para la constitución de hechos ilícitos de suplantación o usurpación de identidad, en el ámbito de su competencia y de conformidad con las disposiciones legales aplicables.

Asimismo, se prevén en dichas bases la realización de acciones comunes y de carácter específico por cada institución que suscribió las Bases; entre las primeras se acordó difundir entre el público en general las medidas preventivas y correctivas para evitar ser víctimas de la suplantación o usurpación de identidad, mediante la distribución del material por parte de las instituciones participantes.

De igual forma, se acordó orientar a las personas que se encuentren ante una presunta suplantación o usurpación de identidad, para que inicien el procedimiento correspondiente ante la institución competente, estableciéndose la comunicación entre autoridades cuando existieran impactos fiscales derivados de la comisión del ilícito.

Sin duda, la suma de esfuerzos y la comunicación entre las diversas autoridades involucradas en el tema del robo o suplantación de identidad, permitirá un ataque frontal para frenar la comisión de este tipo de acciones, desde diversos frentes, entre ellos el competente para garantizar la protección de datos personales.

REFERENCIAS BIBLIOGRÁFICAS

Amigón, Edgar. (2015). Robo de Identidad, un delito en aumento.

Revista proteja su dinero. Año 16, N°186. CONDUSEF. Consultado el 28 de junio de 2016 en: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad y

http://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf

Asociación Mexicana de Internet, AMIPCI. (2014). Estudio sobre los

hábitos de los usuarios de internet en México 2014. Consultado el 28 de junio de 2016 en:

https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf

Comisión Económica para América Latina, CEPAL. (2015). La Nueva Revolución Digital. De la Internet del Consumo a la Internet de la Producción. Chile. Consultado el 28 de junio de 2016 en:

http://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-internet-consumo-la-internet-la-produccion

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, CONDUSEF. (2016). Aumentan 40% reclamaciones imputables a posible robo de identidad en primer semestre de 2015. Comunicado de prensa. Consultado el 28 de junio de 2016 en:

http://www.condusef.gob.mx/index.php/comunicados-de-prensa/1239-aumentan-40-reclamaciones-imputables-a-posible-robo-de-identidad-en-primer-semestre-de-2015

Departamento de Justicia de California. (2013). Primeros auxilios para el

robo de identidad médica. Consejos para consumidores. Hoja informativa para el consumidor 16. Consultado el 28 de junio de 2016 en:

https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft_sp.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI. (2016). INAI y seis instituciones forman frente común para combatir suplantación o usurpación de identidad. Comunicado de prensa INAI/040/16. Consultado el 28 de junio de 2016 disponible en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-040-16.pdf

------ (2016) Guía para Prevenir el Robo de Identidad. Consultada el 28 de junio

de 2016 disponible en:

http://inicio.inai.org.mx/DocumentosdeInteres/Guía_Prevenir_RI.pdf

Ornelas, Lina y Gregorio G., Carlos Compiladores. (2011). Protección de Datos Personales en las Redes Sociales Digitales: En particular de niños y adolescentes. Memorándum de Montevideo, México IIJusticia-IFAI. Consultado el 28 de junio de 2016 de:

http://inicio.ifai.org.mx/Publicaciones/ProteccionRedesSociales.pdf

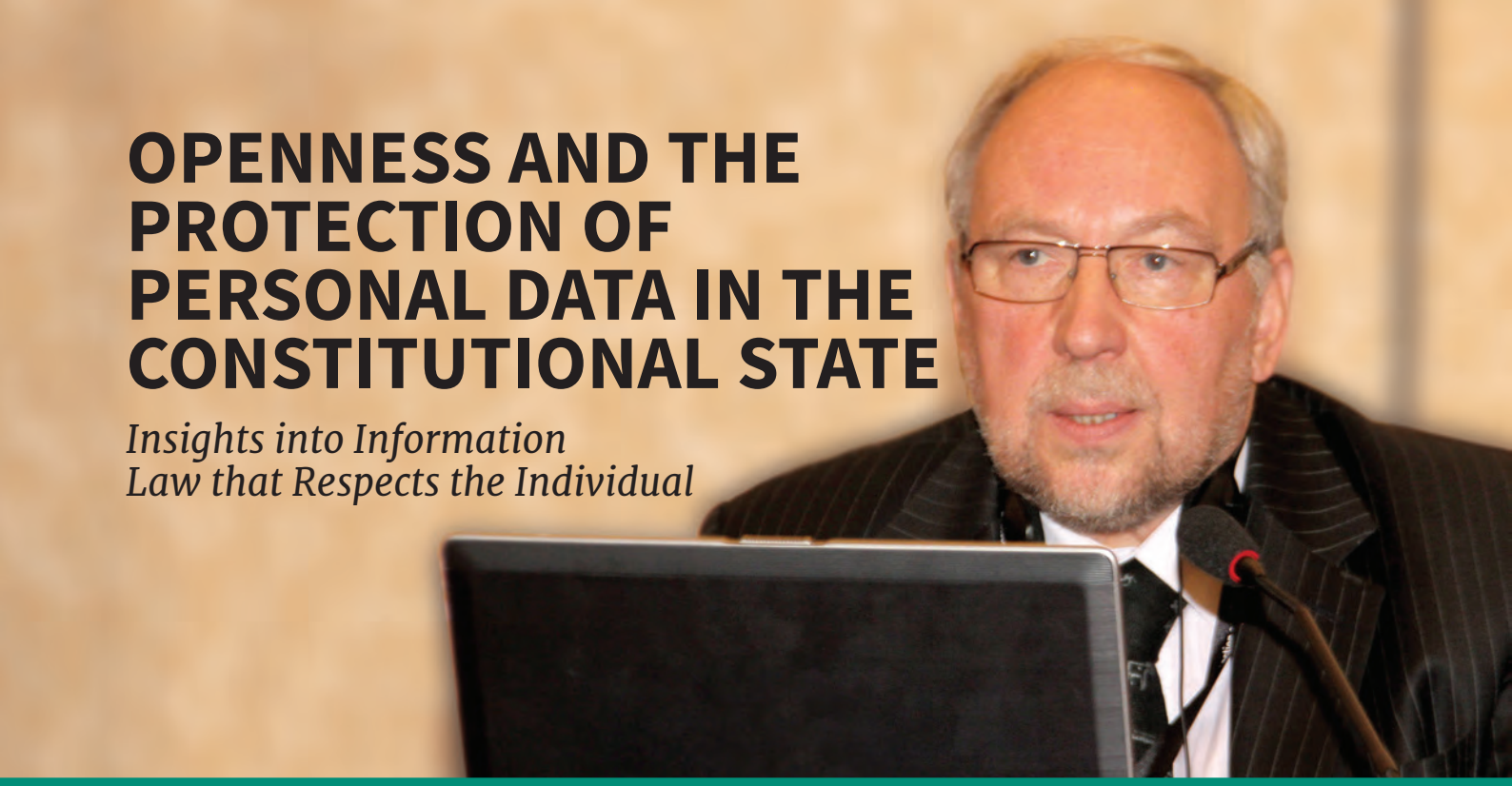
Puig, Álvaro. (2012). Cómo proteger a su hijo contra el robo de Identidad infantil. Alertaen-Línea.gov. Consultado el 28 de junio de 2016 en: https://www.alertaenlinea.gov/blog/como-proteger-su-hijo-contra-el-robo-de-identidad-infantil

Santa Rita, Ilse. (2013). Evite llevar toda su identidad en la cartera. El Economista. Consultado el 28 de junio de 2016 en:

http://eleconomista.com.mx/finanzas-personales/2013/02/07/evite-llevar-toda-su-identidad-cartera

Shiffler, Lisa. (2013). Foro sobre personas mayores y robo de identidad. Comisión Federal de Comercio. Consultado el 28 de junio de 2016 de https://www.consumidor.ftc.gov/blog/foro-sobre-personas-mayores-y-robo-de-identidad

Velasco, JJ. (2011). Robo de Identidad en redes sociales, ¿qué hacer? Hipertextual.com. Consultado el 28 de junio de 2016 en: http://hipertextual.com/archivo/2011/09/robos-de-identidad-que-hacer/



OPENNESS AND THE PROTECTION OF PERSONAL DATA IN THE CONSTITUTIONAL STATE

Insights into Information Law that Respects the Individual

AHTI
SAARENPÄÄ

Es Profesor Emérito de Derecho Privado en la Universidad de Lapland. Fue Director del Instituto para Informática Legal en la Facultad de Derecho por muchos años. Sus responsabilidades a nivel nacional incluyen la Jefatura Delegada de la Junta Finlandesa de Protección de Datos y actividades con la Junta Disciplinaria de la Asociación de Abogados Finlandesa. El Profesor Saarenpää también ha sido miembro de la Junta Legal Consultiva de la Unión Europea.

SUMARIO

RESUMEN

Este año marca un hito en el principio Nórdico de apertura: hace 250 años Finlandia, en ese momento parte de Suecia, sancionó una Ley -el Acta de Libertad de Prensa- que puede describirse como un Acta de Apertura. Hoy en día hablamos de apertura de actividades gubernamentales. En esencia, esto significa acceso a documentos públicos – acceso para ciudadanos y acceso para los medios.

También tenemos una razón para celebrar en lo que refiere a la protección de datos personales. El nuevo Reglamento General Europeo en Protección de Datos puede en forma justificada ser descrito como una legislación para y por la Sociedad en Red y el estado constitucional.

La conmemoración de estos dos hitos sin duda pondrá nuevamente en el foco de atención las tensiones entre las estrechas perspectivas que pueden encontrarse en la informática jurídica cuando trata con la planificación de sistemas de datos. Cuando se pone énfasis en alguno de los principios -apertura o protección de datos personales- muy fácilmente se deja de lado el otro, y se falla en considerar adecuadamente las conexiones entre ambos. La especialización fácilmente limita el conocimiento técnico

Lo que necesitamos aquí son doctrinas generales en Derecho de la Información. Son estas las que nos dirán, como bien sabemos, que es lo correcto en una situación determinada. La elaboración de tales doctrinas ha sido muy lenta en algunos países. Aún así, a este esfuerzo se le ha otorgado una nueva y esencial urgencia, ya que salvaguardará nuestro derecho a saber mientras que respeta los derechos de los otros y asegura el adecuado funcionamiento de la sociedad.

ABSTRACT

This year marks a milestone in the Nordic principle of openness: it was 250 years ago that Finland, part of Sweden at the time, enacted a law – the Freedom of the Press Act - that could be described as an Openness Act. Today we speak about the openness of government activities. In essence, this means access to public documents - access for citizens, and access for the media.

We also have cause for celebration where protection of personal data is concerned. The new European **General Data Protection Regulation** can justifiably be described as legislation of and for the Network Society and the constitutional state.

Celebrating these two milestones will undoubtedly once again bring to the fore the tensions between the narrow perspectives to be found in Legal Informatics when it comes to planning data systems. When we emphasize either of the principles – openness or personal data protection - we easily slight the other, and fail to adequately consider the connections between the two. Specialization easily narrows expertise.

What we need here are general doctrines of Information Law. It is these that will tell us, as we well know, what can be right in a given situation. The elaboration of such doctrines has been very slow in different countries. Yet, this effort is now being given a new, essential urgency, for it will safeguard our right to know while respecting the rights of others and ensuring the smooth functioning of society.

1. THE RIGHT TO KNOW

One of the core elements of an individual's right of self-determination under the rule of law is the right to know. We may consider this a meta-level fundamental right based on the underpinnings of human rights in modern democracy. The right to know is both a necessary precondition for the realization of our other rights and a right in and of itself in the relationship between an individual and society.

The right to know can and should be realized in many different forms. These range from access to official digital documents and databases to the

maintenance of public libraries and various applications of the principles of open data.[1]

Efforts to realize our right to know in the relationship between the individual and government have, however, included mostly guarantees of access to public documents and access to official meetings of importance. In keeping with the Nordic tradition, government documents have, for the most part, long been made available to the public, and it has been possible to follow the decisions made in Parliament and the courts. Today, access to public documents is a fundamental right enshrined in, among other instruments, the EU Charter of Fundamental Rights (Articles 41 and 42). Far-reaching exceptions to this right are hardly thinkable any longer as we strive to realize the ideal of the democratic constitutional state, where law should be simple.

This is all well and good, but in the Network Society and its information government we find ourselves rather far removed from traditional documents and traditional forms of access.[2] To be sure, we still produce paper documents and generation upon generation of lawyers remains well-schooled in how to work with them. But in the Network Society we work primarily on networks in a digital environment and no longer necessarily produce paper documents unless specifically requested to do so. And even when they are created, they represent but a small – albeit extremely important – step on the long and involved path that information travels today.[3]

As such, these observations are not totally novel. Some time ago, when we entered the era of e-government, we began paying greater attention to the process by which documents are created, and the electronic files in which individual documents were stored took on legal importance. Today, however, we must adopt a significantly broader perspective where information management is concerned. Our right to information, if it is to be properly realized, requires adequate knowledge of information systems and their functionality as well as of document design and document logistics. These are considerations that merit scrutiny - not only technically for their robustness, but also legally for how they affect human and fundamental rights. Interoperability in our digital environment must be achieved in both the technology and the law.

2. TRADITIONAL OPENNESS

We often view an open society as the democratic alternative to a closed, totalitarian one. There is no reason to dismiss this basic distinction between the extremes, which is rooted in principle and practice. Openness is an integral element of democracy, whether we are talking about Karl Popper's (1902-1994) well-known conceptual distinction or the Lisbon Treaty.

The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community emphasizes openness as one of the bases on which the Union works. Article 1 of the Treaty states: "This Treaty marks a new stage in the process of creating an ever closer union among the peoples of Europe, in which decisions are taken as openly as possible and as closely as possible to the citizen." This is very well put.

As a legal term, openness has often been, and still is, seen primarily as meaning access to public documents. Consistent with the general Nordic principle of openness, government in Finland, for example, is guided by the Act on Openness in Government Activities. The Act, which focuses on access to public documents, is commonly referred to as the "Openness Act".

The choice of name can be explained by the Act having come into force in 1999, when Finland was President of the EU. It was inspired by the policy on openness which the country promoted in connection with this role. We were trying to do our part to achieve more extensive openness in government throughout Europe. Government had been a good deal more closed in many other member states of the Union. In Finnish perspective, there were many places where the process of openness - in the sense of providing access to public documents - was still in its infancy.

The principle of openness has a far longer history in the Nordic countries. The first steps towards openness can be traced back to the eighteenth century in what was then Sweden-Finland.

1 *See also Girardi - Palmirani Open Government Data: Legal Economical and Semantic Web Aspects pp 187-205 in Saarenpää – Sztobryn Lawyers in the Media society (2016).*

2 *On the Network Society, which represents the next step forward from the Information Society, see for example Saarenpää Data Protection in the Network Society – the exceptional becomes the natural, pp 85-128 in Galindo ed El derecho de la sociedad en red (2013).*

3 *A good example of paperlessness is the Finnish capital Helsinki, whose administration and decision making operate in a totally digital environment where all documents are also archived in digital form, with permission of The National Archives Service of Finland.*

A freedom of the press law introduced at that time – albeit an ultimately short-lived one – was the handiwork of a Finnish representative in Parliament. We can thus justifiably claim that openness was originally a Finnish idea, not an exclusively Swedish one. This is the historical reality.[4]

Openness is also a fundamental right enshrined in the Finnish Constitution, which reads in relevant part: "Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings." This idea is deeply rooted in the minds of most of those working in government, and the media readily appeal to it.

When we work with traditional documents, it is, as it always has been, easy to adhere to the traditional distinction – dichotomy in fact – between public and confidential material. Documents are one or the other. Before privacy and the protection of personal data became the crucial rights of the individual that they are today, little head-scratching was needed before responding to a request for documents. Openness also brought quite a few private matters into the public realm. Often, where details in a document had to be kept confidential, the solution was to cross out the sensitive parts.

An illustrative example of the impacts that easy access to public documents can have on society is the Swedish Credit Reference Act. Sweden can claim the honour of being the first country to have passed a general data protection act, the datalag. The law was enacted in 1973 and came into effect in its full scope in 1974. At the same time, the country began drafting the Credit Reference Act, which also came into force in 1974, but is often – unfortunately – overlooked in the history of data protection legislation. As in the case of the datalag, the drafting work on the Credit Reference Act described how the increasing use of information technology posed threats to people's privacy. In addition, it drew attention to the fact that the Swedish legislation on openness made possible the extensive collection and use of data pertaining to individuals. Gathering public information from different sources around the country and freedom of expression provided an opportunity to assess a person's creditworthiness.[5]

When the age of e-government came during the 1980s and 1990s, it was initially easy to continue with the old document-based openness. Computers were seen as tools used for producing different kind of documents. However, legislators had to think about issues of openness where computer files were concerned. The focal question was: What was the relation between the files inside and documents outside? In Finland, this thinking resulted in the following formulation of the concept of a document in the Openness Act:

A written or visual presentation, and also as a message relating to a given topic or subject-matter and consisting of signs which, by virtue of the use to which they are put, are meant to be taken as a whole, but are decipherable only by means of a computer, an audio or video recorder or some other technical device.

This definition is still quite good. It in fact embodies the very important concept of logical document, which is familiar to us in the field of data protection. In data systems there cannot be any acceptable data protection unless we implement the idea of logical documents.

However, if we confine our focus to digital and logical documents, our perspective on openness and data protection will remain far too narrow. In the new constitutional Network Society we must speak about transparency as well.

3. TRANSPARENCY

Transparency is the second important concept we must consider here after openness. When we say that an open society should be transparent, we mean quite a bit more than ensuring public access to official documents.

The requirements of transparency apply to various procedures in public action, the relationship between the public and private sectors and, in some respects, the operation of the marketplace and so-called third sector. In a word, we have a right to know what is going on. This is why transparency is one of the pillars of modern democracy.

Transparency is referred to in general as something that complements openness, and in particular as a crucial means for combating corruption. Indeed, we can undoubtedly say that in international usage the term has become synonymous with the prevention of corruption. Where there is extensive transparency, this leaves less room for corruption in its different forms. Not surprisingly,

4 *The principal advocate of the statute, the father of the legislation, was the Finnish priest Anders Chydenius (1729-1703), a Member of Parliament in his day. See more in http://www.chydenius.net/eng/index.asp*

5 *In fact, in most countries the compilation and sale of credit information has been based on the on the freedom of speech and the availability of documents describing people's financial situation.*

then, the name of the international anti-corruption watchdog agency is Transparency International.[6]

Here, I use the term in a more neutral sense, one embracing the range of efforts to increase openness in society. These necessarily include the importance of information and how it is processed in different activities. As Professor Silvia Kirkegaard has astutely put it: "The best advice that any government can be given today is to ensure that transparency is firmly embedded into its processes."[7]

In fact, one now hears talk of an open society having an information policy. There is every reason to pursue this line of thinking. From the legal point of view it is important to see that openness and transparency are closely connected. We no longer speak primarily or exclusively of access to public documents but more broadly of the openness of data processing in society. This openness is a foundational component of modern information government in the emergent constitutional state - government based on the use of information systems and information networks.

The importance of openness urges us to take a closer look at the procedures by which data are processed in government and the environments in which this takes place.

4. INFORMATION GOVERNMENT

We have become used to speaking of electronic government, e-government. This has been a visible, welcome development in the modernization of research on government.[8] It marks a significant break with the earlier, text-orientated research tradition.

Historically, e-government is a reasonably new term. But, as I have noted in a number of articles, it is nevertheless passé – it refers to a style of government and a form of state that no longer exist - or should not. Today we have moved on – or we are or should be doing so – to information government.

This transition is a huge step forward from e-government. Six main developments can be cited which characterize and distinguish this crucial conceptual change.[9]

First, the use of computers is a natural, everyday aspect of government today. Government operates in an environment defined by information systems and information networks. The era when computers were no more than tools is over - and so is, and should be, the tool mentality.

Secondly, the age of the Information Society is over as well. Today, in the modern Network Society, we are critically reliant on information networks and their use in government and elsewhere. Use takes diverse forms, from the creation of documents to communication, and from initiating matters electronically to using the wide variety of electronic accounts – in fact secure channels - that individuals and organizations set up.

The third central change – an utterly fundamental one – is the development of the modern constitutional state. Throughout the world, countries have entered, or are at least starting to, the era of the constitutional state. It is a state which places far more weight on human and fundamental rights – the rights of the individual - than its predecessors did and makes those rights essential elements in all systems planning at the governmental level. The deep structure of law has become more important than earlier.

Fourthly, the status of information in society is very different from what it was earlier. Today, views stressing the increased importance of information have their basis in an interest in our right to know and the right to knowledge this entails. The new constitutional state has a significant informational dimension. What we are witnessing is a new step forward in the long history that has seen the development of speech to writing and writing to documents.

The fifth development that merits mention is the transition underway to a digital working environment across the board - citizens, organizations and the public sector. This change makes it possible to design interoperable systems in which the path information takes can be optimized in technical as well as legal terms with a view to respecting the rights of the individual. Our basic documents are digital documents. Paper documents are more and more the exception.

The sixth and last critical change is connected to information security. We are taking it more seri-

6 *See also www.transparency.org*

7 *KIRKEGAARD Open access to public documents – More secrecy, less transparency! Computer Law & Security Review 2009 p. 26.*

8 *See for example NAHABETIÁN BRUNET , Laura Gobierno electrónico y gobernanza electrónica, passim (2010)*

9 *See also SAARENPÄÄ Information Government pp XX in Reyes Olmedo, Patricia (ed) (2016)*

ously than before – and we must. We have to sit up and take notice of the fact that information security is a central condition for the realization of our fundamental rights both in general and in government. The lack of acceptable information security is nowadays one of the most serious informational problems in the world.

In the era of information government that we have now entered, government must show due regard for the rights of individuals and organizations when it processes their information on the long path that information travels in the Network Society.[10]

In legal perspective, that path begins early on, when we have to decide, with a view to further use, how data is attached to a template and what kind of template this is.[11] The information then continues its journey - with due consideration given to transparency - to be processed in a secure environment of interoperable software applications until it is it is archived, or erased if no longer needed.

In the modern constitutional state, law must be taken into account earlier and earlier in all processes. It is important but no longer enough to point to the fair trial as the main pillar of a state governed by the rule of law. In the digital environment we must take citizens' rights into account much, much earlier in everything we plan.[12] Data protection legislation is a good example of this. We can say that privacy by design must be one of the trademarks of the constitutional state in the Network Society.

At the end of the day, good government is not merely a matter of procedure, of how things are done. It is also, and above all, well-designed, sound data processing in high-calibre digital operating environments. In that process of design and in those environments, the legal perspective is the starting-point for everything. We can and should speak of the legal planning of information systems.

5. LEGAL PLANNING

As I see it, the legal planning of information systems is a process that centres on various rights and their realization and takes into account, in its entirety, the long path information must travel in society today. The focus on rights figures crucially early on, when a decision is made on what template to use and how data will be attached to it. Yes, even this phase of planning requires legal expertise. The planning process then continues to anticipate the different situations in which the information systems will be used, and extends to the point where information is archived or expunged. In fact, in planning that covers the entire lifespan of information, there are few, if any, phases that do not require legal expertise.[13]

Where legal planning is lacking, we may encounter rather odd and revealing situations, ones that expose baffling attitudes on the part of officials.

I will illustrate this through two rather regrettable examples from Finland. The first involves document management in the Finnish police force and the second the work of the highest-ranking body of experts dealing with patient injuries, the Patient Injuries Board.

The Parliamentary Ombudsman had to issue a reprimand to the police administration where, after the pre-trial investigation in a criminal case had ended, the police sent each of the parties involved a document that included the personal identification codes of all the other parties. The codes were in the same document and the police administration justified its procedure by saying that it was not good document management to strike out personal data in documents. Presumably, a paper document should look "pretty". In other words, for the police administration, good document management was more important than people's fundamental rights. Terrible!

The second example illustrates a technically outdated procedure and the dubious approval it enjoys under the law. It involves a case where the Patient Injuries Board – a public expert body - refused to supply decisions made in its plenary sessions to a law firm that had requested them. One reason was that the text of the decisions contained personal data. The structure of the document had not been planned with transparency in mind. Here, crossing out sensitive data – and that

10 *Here I am not talking about digitalization. It, too, has become a common term throughout Europe but is used largely to political ends; it seems to me that it refers primarily to a rather late awakening to the societal changes and needs for change occasioned by the increased use of IT.*

11 *See more for example Palmirani Legislative XML: principles and technical tools pp 31-35*

12 *In the 1980s and even in the 1990s, the notion held sway that government authorities enjoyed free discretion. Countering this was the citizen's right to appeal their decisions.*

13 *See also SAARENPÄÄ, Legal welfare and legal planning in the network society, in J. LUIZ BARZALLO, J. TELLEZ VALDES, P. REYES OLMEDO, Y. AMOROSO FERNANDEZ (ed.), XVI Congreso Iberoamericano de Derecho e Informatica,(2012) p. 57*

is what medical records are – would have made the document very difficult to read. Accordingly, the Supreme Administrative Court concluded that the information did not have to be given to the law firms. An additional ground for the ruling was that members of the Board often discuss the decisions in medical publications and seminars, meaning that the information is published, at least to some extent.

In terms of legal informatics and document logistics, this ruling is nothing short of unbelievable. It was possible to ignore our right to know due to a lack of legal document planning.[14]

These Finnish cases reveal not only the attitudes at work but also the basic problems associated with static documents. A paper document is basically static, the same no matter where and how it is used. It can be altered by crossing out information or preparing extracts. However, alteration of a document has been regarded as an exception to the main rule, an act requiring extensive justification – and preferably backed up by a provision in the law.

Digital document systems and electronic document management provide an opportunity to produce dynamic documents. Being digital is in fact one of the fundamental technical characteristics of such systems. Documents can be planned for different purposes and with different content while retaining - using metadata - information on the original document and the different forms in which it has been distributed.[15] For this to succeed, we need more than merely the requisite technical and legal planning of the information and communications system involved. The path information travels, like openness and legal welfare in society, should be legally invulnerable. Then and only then can transparency be appropriately realized and realized to its full extent.

And, as I have noted above, what we are considering here is not only the planning of individual documents but the legal planning of entire systems. When examining the path that information must travel in the Network Society, it is helpful to distinguish at least five basic considerations: content, access, delivery, usability, and information security.[16] The right information must be in the right form at the right time and available in the right manner to those who have a right to use it.

These aims are, in principle, straightforward and, indeed, essential in a democratic constitutional state. But in practice they are sometimes difficult to implement, above all because legal planning is sketchy, planning is downright lacking and even the required know-how is not there. Adding to the problem is that IT planning has generally been specific to each branch of administration. Planning has often been entrusted to experts whose expertise is narrow in scope.

It would be misleading - wrong in fact - to claim that these issues have not been given any attention. In fact, Legal Informatics can boast a long history of addressing them. We cannot forget the work that was done in German Legal Informatics as early as in the 1970s or the Nordic research of the 1980s. Yet these all predate the Network Society and today's constitutional state. Needless to say, the efforts mounted in the 2000s to achieve more interoperability in the administrative services in Europe also merit our attention. Effective interoperability of the administrative apparatuses in different countries is essential in the long run in a community such as the EU. The EIF and EIS programmes have already shown that interoperability can at least partly be successfully promoted through recommendations.[17]

In Finland, the approach taken to improving interoperability thus far has been legislation – the Act on Information Management Governance in Public Administration, which came into force in 2011 and whose particular objective is to promote interoperability and systems architectures as a whole. The impetus for the Act was straightforward: the extensive incompatibility of software applications and the use of data systems in the public sector that resulted from old fashioned, e-government thinking. This has been particularly visible and harmful in social welfare and public health care. In that sector, the far-reaching autonomy of Finnish municipalities resulted in the deployment of a wide variety of different information systems and software solutions.[18] What had been observed and taken to heart early on in telecommunications – of necessity – had long been

14 *The Patient Injuries Board has since changed its practice. Documents are now planned with due consideration for the need to disclose the information in them.*

15 *An illustrative example of this is the provision in the Finnish Personal Data Protection Act prescribing that hard copies, that is, documents which are not original documents as such, may not show personal identification codes unless the nature of the matter involved makes it absolutely essential.*

16 *See also SAARENPÄÄ E-justice and the Network Society. Some comments from the Finnish point of view in Cerbena (ed) Brazilian and European perspectives on e-Justice (2016)*

17 *EIF was* **European Interoperability Framework** *and ISA is* **Interoperability** *Solutions for European Public Administrations. ISA2, a wide-ranging initiative, began in 2016. One component of the project focuses on making use of fingerprints in government. In practice, the use of fingerprints often means the use of automated decision making.*

18 *However, the law itself has an unfortunate cosmetic defect: it defines information management as a support activity only. And, as I have often told my students, the law was enacted about 30 years too late.*

neglected in data processing in both technical and legal terms in public administration.

What I mean here by "legal" is planning that proceeds from human and fundamental rights and encompasses the entire path information travels, beginning with the acquisition of an information system and the attachment of data to a template. Such planning anticipates and defines all of the situations in which data will be processed and sees to it that this processing is implemented as automatically as possible. Automatic data processing in which the accuracy of documents always has to be judged manually is a contradiction in terms - an oddity - in efforts to improve administration.

I will now go on to examine the issues as they bear on the protection of personal data. The reason for doing so is straightforward: a great deal of government involves the processing of personal data. A significant proportion of the information systems used in government contain personal data. Moreover, the new European **General Data Protection Regulation** introduces some rather novel views on the part of the legislator that merit our attention.

6. DATA PROTECTION AND INFORMATION GOVERNMENT

In April 2016, we entered a new era in the protection of personal data in Europe. The General Data Protection Regulation that came into force then will guide all planning of how personal data are used throughout the EU; the instrument will become fully applicable in May 2018.[19]

The Regulation, 99 articles in length, is strikingly more extensive as a text than any of its predecessors. The number and content of the recitals have also increased markedly. While the instrument has brought a great deal more to read, there is comparatively little wholly new regulation. Most significantly, the central principles of the present Data Protection Directive have been retained (Article 5) as they stand.[20] They are worth citing here:

(a) lawfulness, fairness and transparency

(b) purpose limitation

(c) data minimisation

(d) accuracy

(e) storage limitation

(f) integrity and confidentiality

For present purposes, there are two considerations we should examine in detail: data protection by design and the relationship between data protection and openness. How and where do we see these addressed in the new Regulation?

Privacy by design and data protection by design are anything but new concerns. The Regulation embraces data protection by design as a basic concept, because its overarching purpose is to protect our personal data, not our privacy. In the EU privacy and data protection are different fundamental rights. We do not even find privacy mentioned in the Regulation. Every single time we process personal data we must follow the rules and principles in the Regulation. There is no reason to think about how private the circumstances are.

Privacy by design is a notion promoted by Dr Ann Cavoukian the well-known Canadian privacy commissioner.[21] Without doubt it is a good, illuminating concept. But the idea is not a new one. It is easy to see that data protection legislation in the Nordic countries has followed this idea from the very outset. And the Data Protection Directive in fact was based on the principle, although it did not coin a special concept to describe it.

Of particular interest in this connection is what procedural and technical advances the new concept offers those who will be applying the Regulation. To date, we have understood the principle on a general level: good personal data protection is not possible without good planning.

It is in fact easy to see that data protection by design, connected to the concept by default in the Regulation, is set out in far greater detail than in the earlier discussion of privacy by design. Yet, due to the principle of proportionality, those who want to minimize the level of data protection are given rather free hand to do so. For this reason,

19 *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

20 *As rule of thumb, the Finnish Data Protection Ombudsman Dr. h.c. Reijo AARNIO has noted that if those principles are being implemented already, the new Regulation will not put much pressure for change on controllers.*

21 *Dr. CAVOUKIAN was the Information and Privacy Commissioner in Ontario 2007-2014.*

certifications will take on considerable importance as indications of compliance with the required standard of data protection. The data-processing standards and certification mechanism are described in Article 25:[22]

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

In order for data protection by design and by default to produce the desired result, we will need not only certifications but standards and official guidelines as well. In fact, standards were one of the regulatory tools envisaged by the EU Commission when drafting the Regulation; they represent a step forward from manual data protection to a more automatic safeguarding of the rights of the individual when processing personal data.

Without doubt the most challenging area in the planning of information systems in information government is still the legal planning of the relationship between public access to official documents and the protection of personal data. The Regulation contains an article, article 86, specifically dedicated to this concern:[23]

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

As can be readily seen, this provision largely relegates the planning and implementation of government information systems to the national level. This leaves the relevant processes open to influences from the national legal cultures – and to a significant extent. The harmonizing effect sought by the Regulation might thus end up being less than originally anticipated.[24] It is not easy to achieve a consensus on the right thing to do.

Moreover, I should point out that the Regulation has brought a number of new obligations for the public sector. A particularly salient one is the requirement that a data protection officer be appointed in all public authorities or bodies. Well-educated data protection officers may play a crucial role in the development of information government.

In order that we might see things in their proper light, we also have to take a look at the relationship between data protection and freedom of expression embodied in the Regulation. It naturally respects freedom of expression as a human right, but lays down no detailed provisions on how this is to be done; rather, it is left to the domestic legislation of each member state to effect a balance between freedom of expression and protection of personal data (Article 86). In addition, the recitals speak for a broad interpretation of the concept of journalism. In this light, it will come as no surprise when the European Court of Human Rights and the Court of Justice of the EU continue to find themselves busy ruling on the relationship between freedom of expression, freedom of information and the protection of personal data.

22 *Correspondingly, today there is a possibility in Finland to perform an assessment of the information security of information systems. This is provided for in the law.*

23 *The Directive had a recital (72) insisted on by Finland and Sweden stating that the principle of openness could be taken into account. The operative part of the Directive makes no mention of this. When the Regulation was being drafted Finland and Sweden insisted the matter be incorporated into the articles proper.*

24 *Recital 154, however, points out the positive relevance of the Regulation: "Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation."*

One might ask why a proper understanding of the protection of personal data and, more broadly, the protection of privacy has eluded us – and continues to. The answer lies in the limited visibility of Information Law as a branch of law and as an academic discipline. I will move on to take up this issue in concluding.

7. INFORMATION LAW

Information Law has been a fundamental component of Finnish Legal Informatics for many years. In the Network Society information is no longer merely cheap raw material that helps us to achieve an end. It is an element that has taken on a new importance in what is a new society and a new, digital environment.[25]

Previously, the notion that Information Law was a field in its own right was often considered dubious. The main argument was that since information is everywhere, it would be difficult or even impossible to find the common principles needed to give the field an internal consistency. And in the case of a particular legal discipline, having a general theory with common concepts, principles and theories is the key to a better constitutional state.

Today, however, we can justifiably speak of the leading principles of information law – and we must. In my view, the most important principles are, as I have already indicated, the right to know and the right to information. But there are other leading principles too: the right to communication, freedom of information, the free flow of information, the informational right to self-determination, the right to an information balance, the right to good information government and the right to information security.

Each of these is a fundamental meta right in the constitutional state; that is, each is a goal-oriented moral right on the level of a social contract. Most of these meta rights have no express reflections on the level of fundamental rights in the form of legal provisions, but they are clear backdrops for regulating and understanding human and fundamental rights.

I will not go into a detailed description of these rights or their interrelationship here. The topic would warrant a presentation of its own. What I would like to do, with a note of challenge, is to assert that anyone engaged in the legal planning of information systems must have a sound knowledge of these rights and an ability to take their implications into account. By way of contrast, I would like to speak of "blind balancing", in which attitudes regularly steer things in the same direction without taking all relevant information seriously. This is a very real problem today, when some data systems accentuate openness, and some data protection. When planning data systems, digital lawyers in the modern Network Society must be able to strike a balance between our constitutional rights.[26]

To be sure, as we know, in most cases data processing in its different forms, disclosure of data and decisions based on the data are relatively straightforward processes. What we call hard cases are the exception rather than the rule – in administrative and legal decision making alike. Sound planning and use of dynamic documents will – or could - reduce the number of such cases. This alone would be a step forward towards better information government.

But we would still be left with some tough nuts to crack – and there will be plenty of such cases. Information government in the constitutional state cannot be allowed to operate on a case-by-case basis dependent on the skills of the users of data systems. We need informational tools that will support decision making. In my view, these are to be found in computer-based expert systems, designed and built on the principles of Information Law, that is, with due regard for the rights of the individual.

These tools can range from the various visual signs associated with law to legal expert systems.27 Both are needed. The need for appropriate visualization was noted already by the EU Commission when working on the first drafts of the Regulation. And advances in IT make it more feasible than ever to build agile expert systems that will alert users of information systems to situations

25 *See also SAARENPÄÄ Legal informatics today – The view from the University of Lapland pp. 10-16 in Saarenpää – Sztobryn Lawyers in the Media Society (2016). In Germany there was some discussion about information law back in the early 1970s. But the modern European concept of information law was first introduced by the Norwegian scholar Jon Bing in the early 1980s. See Bing, Information Law. Journal of Media Law and Practice, 1981, p. 219.*

26 *See more SAARENPÄÄ The Digital Lawyer. What skills are required of the lawyer in the Network Society? IRIS 2015 pp.73-85.*

27 *See also SAARENPÄÄ Law: linear texts or visual experiences? pp 34-42 in Saarenpää – Sztobryn Lawyers in the Media society.*

where there might be legal obstacles to automatic decision making or to the printing of documents. We are at last witnessing the advent of expert systems.

8. CONCLUDING REMARKS

One threat we must constantly contend with in legal life is the increasing scarcity of justice. Poor bureaucracy and poor routines result in needless constraints on, or even insurmountable obstacles to, people and organizations being able to exercise the rights they have. This is of course a problem that has plagued us for as long as we can remember. However, it is one that poor legal planning of information systems can very easily exacerbate.

We most certainly need tools to steer our decisions in the right direction – whether we are dealing with individual cases or more sweeping solutions. These tools are the general theories of law. Concepts, principles and system connected theories are the key tools of our trade. As the late Finnish professor of legal theory Hannu Tolonen so aptly put it, these tools tell us what is or what can be right and wrong. A good lawyer has a good toolbox at his or her disposal for recognizing legal phenomena and problems. Today this toolbox can at least partly include expert systems within information systems.

But before we can engage in legal planning and design expert systems, we need general doctrines that are equal to the task, ones that are up to date. It is here that we run into one undeniable problem in information government today. The general theories of Information Law have developed very slowly indeed. We see a varied set of tools being used in different countries to achieve an equitable balance where the fundamental rights of individuals are concerned. The government, and above all the media, engage in practices that seriously compromise people's informational rights, laying fertile ground for blind, specious balancing of rights. Sophisticated general theories make it possible to counter such practices.

The impacts of the European General Data Protection Regulation may to some extent make our work in Europe easier with regard to protection of personal data and the media. Like the Directive, the Regulation stresses that the processing of personal data for journalistic purposes is essential. Only that which is essential in a democracy is enough to justify an exception to the protection afforded personal data. The Regulation shows no desire on the part of the legislator to create new rights for the media.

Yet, as noted above, the openness/transparency of government is left largely up to the individual member states. If we recall that most of those working in government received their education and training back when traditional conceptions of openness prevailed, we have a goodly number of challenging years ahead of us, especially in the Nordic countries, where modern legal planning of information systems is concerned. The challenges ahead are ones that Legal Informatics can and should address – readily and robustly. And always we must remember the words in recital 4 of the new Regulation: "The processing of personal data should be designed to serve mankind."

BIBLIOGRAPHY

Baradan, Shima Rebalancing the Fourth Amendment, Georgetown Law Journal (2013).

Barzallo – Valdés – Reyes Olmedo – Amoroso Fernándes (eds) XVI Congreso Iberoamericano de Derecho e Informatica (2012)Carlsson Ulla (ed) Freedom of Expression Revisited. Citizenship and Journalism in the Digital Era (2013)

Galindo, Fernando (ed) , El derecho de la sociedad en red, Lefis Series, Band 14 (2013)

Girardi, Dino –Palmirani, Monica Open Government Data: Legal Economical and Semantic Web Aspects pp 187-205 in Saarenpää - Sztobryn (ed) Lawyers in the Media society.

incke, Wolfgang Knowledge, Information and Individuals pp 17-33 in Saarenpää - Sztobryn (ed) Lawyers in the Media society

ordenstreng, Kaarle Deconstructing Libertarian Myths About Press Freedom pp 45-59 in Carlsson (ed) Freedom of Expression Revisited

Palmirani, Monica Legislative XML: principles and technical tools (2012)

Reyes Olmedo, Patricia (ed) Gobierno de la Información: realidades contemporáneas. Libro en edición.

Saarenpää Ahti Information and Law in the Constitutional State pp. 443-452 in Traunmüller (ed) Electronic Government Third International Conference, EGOV 2004

Saarenpää, Ahti Regulating the Network Society. A challenge for the Quality of Legislation and other activities pp 99 in Schweighofer – Saarenpää – Böszörmenyi (eds) KnowRight 2012

Saarenpää, Ahti Legal welfare and legal planning pp 47-69 in Barzallo – Valdés – Reyes Olmedo – Amoroso Fernándes (eds) XVI Congreso Iberoamericano de Derecho e Informatica (2012)

Saarenpää, Ahti Data Protection in the Network Society – the exceptional becomes the natural pp 85-124 in Galindo (ed) El derecho de la sociedad en red

Saarenpää, Ahti The Digital Lawyer. What skills are required of the lawyer in the Network Society? IRIS 2015

Saarenpää, Ahti Openness, Journalism and Personal Data Protection – Lessons from the Taxation Data Business 489-494 in Schweighofer – Kummer –Hötzendorfer – Borges

Saarenpää, Ahti Legal Informatics today –the view from the university of Lapland pp 10-16 in Saarenpää – Sztobryn Lawyers in the Media society

Saarenpää, Ahti Law: Linear texts or visual experiences? Challenges for teaching law in the Network Society pp 33-42 in Saarenpää – Sztobryn Lawyers in the Media society

Saarenpää, Ahti – Sztobryn, Karolina Lawyers in the Media society. The legal challenges of the Media society (2016)

Saarenpää, Ahti E-justice and the Network Society Some comments from the Finnish point of View in Serbena.(ed) Brazilian and European perspectives on e-Justice Serbena Cesar A.(ed) Brazilian and European perspectives on e-Justice. (ed) Edition in Portuguese and English (2016). Schartum Dag Wiese Developing eGovernment Systems – legal, technological and organizational aspects pp 69-94 in Schartum – Becken (ed) YULEX 2011

Schweighofer – Kummer – Hötzendorfer Kooperation IRIS 2015

Schweighofer – Kummer –Hötzendorfer – Borges Netzwerke IRIS 2016

Saarenpää, Ahti – Wiatrowski, Aleksander Society Trapped in the Network. Does it have a Future? (2016)

Schweighofer – Saarenpää – Böszörmenyi (eds.), KnowRight 2012

Solove, Daniel The Digital person: Technology and Privacy in the information Age (2004)*Staudt, Ronald W.* Law Office Automation Approaching the Millennium , International Journal of Law and Information Technology, 1993 nr 1 pp 59-76

Svantesson Dan Jerker B. Extraterritoriality in Data Privacy Law (2013)

Willinsky, John The Access Principle . The case for open access to research and scholarship (2006)

JURISPRUDENCIA

SENTENCIA DEL TRIBUNAL DE JUSTICIA

(Gran Sala) de 13 de mayo de 2014 (*)

«Datos personales

— Protección de las personas físicas en lo que respecta al tratamiento de dichos datos — Directiva 95/46/CE — Artículos 2, 4, 12 y 14 — Ámbito de aplicación material y territorial — Motores de búsqueda en Internet — Tratamiento de datos contenidos en sitios de Internet — Búsqueda, indexación y almacenamiento de estos datos — Responsabilidad del gestor del motor de búsqueda — Establecimiento en territorio de un Estado miembro — Alcance de las obligaciones de dicho gestor y de los derechos del interesado — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7 y 8»

En el asunto C-131/12, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, recibido en el Tribunal de Justicia el 9 de marzo de 2012, en el procedimiento entre **Google Spain, S.L., Google Inc.** Y **Agencia Española de Protección de Datos (AEPD), Mario Costeja González,** EL TRIBUNAL DE JUSTICIA (Gran Sala), integrado por el Sr. V. Skouris, Presidente, el Sr. K. Lenaerts, Vicepresidente, los Sres. M. Ilešič (Ponente), L. Bay Larsen, T. von Danwitz y M. Safjan, Presidentes de Sala, y los Sres. J. Malenovský, E. Levits, A. Ó Caoimh y A. Arabadjiev y las Sras. M. Berger y A. Prechal y el Sr. E. Jarašiūnas, Jueces; Abogado General: Sr. N. Jääskinen; Secretaria: Sra. M. Ferreira, administradora principal; habiendo considerado los escritos obrantes en autos y celebrada la vista el 26 de febrero de 2013 consideradas las observaciones presentadas:

- en nombre de Google Spain, S.L., y Google Inc., por los Sres. F. González Díaz, J. Baño Fos y B. Holles, abogados;
- en nombre del Sr. Costeja González, por el Sr. J. Muñoz Rodríguez, abogado;
- en nombre del Gobierno español, por el Sr. A. Rubio González, en calidad de agente;
- en nombre del Gobierno helénico, por la Sra. E.-M. Mamouna y el Sr. K. Boskovits, en calidad de agentes;
- en nombre del Gobierno italiano, por la Sra. G. Palmieri, en calidad de agente, asistida por el Sr. P. Gentili, avvocato dello Stato;
- en nombre del Gobierno austriaco, por el Sr. G. Kunnert y la Sra. C. Pesendorfer, en calidad de agentes;
- en nombre del Gobierno polaco, por los Sres. B. Majczyna y M. Szpunar, en calidad de agentes;
- en nombre de la Comisión Europea, por la Sra. I. Martínez del Peral y Sr. B. Martenczuk, en calidad de agentes;

Oídas las conclusiones del Abogado General, presentadas en audiencia pública el 25 de junio de 2013, dicta la siguiente

SENTENCIA

1 La petición de decisión prejudicial versa sobre la interpretación de los artículos 2, letras b) y d), 4, apartado 1, letras a) y c), 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), y del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2 Esta petición se presentó en el marco de un litigio entre Google Spain, S.L. (en lo sucesivo, «Google Spain»), y Google Inc., por un lado, y la Agencia Española de Protección de Datos (en lo sucesivo, «AEPD») y el Sr. Costeja González, por otro, en relación con una resolución de dicha Agencia por la que se estimó la reclamación del Sr. Costeja González contra ambas sociedades y se ordenaba a Google Inc. que adoptara las medidas necesarias para retirar los datos personales del Sr. Costeja González de su índice e imposibilitara el acceso futuro a los mismos.

MARCO JURÍDICO

Derecho de la Unión

3 La Directiva 95/46, que, según su artículo 1, tiene por objeto la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales y la eliminación de los obstáculos a la libre circulación de estos datos, enuncia lo siguiente en sus considerandos 2, 10, 18 a 20 y 25:

«(2) Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir [...] al bienestar de los individuos;

[...]

(10) Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[,firmado en Roma el 4 de noviembre de 1950], así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

[...]

(18) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado;

(19) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;

(20) Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;

[...]

(25) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas [...] que efectúen tratamientos- obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento- y, por

otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias».

4 El artículo 2 de la Directiva 95/46 establece que «a efectos de [ésta], se entenderá por:

a) "datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

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

[...]

d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

[...]»

5 El artículo 3 de dicha Directiva, titulado «Ámbito de aplicación», precisa en su apartado 1:

«Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.»

6 El artículo 4 de la misma Directiva, titulado «Derecho nacional aplicable», dispone:

«1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.»

7 El artículo 6 de la Directiva 95/46, titulado «Principios relativos a la calidad de los datos», incluido en el capítulo II, sección I, de dicha Directiva, tiene el siguiente tenor:

«1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.»

8 El artículo 7 de la Directiva 95/46, titulado «Principios relativos a la legitimación del tratamiento de datos», incluido en el capítulo I, sección II, de esta Directiva, establece:

«Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

[...]

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.»

9 El artículo 9 de la mencionada Directiva, titulado «Tratamiento de datos personales y libertad de expresión», dispone:

«En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.»

10 El artículo 12 de la misma Directiva, titulado «Derecho de acceso», establece:

«Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

[...]

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

[...]»

11 El artículo 14 de la Directiva 95/46, titulado «Derecho de oposición del interesado», dispone:

«Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

[...]»

12 El artículo 28 de dicha Directiva, rubricado «Autoridad de control», tiene el siguiente tenor:

«1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

[...]

3. La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de [...] ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento [...]
- [...]

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

[...]

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

[...]»

Derecho español

13 La Directiva 95/46 ha sido transpuesta en Derecho español por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 298, de 14 de diciembre de 1999, p. 43088).

LITIGIO PRINCIPAL Y CUESTIONES PREJUDICIALES

14 El 5 de marzo de 2010, el Sr. Costeja González, de nacionalidad española y domiciliado en España, presentó ante la AEPD una reclamación contra La Vanguardia Ediciones, S.L., que publica un periódico de gran difusión, concretamente en Cataluña (en lo sucesivo, «La Vanguardia»), y contra Google Spain y Google Inc. Esta reclamación se basaba en que, cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google (en lo sucesivo, «Google Search»), obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González.

15 Mediante esta reclamación, el Sr. Costeja González solicitaba, por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados

a los enlaces de La Vanguardia. En este marco, el Sr. Costeja González afirmaba que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente.

16 Mediante resolución de 30 de julio de 2010, la AEPD desestimó la reclamación en la medida en que se refería a La Vanguardia, al considerar que la publicación que ésta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores.

17 En cambio, se estimó la misma reclamación en la medida en que se dirigía contra Google Spain y Google Inc. A este respecto, la AEPD consideró que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. La AEPD estimó que este requerimiento puede dirigirse directamente a los explotadores de motores de búsqueda, sin suprimir los datos o la información de la página donde inicialmente está alojada e, incluso, cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal.

18 Google Spain y Google Inc. interpusieron sendos recursos contra dicha resolución ante la Audiencia Nacional, que decidió acumularlos.

19 El mencionado tribunal expone en el auto de remisión que estos recursos plantean la cuestión de cuáles son las obligaciones que tienen los gestores de motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contiene sus datos personales y permite relacionarles con la misma, sea localizada, indexada y sea puesta a disposición de los internautas de forma indefinida. Considera que la respuesta a esta cuestión depende del modo en que debe interpretarse la Directiva 95/46 en el marco de estas tecnologías, que han surgido después de su publicación.

20 En estas circunstancias, la Audiencia Nacional decidió suspender el procedimiento y plantear al Tribunal de Justicia las cuestiones prejudiciales siguientes:

«1) ¿Por lo que respecta a la aplicación territorial de la Directiva [95/46] y, consiguientemente de la normativa española de protección de datos:

a) Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la [Directiva 95/46], cuando concurra alguno o algunos de los siguientes supuestos:

- cuando la empresa proveedora del motor de búsqueda crea en un Estado miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes del Estado,

  o

- cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa,

  o

- cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria?

b) ¿Debe interpretarse el art. 4.1.c de la [Directiva 95/46] en el sentido de que existe un "recurso a medios situados en el territorio de dicho Estado miembro":

- cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro

  o

- cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro?

c) ¿Puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la [Directiva 95/46], el almacenamiento temporal de la información indexada por los buscadores en internet? Si la respuesta a esta última cuestión fuera afirmativa, ¿puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas?

d) Con independencia de la respuesta a las preguntas anteriores y especialmente en el caso en que se considerase por el Tribunal de Justicia de la Unión que no concurren los criterios de conexión previstos en el art. 4 de la [Directiva 95/46]:

¿Debe aplicarse la [Directiva 95/46], a la luz del art. 8 de la [Carta], en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión [...]?

2) Por lo que respecta a la actividad de los buscadores como proveedor de contenidos en relación con la [Directiva 95/46]:

a) En relación con la actividad [de Google Search], como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos", contenido en el art. 2.b de la [Directiva 95/46]?

b) En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita:

¿Debe interpretarse el artículo 2.d) de la [Directiva 95/46], en el sentido de considerar que la empresa que gestiona [Google Search] es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?

c) En el caso de que la respuesta anterior fuera afirmativa:

¿Puede la [AEPD], tutelando los derechos contenidos en el art. 12.b) y 14.a) de la [Directiva 95/46], requerir directamente [a Google Search] para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?

d) En el caso de que la respuesta a esta última pregunta fuera afirmativa:

¿Se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene esos datos se haya publicado lícitamente por terceros y se mantenga en la página web de origen?

3) Respecto al alcance del derecho de cancelación y/oposición en relación con el derecho al olvido se plantea la siguiente pregunta:

¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la [Directiva 95/46] comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?»

SOBRE LAS CUESTIONES PREJUDICIALES

Sobre la segunda cuestión prejudicial, letras a) y b), relativa al ámbito de aplicación material de la Directiva 95/46

21 Mediante su segunda cuestión prejudicial, letras a) y b), que procede examinar en primer lugar, el tribunal remitente desea saber, en esencia, si el artículo 2, letra b), de la Directiva 95/46 debe examinarse en el sentido de que la actividad de un motor de búsqueda como proveedor de contenidos, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido de dicha disposición, cuando esa información contiene datos personales. En el supuesto de que se responda afirmativamente a esa cuestión, el tribunal remitente desea saber, además, si la letra d) del mencionado artículo 2 debe interpretarse en el sentido de que el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento de datos personales, en el sentido de esa disposición.

22 Según Google Spain y Google Inc., la actividad de los motores de búsqueda no puede considerarse tratamiento de los datos que se muestran en las páginas web de terceros que presenta la lista de resultados de la búsqueda, dado que estos motores tratan la información accesible en Internet globalmente sin seleccionar entre datos personales y el resto de información. En su opinión, además, aun suponiendo que esta actividad deba ser calificada de «tratamiento de datos», el gestor de un motor de búsqueda no puede considerarse «responsable» de ese tratamiento, ya que no conoce dichos datos y no ejerce control sobre ellos.

23 En cambio, el Sr. Costeja González, los Gobiernos español, italiano austriaco y polaco y la Comisión Europea sostienen que dicha actividad implica claramente un «tratamiento de datos», en el sentido de la Directiva 95/46, que es distinto del tratamiento de datos realizado por los editores de los sitios de Internet y persigue objetivos distintos al de éste. A su juicio, el gestor de un motor de búsqueda es «responsable» del tratamiento de datos efectuado por él desde el momento en que es él quien determina la finalidad y los medios de dicho tratamiento.

24 Según el Gobierno helénico, la actividad controvertida constituye tal «tratamiento», pero, en la medida en que los motores de búsqueda sirven de simples intermediarios, las empresas que los gestionan no pueden considerarse «responsables», salvo en los casos en los que almacenan datos en una «memoria intermedia» o una «memoria oculta» por un período de tiempo que supere lo técnicamente necesario.

25 A este respecto, ha de señalarse que el artículo 2, letra b), de la Directiva 95/46 define el «tratamiento de datos personales» como «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción».

26 En lo que atañe, en particular, a Internet, el Tribunal de Justicia ya ha tenido ocasión de declarar que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un «tratamiento» de esta índole, en el sentido del artículo 2, letra b), de la Directiva 95/46 (véase la sentencia Lindqvist, C-101/01, EU:C:2003:596, apartado 25).

27 En cuanto a la actividad controvertida en el litigio principal, no se discute que entre los datos hallados, indexados, almacenados por los motores de búsqueda y puestos a disposición de sus usuarios figura también información relativa a personas físicas identificadas o identificables y, por tanto, «datos personales» en el sentido del artículo 2, letra a), de dicha Directiva.

28 Por consiguiente, debe declararse que, al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46,

deben calificarse de «tratamiento» en el sentido de dicha disposición, sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales.

29 Tampoco contradice la apreciación anterior el hecho de que estos datos hayan sido ya objeto de publicación en Internet y dicho motor de búsqueda no los modifique.

30 De este modo, el Tribunal de Justicia ya ha declarado que las operaciones a las que se refiere el artículo 2, letra b), de la Directiva 95/46 deben calificarse de tal tratamiento también en el supuesto de que se refieran únicamente a información ya publicada tal cual en los medios de comunicación. En efecto, señaló a este respecto que una excepción general a la aplicación de la Directiva 95/46 en tal supuesto dejaría esta última en gran medida vacía de contenido (véase, en este sentido, la sentencia Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartados 48 y 49).

31 Además, se desprende de la definición contenida en el artículo 2, letra b), de la Directiva 95/46 que, aunque la modificación de datos personales constituye, ciertamente, un tratamiento, en el sentido de ésta, en cambio el resto de operaciones que se mencionan en ella no precisan en modo alguno de que estos datos se modifiquen.

32 En cuanto a si el gestor de un motor de búsqueda debe o no considerarse «responsable del tratamiento» de los datos personales efectuado por dicho motor en el marco de una actividad como la controvertida en el litigio principal, debe recordarse que el artículo 2, letra d), de la Directiva 95/46 define al responsable como «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales».

33 Ahora bien, el gestor del motor de búsqueda es quien determina los fines y los medios de esta actividad y, así, del tratamiento de datos personales que efectúa él mismo en el marco de ésta y, por consiguiente, debe considerarse «responsable» de dicho tratamiento en virtud del mencionado artículo 2, letra d).

34 Por otro lado, es necesario declarar que sería contrario, no sólo al claro tenor de esta disposición sino también a su objetivo, consistente en garantizar, mediante una definición amplia del concepto de «responsable», una protección eficaz y completa de los interesados, excluir de esta disposición al gestor de un motor de búsqueda debido a que no ejerce control sobre los datos personales publicados en las páginas web de terceros.

35 Sobre este particular, procede poner de manifiesto que el tratamiento de datos personales llevado a cabo en el marco de la actividad de un motor de búsqueda se distingue del efectuado por los editores de sitios de Internet, que consiste en hacer figurar esos datos en una página en Internet, y se añade a él.

36 Además, es pacífico que esta actividad de los motores de búsqueda desempeña un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado, incluidos los internautas que, de no ser así, no habrían encontrado la página web en la que se publican estos mismos datos.

37 Además, la organización y la agregación de la información publicada en Internet efectuada por los motores de búsqueda para facilitar a sus usuarios el acceso a ella puede conducir, cuando la búsqueda de los usuarios se lleva a cabo a partir del nombre de una persona física, a que éstos obtengan mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet que les permita establecer un perfil más o menos detallado del interesado.

38 En consecuencia, en la medida en que la actividad de un motor de búsqueda puede afectar, significativamente y de modo adicional a la de los editores de sitios de Internet, a los derechos fundamentales de respeto de la vida privada y de protección de datos personales, el gestor de este motor, como persona que determina los fines y los medios de esta actividad, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicha actividad satisface las exigencias de la Directiva 95/46 para que las garantías establecidas en ella puedan tener pleno efecto y pueda llevarse a cabo una protección eficaz y completa de los interesados, en particular, de su derecho al respeto de la vida privada.

39 Por último, el que los editores de sitios de Internet tengan la facultad de indicar a los gestores de los motores de búsqueda, con la ayuda, concretamente, de protocolos de exclusión como «robot.txt», o de códigos como «noindex» o «noarchive», que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores, no significa que la falta de tal indicación por parte de estos editores libere al gestor de un motor de búsqueda de su responsabilidad por el tratamiento de datos personales que lleva a cabo en el marco de la actividad de dicho motor.

40 En efecto, esta circunstancia no modifica el hecho de que el gestor determina los fines y los medios de este tratamiento. Además, aun suponiendo que dicha facultad de los editores de sitios de Internet signifique que éstos determinen conjuntamente con dicho gestor los medios del mencionado tratamiento, tal afirmación no elimina en modo alguno la responsabilidad del gestor, ya que el artículo 2, letra d), de la Directiva 95/46 prevé expresamente que esta determinación puede realizarse «sólo o conjuntamente con otros».

41 Del conjunto de las consideraciones precedentes se desprende que procede responder a la segunda cuestión prejudicial, letras a) y b), que el artículo 2, letras b) y d), de la Directiva 95/46 debe interpretarse en el sentido de que, por un lado, la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del mencionado artículo 2, letra d).

Sobre la primera cuestión prejudicial, letras a) a d), relativas al ámbito de aplicación territorial de la Directiva 95/46

42 Mediante su primera cuestión prejudicial, letras a) a d), el tribunal remitente desea que se aclare si es posible aplicar la norma nacional que traspone la Directiva 95/46 en circunstancias como las controvertidas en el litigio principal.

43 En este marco, el tribunal remitente considera acreditados los siguientes hechos:

- Google Search se presta a nivel mundial a través del sitio de Internet «www.google.com». En muchos países existen versiones locales adaptadas al idioma nacional. La versión española de Google Search se presta a través del sitio www.google.es, dominio que tiene registrado desde el 16 de septiembre de 2003. Google Search es uno de los motores de búsqueda más utilizados en España.
- Google Inc. (empresa matriz del grupo Google), con domicilio en los Estados Unidos, gestiona Google Search.
- Google Search indexa páginas web de todo el mundo, incluyendo páginas web ubicadas en España. La información indexada por sus «arañas» o robots de indexación, es decir, programas informáticos utilizados para rastrear y realizar un barrido del contenido de páginas web de manera metódica y automatizada, se almacena temporalmente en servidores cuyo Estado de ubicación se desconoce, ya que este dato es secreto por razones competitivas.
- Google Search no sólo facilita el acceso a los contenidos alojados en las páginas web indexadas, sino que también aprovecha esta actividad para incluir publicidad asociada a los patrones de búsqueda introducidos por los internautas, contratada, a cambio de un precio, por las empresas que desean utilizar esta herramienta para ofrecer sus bienes o servicios a éstos.
- El grupo Google utiliza una empresa filial, Google Spain, como agente promotor de venta de los espacios publicitarios que se generan en el sitio de Internet «www.google.com». Google Spain tiene personalidad jurídica propia y domicilio social en Madrid, y fue creada el 3 de septiembre de 2003. Dicha empresa dirige su actividad fundamentalmente a las empresas radicadas en España, actuando como agente comercial del grupo en dicho Estado miembro. Tiene como objeto social promocionar, facilitar y procurar la venta de productos y servicios de publicidad «on line» a través de Internet para terceros, así como la comercialización de esta publicidad.

- Google Inc. designó a Google Spain como responsable del tratamiento en España de dos ficheros inscritos por Google Inc. ante la AEPD; el objeto de tales ficheros era almacenar los datos de las personas relacionadas con los clientes de servicios publicitarios que en su día contrataron con Google Inc.

44 Concretamente, el tribunal remitente se pregunta, con carácter principal, sobre el concepto de «establecimiento», en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46, y sobre el de «recurso a medios situados en el territorio de dicho Estado miembro», en el sentido del mencionado artículo 4, apartado 1, letra c).

Primera cuestión prejudicial, letra a)

45 Mediante su primera cuestión prejudicial, letra a), el tribunal remitente desea saber, en esencia, si el artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando se cumplen uno o varios de los tres requisitos siguientes:

- cuando la empresa proveedora del motor de búsqueda crea en un Estado miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del motor, que dirige su actividad a los habitantes de ese Estado, o
- cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa, o
- cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos personales, aun cuando dicha colaboración se realice de forma voluntaria.

46 Por lo que respecta al primer requisito, el tribunal remitente señala que Google Inc. gestiona técnica y administrativamente Google Search y que no está probado que Google Spain realice en España una actividad directamente vinculada a la indexación o al almacenamiento de información o de datos contenidos en los sitios de Internet de terceros. Sin embargo, la actividad de promoción y venta de espacios publicitarios, de la que Google Spain es responsable para España, constituye la parte esencial de la actividad comercial del grupo Google y puede considerarse que está estrechamente vinculada a Google Search.

47 El Sr. Costeja González, los Gobiernos español, italiano, austriaco y polaco y la Comisión consideran que, habida cuenta del vínculo indisociable entre la actividad del motor de búsqueda gestionado por Google Inc. y la de Google Spain, ésta debe considerarse un establecimiento de aquélla, en el marco de cuyas actividades se lleva a cabo el tratamiento de datos personales. En cambio, según Google Spain, Google Inc. y el Gobierno helénico, el artículo 4, apartado 1, letra a), de la Directiva 95/46 no se aplica en el supuesto de que se esté ante el primero de los tres requisitos enumerados por el tribunal remitente.

48 Sobre este particular, procede recordar, en primer lugar, que el considerando 19 de la Directiva aclara que «el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable», y «que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante».

49 Pues bien, no se discute que Google Spain se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España. Además, al estar dotada de personalidad jurídica propia, es de este modo una filial de Google Inc. en territorio español, y, por lo tanto, un «establecimiento», en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46.

50 Para cumplir el requisito establecido en dicha disposición, es necesario además que el tratamiento de datos personales por parte del responsable del tratamiento se «lleve a cabo en el marco de las actividades» de un establecimiento de dicho responsable situado en territorio de un Estado miembro.

51 Google Spain y Google Inc. niegan que éste sea el caso, dado que el tratamiento de datos personales controvertido en el litigio principal lo lleva a cabo exclusivamente Google Inc., que gestiona Google Search sin ninguna intervención por parte de Google Spain, cuya actividad se limita a prestar apoyo a la actividad publicitaria del grupo Google, que es distinta de su servicio de motor de búsqueda.

52 No obstante, como subrayaron, en particular, el Gobierno español y la Comisión, el artículo 4, apartado 1, letra a), de la Directiva 95/46 no exige que el tratamiento de datos personales controvertido sea efectuado «por» el propio establecimiento en cuestión, sino que se realice «en el marco de las actividades» de éste.

53 Además, visto el objetivo de la Directiva 95/46 de garantizar una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, ésta expresión no puede ser objeto de una interpretación restrictiva (véase, por analogía, la sentencia L'Oréal y otros, C-324/09, EU:C:2011:474, apartados 62 y 63).

54 En este marco, cabe señalar que se desprende, concretamente de los considerandos 18 a 20 y del artículo 4 de la Directiva 95/46, que el legislador de la Unión pretendió evitar que una persona se viera excluida de la protección garantizada por ella y que se eludiera esta protección, estableciendo un ámbito de aplicación territorial particularmente extenso.

55 Habida cuenta de este objetivo de la Directiva 95/46 y del tenor de su artículo 4, apartado 1, letra a), procede considerar que el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa «en el marco de las actividades» de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor.

56 En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades.

57 Sobre este particular, es necesario recordar que, como se ha precisado en los apartados 26 a 28 de la presente sentencia, la propia presentación de datos personales en una página de resultados de una búsqueda constituye un tratamiento de tales datos. Pues bien, toda vez que dicha presentación de resultados está acompañada, en la misma página, de la presentación de publicidad vinculada a los términos de búsqueda, es obligado declarar que el tratamiento de datos personales controvertido se lleva a cabo en el marco de la actividad publicitaria y comercial del establecimiento del responsable del tratamiento en territorio de un Estado miembro, en el caso de autos el territorio español.

58 En tales circunstancias, no se puede aceptar que el tratamiento de datos personales llevado a cabo para el funcionamiento del mencionado motor de búsqueda se sustraiga a las obligaciones y a las garantías previstas por la Directiva 95/46, lo que menoscabaría su efecto útil y la protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas que tiene por objeto garantizar (véase, por analogía, la sentencia L'Oréal y otros, EU:C:2011:474, apartados 62 y 63), en particular, el respeto de su vida privada en lo que respecta al tratamiento de datos personales, al que esta Directiva concede una importancia especial, como confirman, concretamente, su artículo 1, apartado 1, y sus considerandos 2 y 10 (véanse, en este sentido, las sentencias Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 70; Rijkeboer, C-553/07, EU:C:2009:293, apartado 47, e IPI, C-473/12, EU:C:2013:715, apartado 28 y jurisprudencia citada).

59 En la medida en que el primero de los tres requisitos enumerados por el tribunal remitente basta por sí mismo para concluir que un establecimiento como Google Spain cumple el criterio recogido en el artículo 4, apartado 1, letra a), de la Directiva 95/46, no es necesario examinar los otros dos requisitos.

60 De lo anterior se deduce que procede responder a la primera cuestión prejudicial, letra a), que el artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento

del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.

Primera cuestión prejudicial, letras b) a d)

61 En vista de la respuesta dada a la primera cuestión prejudicial, letra a), no es preciso contestar a la primera cuestión, letras b) a d).

Sobre la segunda cuestión prejudicial, letras c) y d), relativa al alcance de la responsabilidad del gestor de un motor de búsqueda en virtud de la Directiva 95/46

62 Mediante su segunda cuestión prejudicial, letras c) y d), el tribunal remitente desea saber, en esencia, si los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en sí misma en dichas páginas sea lícita.

63 Google Spain y Google Inc. consideran que, en virtud del principio de proporcionalidad, cualquier solicitud que tenga por objeto que se elimine información debe dirigirse al editor del sitio de Internet de que se trate, ya que éste es quien asume la responsabilidad de publicar la información, quien puede examinar la licitud de esta publicación y quien dispone de los medios más eficaces y menos restrictivos para hacer que esa información sea inaccesible. Además, consideran que imponer al gestor de un motor de búsqueda que retire de sus índices información publicada en Internet no tiene suficientemente en cuenta los derechos fundamentales de los editores de sitios de Internet, del resto de los internautas y del propio gestor.

64 Según el gobierno austriaco, una autoridad de control nacional únicamente puede ordenar a tal gestor que borre de sus ficheros información publicada por terceros si anteriormente se ha declarado la ilegalidad o la inexactitud de los datos controvertidos o si el interesado ha ejercido con éxito su derecho de oposición ante el editor del sitio de Internet en el que se ha publicado la información.

65 El Sr. Costeja González, los Gobiernos español, italiano y polaco y la Comisión consideran que la autoridad nacional puede ordenar directamente al gestor de un motor de búsqueda que retire de sus índices y de su memoria intermedia información que contiene datos personales publicada por terceros, sin dirigirse previa o simultáneamente al editor de la página web en la que se ubica dicha información. Además, a juicio del Sr. Costeja González, de los Gobiernos español e italiano y de la Comisión, el que dicha información se publicara de forma lícita y que siga figurando en la página web de origen carece de relevancia sobre las obligaciones de dicho gestor con arreglo a la Directiva 95/46. En cambio, para el Gobierno polaco, este hecho le libera de sus obligaciones.

66 Con carácter previo, procede recordar que, como se desprende de su artículo 1 y de su considerando 10, la Directiva 95/46 tiene por objeto garantizar un nivel elevado de protección de las libertades y los derechos fundamentales de las personas físicas, sobre todo de su vida privada, en relación con el tratamiento de datos personales (véase, en este sentido, la sentencia IPI, EU:C:2013:715, apartado 28).

67 Según el considerando 25 de la Directiva 95/46, los principios de la protección que ésta establece tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas que efectúen tratamientos —obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento—, y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias.

68 El Tribunal de Justicia ya ha declarado que las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad, deben ser interpretadas a la luz de los dere-

chos fundamentales que, según reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia y que están actualmente recogidos en la Carta (véanse, en particular, las sentencias Connolly/Comisión, C-274/99 P, EU:C:2001:127, apartado 37, y Österreichischer Rundfunk y otros, EU:C:2003:294, apartado 68).

69 De este modo, el artículo 7 de la Carta garantiza el respecto de la vida privada, mientras que el artículo 8 de la Carta proclama expresamente el derecho a la protección de los datos personales. Los apartados 2 y 3 de este último precisan que estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, que toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación y que el respeto de estas normas estará sujeto al control de una autoridad independiente. Aplican estos requisitos, en particular, los artículos 6, 7, 12, 14 y 28 de la Directiva 95/46.

70 En relación con el artículo 12, letra b), de la Directiva 95/46, éste dispone que los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento, en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos. Esta última aclaración, relativa al supuesto del incumplimiento de algunos requisitos recogidos en el artículo 6, apartado 1, letra d), de la Directiva 95/46, tiene carácter de ejemplo y no es taxativa, de lo que se desprende que la falta de conformidad del tratamiento, que puede ofrecer al interesado el derecho garantizado por el artículo 12, letra b), de dicha Directiva, puede también derivarse del incumplimiento de otros requisitos de legalidad impuestos por ésta al tratamiento de datos personales.

71 Sobre este particular, procede recordar que, no obstante las excepciones admitidas al amparo del artículo 13 de la Directiva 95/46, todo tratamiento de datos personales debe ser conforme, por una parte, con los principios relativos a la calidad de los datos, enunciados en el artículo 6 de dicha Directiva, y, por otra, con alguno de los principios relativos a la legitimación del tratamiento de datos, enumerados en el artículo 7 de la Directiva (véanse las sentencias Österreichischer Rundfunk y otros, EU:C:2003:294, apartado 65; ASNEF y FECEMD, C-468/10 y C-469/10, EU:C:2011:777, apartado 26, y Worten, C-342/12, EU:C:2013:355, apartado 33).

72 A tenor de este artículo 6 y sin perjuicio de las disposiciones específicas que los Estados miembros puedan establecer para el tratamiento con fines históricos, estadísticos o científicos, incumbe al responsable del tratamiento garantizar que los datos personales sean «tratados de manera leal y lícita», que sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines», que sean «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente», que sean «exactos y, cuando sea necesario, actualizados», y, por último, que sean «conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente». En este marco, el mencionado responsable debe adoptar todas las medidas razonables para que los datos que no responden a los requisitos de esta disposición sean suprimidos o rectificados.

73 En cuanto a la legitimación, en virtud del artículo 7 de la Directiva 95/46, de un tratamiento como el controvertido en el litigio principal efectuado por el gestor de un motor de búsqueda, éste puede estar incluido en la razón recogida en dicho artículo 7, letra f).

74 Esta disposición permite el tratamiento de datos personales cuando es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado, en particular, su derecho al respeto de su vida privada, en lo que respecta al tratamiento de datos personales, que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva. De este modo, la aplicación del mencionado artículo 7, letra f), precisa de una ponderación de los derechos e intereses en liza de que se trate, en cuyo marco debe tenerse en cuenta la importancia de los derechos del interesado, que resulta de los artículos 7 y 8 de la Carta (véase la sentencia ASNEF y FECEMD, EU:C:2011:777, apartados 38 y 40).

75 Aunque la conformidad del tratamiento con los artículos 6 y 7, letra f), de la Directiva 95/46 puede comprobarse en el marco de una solicitud, en el sentido del artículo 12, letra b), de esta Directiva, el

interesado puede además invocar en determinados supuestos el derecho de oposición previsto en el artículo 14, párrafo primero, letra a), de ésta.

76 Según dicho artículo 14, párrafo primero, letra a), los Estados miembros reconocerán al interesado el derecho a oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7 de la Directiva 95/46, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. La ponderación que ha de efectuarse en el marco de dicho artículo 14, párrafo primero, letra a), permite así tener en cuenta de modo más específico todas las circunstancias que rodean a la situación concreta del interesado. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos.

77 El interesado puede dirigir las solicitudes con arreglo a los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 directamente al responsable del tratamiento, que debe entonces examinar debidamente su fundamento y, en su caso, poner fin al tratamiento de los datos controvertidos. Cuando el responsable del tratamiento no accede a las solicitudes, el interesado puede acudir a la autoridad de control o a los tribunales para que éstos lleven a cabo las comprobaciones necesarias y ordenen a dicho gestor las medidas precisas en consecuencia.

78 A este respecto, procede recordar que se deriva del artículo 28, apartados 3 y 4, de la Directiva 95/46 que toda autoridad de control entenderá de las solicitudes de cualquier persona relativas a la protección de sus derechos y libertades en relación con el tratamiento de datos personales y que dispone de poderes de investigación y de poderes efectivos de intervención, que le permiten, en particular, ordenar el bloqueo, la supresión o la destrucción de datos, o prohibir provisional o definitivamente un tratamiento.

79 Deben interpretarse y aplicarse a la luz de estas consideraciones las disposiciones de la Directiva 95/46 que regulan los derechos del interesado cuando la autoridad de control o los tribunales conocen de una solicitud como la controvertida en el litigio principal.

80 A este respecto, debe señalarse, en primer lugar, que, como se ha afirmado en los apartados 36 a 38 de la presente sentencia, un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo (véase, en este sentido, la sentencia eDate Advertising y otros, C-509/09 y C-161/10, EU:C:2011:685, apartado 45).

81 Vista la gravedad potencial de esta injerencia, es obligado declarar que el mero interés económico del gestor de tal motor en este tratamiento no la justifica. Sin embargo, en la medida en que la supresión de vínculos de la lista de resultados podría, en función de la información de que se trate, tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión, es preciso buscar, en situaciones como las del litigio principal, un justo equilibrio, en particular entre este interés y los derechos fundamentales de la persona afectada con arreglo a los artículos 7 y 8 de la Carta. Aunque, ciertamente, los derechos de esa persona protegidos por dichos artículos prevalecen igualmente, con carácter general, sobre el mencionado interés de los internautas, no obstante este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública.

82 Como resultado del examen de los requisitos de aplicación de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, que se ha de realizar cuando conocen de una solicitud como la controvertida en el litigio principal, la autoridad de control o el órgano jurisdiccional pueden

ordenar a dicho gestor eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, sin que una orden en dicho sentido presuponga que ese nombre o esa información sean, con la conformidad plena del editor o por orden de una de estas autoridades, eliminados con carácter previo o simultáneamente de la página web en la que han sido publicados.

83 En efecto, como se ha afirmado en los puntos 35 a 38 de la presente sentencia, en la medida en que el tratamiento de datos personales llevado a cabo en la actividad de un motor de búsqueda se distingue del efectuado por los editores de sitios de Internet y se añade a éste y afecta de modo adicional a los derechos fundamentales del interesado, el gestor de este motor, como responsable del tratamiento, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicho tratamiento cumple los requisitos de la Directiva 95/46, para que las garantías que ella establece puedan tener pleno efecto.

84 A este respecto, cabe señalar que, habida cuenta de la facilidad con que la información publicada en un sitio de Internet puede ser copiada en otros sitios y de que los responsables de su publicación no están siempre sujetos al Derecho de la Unión, no podría llevarse a cabo una protección eficaz y completa de los interesados si éstos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de sitios de Internet.

85 Además, el tratamiento por parte del editor de una página web, que consiste en la publicación de información relativa a una persona física, puede, en su caso, efectuarse «con fines exclusivamente periodísticos» y beneficiarse, de este modo, en virtud del artículo 9 de la Directiva 95/46, de las excepciones a los requisitos que ésta establece, mientras que ése no es el caso en el supuesto del tratamiento que lleva a cabo el gestor de un motor de búsqueda. De este modo, no puede excluirse que el interesado pueda en determinadas circunstancias ejercer los derechos recogidos en los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 contra el gestor, pero no contra el editor de dicha página web.

86 Por último, debe observarse que no sólo la razón que justifica, en virtud del artículo 7 de la Directiva 95/46, la publicación de un dato personal en un sitio de Internet no coincide forzosamente con la que se aplica a la actividad de los motores de búsqueda, sino que, aun cuando éste sea el caso, el resultado de la ponderación de los intereses en conflicto que ha de llevarse a cabo en virtud de los artículos 7, letra f), y 14, párrafo primero, letra a), de la mencionada Directiva puede divergir en función de que se trate de un tratamiento llevado a cabo por un gestor de un motor de búsqueda o por el editor de esta página web, dado que, por un lado, los intereses legítimos que justifican estos tratamientos pueden ser diferentes, y, por otro, las consecuencias de estos tratamientos sobre el interesado, y, en particular, sobre su vida privada, no son necesariamente las mismas.

87 En efecto, en la medida en que la inclusión, en la lista de resultados obtenida tras una búsqueda llevada a cabo a partir del nombre de una persona, de una página web y de información contenida en ella relativa a esta persona facilita sensiblemente la accesibilidad de dicha información a cualquier internauta que lleve a cabo una búsqueda sobre el interesado y puede desempeñar un papel decisivo para la difusión de esta información, puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página web.

88 A la luz del conjunto de consideraciones precedentes procede responder a la segunda cuestión prejudicial, letras c) y d), que los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.

Sobre la tercera cuestión prejudicial, relativa al alcance de los derechos del interesado garantizados por la Directiva 95/46

89 Mediante su tercera cuestión prejudicial, el tribunal remitente desea saber, en esencia, si los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que permiten al interesado exigir al gestor de un motor de búsqueda eliminar de la lista de resultados obtenida como consecuencia de una búsqueda efectuada a partir de su nombre vínculos a páginas web, publicadas legalmente por terceros y que contienen datos e información verídicos relativos a su persona, debido a que estos datos e información pueden perjudicarle o que desee que estos datos e información se «olviden» tras un determinado lapso de tiempo.

90 Google Spain, Google Inc., los Gobiernos helénico, austriaco y polaco y la Comisión consideran que debe darse una respuesta negativa a esta cuestión. Google Spain, Google Inc., el Gobierno polaco y la Comisión alegan a este respecto que los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 confieren derechos a los interesados únicamente a condición de que el tratamiento controvertido sea incompatible con dicha Directiva o por razones legítimas propias de su situación particular, y no por la mera razón de que consideren que este tratamiento puede perjudicarles o deseen que los datos objeto de ese tratamiento caigan en el olvido. Los Gobiernos helénico y austriaco consideran que el interesado debe dirigirse al editor del sitio de Internet de que se trate.

91 El Sr. Costeja González y los Gobiernos español e italiano son de la opinión de que el interesado puede oponerse a la indexación de sus datos personales por un motor de búsqueda cuando la difusión de estos datos por la intermediación de éste le perjudica y de que sus derechos fundamentales a la protección de dichos datos y de respeto a la vida privada, que engloban el «derecho al olvido», prevalecen sobre los intereses legítimos del gestor de dicho motor y el interés general en la libertad de información.

92 En relación con el artículo 12, letra b), de la Directiva 95/46, cuya aplicación está sometida al requisito de que el tratamiento de datos personales sea incompatible con dicha Directiva, es necesario recordar que, como se ha señalado en el apartado 72 de la presente sentencia, tal incompatibilidad puede resultar no sólo de que los datos sean inexactos, sino en particular, de que sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, de que no estén actualizados o de que se conserven durante un período superior al necesario, a menos que se imponga su conservación por fines históricos, estadísticos o científicos.

93 Se deduce de estos requisitos, establecidos en el artículo 6, apartado 1, letras c) a e), de la Directiva 95/46, que incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Éste es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido.

94 Por consiguiente, en el supuesto en el que se aprecie, tras una solicitud del interesado en virtud del artículo 12, letra b), de la Directiva 95/46, que la inclusión en la lista de resultados obtenida como consecuencia de una búsqueda efectuada a partir de su nombre, de vínculos a páginas web, publicadas legalmente por terceros y que contienen datos e información verídicos relativos a su persona, es, en la situación actual, incompatible con dicho artículo 6, apartado 1, letras c) a e), debido a que esta información, habida cuenta del conjunto de las circunstancias que caracterizan el caso de autos, es inadecuada, no es pertinente, o ya no lo es, o es excesiva en relación con los fines del tratamiento en cuestión realizado por el motor de búsqueda, la información y los vínculos de dicha lista de que se trate deben eliminarse.

95 En lo que atañe a las solicitudes en el sentido de este artículo 12, letra b), basadas en el supuesto incumplimiento de los requisitos establecidos en el artículo 7, letra f), de la Directiva 95/46 y con arreglo al artículo 14, párrafo primero, letra a), de dicha Directiva, ha de señalarse que cada tratamiento de datos personales debe ser legítimo, en virtud del artículo 7, durante todo el período en el que se efectúa.

96 Visto lo que antecede, al apreciar tales solicitudes presentadas contra un tratamiento como el controvertido en el litigio principal, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre. A

este respecto, cabe señalar que la apreciación de la existencia de tal derecho no presupone que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado.

97 Ya que el interesado puede, habida cuenta de sus derechos con arreglo a los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, es necesario considerar, como se desprende, en particular, del apartado 81 de la presente sentencia, que estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.

98 En relación con una situación como la del litigio principal, que se refiere a la presentación, en la lista de resultados que el internauta obtiene al efectuar una búsqueda a partir del nombre del interesado con ayuda de Google Search, de vínculos a dos páginas de archivos en línea de un periódico que contienen anuncios que mencionan el nombre de esta persona y relativos a una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social, es preciso considerar que, teniendo en cuenta el carácter sensible de la información contenida en dichos anuncios para la vida privada de esta persona y de que su publicación inicial se remonta a 16 años atrás, el interesado justifica que tiene derecho a que esta información ya no se vincule a su nombre mediante esa lista. Por tanto, en la medida en que en el caso de autos no parece existir razones concretas que justifiquen un interés preponderante del público en tener acceso a esta información en el marco de tal búsqueda, lo que no obstante incumbe comprobar al órgano jurisdiccional remitente, el interesado puede, en virtud de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, exigir que se eliminen estos vínculos de la lista de resultados.

99 De las consideraciones anteriores se desprende que procede responder a la tercera cuestión prejudicial que los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.

COSTAS

100 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante el órgano jurisdiccional nacional, corresponde a éste resolver sobre las costas. Los gastos efectuados al presentar observaciones ante el Tribunal de Justicia, distintos de aquellos en que hayan incurrido dichas partes, no pueden ser objeto de reembolso.

En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara:

1) El artículo 2, letras b) y d), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que, por un lado, la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un

orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del mencionado artículo 2, letra d).

2) **El artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.**

3) **Los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.**

4) **Los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.**

Firmas

SENTENCIA DEL TRIBUNAL DE JUSTICIA (GRAN SALA)

de 6 de octubre de 2015 (*)

«Procedimiento prejudicial — Datos personales — Protección de las personas físicas frente al tratamiento de esos datos — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8 y 47 — Directiva 95/46/CE — Artículos 25 y 28 — Transferencia de datos personales a países terceros — Decisión 2000/520/CE — Transferencia de datos personales a Estados Unidos — Nivel de protección inadecuado — Validez — Reclamación de una persona física cuyos datos han sido transferidos desde la Unión Europea a Estados Unidos — Facultades de las autoridades nacionales de control»

En el asunto C-362/14,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la High Court (Irlanda), mediante resolución de 17 de julio de 2014, recibida en el Tribunal de Justicia el 25 de julio de 2014, en el procedimiento entre

Maximillian Schrems

y

Data Protection Commissioner,

con intervención de:

Digital Rights Ireland Ltd,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. V. Skouris, Presidente, el Sr. K. Lenaerts, Vicepresidente, el Sr. A. Tizzano, la Sra. R. Silva de Lapuerta, los Sres. T. von Danwitz (Ponente) y S. Rodin y la Sra. K. Jürimäe, Presidentes de Sala, y los Sres. A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský y D. Šváby, la Sra. M. Berger y los Sres. F. Biltgen y C. Lycourgos, Jueces;

Abogado General: Sr. Y. Bot;

Secretario: Sra. L. Hewlett, administradora principal;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 24 de marzo de 2015;

consideradas las observaciones presentadas:

- en nombre del Sr. Schrems, por el Sr. N. Travers, SC, el Sr. P. O'Shea, BL, el Sr. G. Rudden, Solicitor, y el Sr. H. Hofmann, Rechtsanwalt;
- en nombre del Data Protection Commissioner, por el Sr. P. McDermott, BL, la Sra. S. More O'Ferrall y el Sr. D. Young, Solicitors;
- en nombre de Digital Rights Ireland Ltd, por el Sr. F. Crehan, BL, y los Sres. S. McGarr y E. McGarr, Solicitors;
- en nombre de Irlanda, por los Sres. A. Joyce y B. Counihan y la Sra. E. Creedon, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;
- en nombre del Gobierno belga, por el Sr. J.-C. Halleux y la Sra. C. Pochet, en calidad de agentes;
- en nombre del Gobierno checo, por los Sres. M. Smolek y J. Vláčil, en calidad de agentes;
- en nombre del Gobierno italiano, por la Sra. G. Palmieri, en calidad de agente, asistida por el Sr. P. Gentili, avvocato dello Stato;
- en nombre del Gobierno austriaco, por los Sres. G. Hesse y G. Kunnert, en calidad de agentes;
- en nombre del Gobierno polaco, por las Sras. M. Kamejsza y M. Pawlicka y el Sr. B. Majczyna, en calidad de agentes;
- en nombre del Gobierno esloveno, por las Sras. A. Grum y V. Klemenc, en calidad de agentes;
- en nombre del Gobierno del Reino Unido, por el Sr. L. Christie y la Sra. J. Beeko, en calidad de agentes, asistidos por el Sr. J. Holmes, Barrister;

- en nombre del Parlamento Europeo, por los Sres. D. Moore y A. Caiola y la Sra. M. Pencheva, en calidad de agentes;
- en nombre de la Comisión Europea, por los Sres. B. Schima, B. Martenczuk y B. Smulders y la Sra. J. Vondung, en calidad de agentes;
- en nombre del Supervisor Europeo de Protección de Datos (SEPD), por los Sres. C. Docksey, A. Buchta y V. Pérez Asinari, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 23 de septiembre de 2015;

dicta la siguiente

SENTENCIA

1 La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), de los artículos 25, apartado 6, y 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), en su versión modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003 (DO L 284, p. 1) (en lo sucesivo, «Directiva 95/46»), así como, en sustancia, la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, p. 7).

2 Esa petición se ha presentado en el marco de un litigio entre el Sr. Schrems y el Data Protection Commissioner (comisario para la protección de datos; en lo sucesivo, «comisario»), acerca de la negativa de éste a instruir una reclamación presentada por el Sr. Schrems, basada en que Facebook Ireland Ltd (en lo sucesivo, «Facebook Ireland») transfiere a Estados Unidos los datos personales de sus usuarios y los conserva en sus servidores situados en ese país.

MARCO JURÍDICO

Directiva 95/46

3 Los considerandos 2, 10, 56, 57, 60, 62 y 63 de la Directiva 95/46 están así redactados:

«(2) [...] los sistemas de tratamiento de datos están al servicio del hombre; [...] deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la [vida privada], y contribuir [...] al bienestar de los individuos;

[...]

(10) [...] las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[, firmado en Roma el 4 de noviembre de 1950], así como en los principios generales del Derecho comunitario; [...] por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

[...]

(56) [...] los flujos transfronterizos de datos personales son necesarios para [el] desarrollo del comercio internacional; [...] la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; [...] el carácter adecuado del nivel de protección

ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;

(57) [...] por otra parte, [...] cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

[...]

(60) [...] en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, y, en particular, de su artículo 8;

[...]

(62) [...] la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;

(63) [...] dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; [...]»

4 Los artículos 1, 2, 25, 26, 28 y 31 de la Directiva 95/46 disponen:

«Artículo 1

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la [vida privada], en lo que respecta al tratamiento de los datos personales.

[...]

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

a) "datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

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

[...]

d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

[...]

Artículo 25

Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.
3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.
4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.
5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.
6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26

Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:
   a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
   b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
   c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
   d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
   e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

[...]

Artículo 28

Autoridad de control

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control,
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales,
- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o [capacidad para] poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

[...]

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

[...]

Artículo 31

[...]

2. En los casos en que se haga referencia al presente artículo, serán de aplicación los artículos 4 y 7 de la Decisión 1999/468/CE [del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión (DO L 184, p. 23)], observando lo dispuesto en su artículo 8.

[...]»

Decisión 2000/520

5 La Decisión 2000/520 fue adoptada por la Comisión con fundamento en el artículo 25, apartado 6, de la Directiva 95/46.

6 Los considerandos 2, 5 y 8 de esa Decisión están así redactados:

«(2) La Comisión puede determinar que un tercer país garantiza un nivel de protección adecuado. En tal caso, pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional.

[...]

(5) El nivel adecuado de protección de la transferencia de datos desde la Comunidad a Estados Unidos de América, reconocido por la presente Decisión, debe alcanzarse si las entidades cumplen los principios de puerto seguro para la protección de la vida privada, con objeto de proteger los datos personales transferidos de un Estado miembro a Estados Unidos de América (en lo sucesivo denominados "los principios"), así [como] las preguntas más frecuentes (en lo sucesivo denominadas "FAQ"), en las que se proporciona orientación para aplicar los principios, publicadas por el Gobierno de Estados Unidos de América con fecha 21 de julio de 2000. Además, las entidades deben dar a conocer públicamente sus políticas de protección de la vida privada y someterse a la jurisdicción de la Federal Trade Commission (Comisión Federal de Comercio, FTC) a tenor de lo dispuesto en el artículo 5 de la Federal Trade Commission Act, en la que se prohíben actos o prácticas desleales o fraudulentas en el comercio o en relación con él, o a la jurisdicción de otros organismos públicos que garanticen el cumplimiento efectivo de los principios y su aplicación de conformidad con las FAQ.

[...]

(8) Aunque se compruebe el nivel adecuado de la protección, por motivos de transparencia y para proteger la capacidad de las autoridades correspondientes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar en la presente Decisión las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información.»

7 A tenor de los artículos 1 a 4 de la Decisión 2000/520:

«Artículo 1

1. A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, para todas las actividades cubiertas por la misma, se considerará que los principios de puerto seguro (en lo sucesivo denominados "los principios"), que figuran en el anexo I de la presente Decisión, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes (en lo sucesivo denominadas "FAQ") publicadas por el Departamento de Comercio de Estados Unidos de América con fecha 21 de julio de 2000, que figuran en el anexo II de la presente Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a entidades establecidas en Estados Unidos de América, habida cuenta de los siguientes documentos publicados por el Departamento de Comercio de Estados Unidos de América:

   a) Estudio de aplicación, que figura en el anexo III;

   b) Memorando sobre daños y perjuicios por violación de la vida privada y autorizaciones explícitas en la legislación estadounidense, que figura en el anexo IV;

   c) Carta de la Comisión Federal de Comercio, que figura en el anexo V;

   d) Carta del Departamento estadounidense de Transporte, que figura en el anexo VI.

2. En relación con cada transferencia de datos deberán cumplirse las condiciones siguientes:

   a) la entidad receptora de los datos deberá haber manifestado de forma inequívoca y pública su compromiso de cumplir los principios aplicados de conformidad con las FAQ;

   b) la entidad estará sujeta a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el anexo VII de la presente Decisión, que estará facultado para investigar las quejas que se presenten y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como reparaciones para los particulares, independientemente de su país de residencia o de su nacionalidad, en caso de incumplimiento de los principios y su aplicación de conformidad con las FAQ.

3. Se considerará que la entidad que autocertifica su adhesión a los principios y su aplicación de conformidad con las FAQ cumple las condiciones mencionadas en el apartado 2 a partir de la fecha en que notifique al Departamento de Comercio de Estados Unidos de América o a su representante el compromiso a que se refiere la letra a) del apartado 2, así como la identidad del organismo público a que se refiere la letra b) del apartado 2.

Artículo 2

La presente Decisión se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE, y no afecta a la aplicación de las demás disposiciones de dicha Directiva [correspondientes] al tratamiento de datos personales en los Estados miembros, y en particular a su artículo 4.

Artículo 3

1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos siguientes:

   a) el organismo público de Estados Unidos de América contemplado en el anexo VII de la presente Decisión, o un [órgano] independiente de recurso, a efectos de la letra a) del principio de aplicación, que figura en el anexo I de la presente Decisión, ha resuelto que la entidad ha vulnerado los principios y su aplicación de conformidad con las FAQ; o

   b) existen grandes probabilidades de que se estén vulnerando los principios; existen razones para creer que el [órgano] de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las

autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad y proporcionarle la oportunidad de alegar.

La suspensión cesará en cuanto esté garantizado el cumplimiento de los principios y su aplicación de conformidad con las FAQ y las autoridades correspondientes de la Unión Europea hayan sido notificadas de ello.

2. Los Estados miembros informarán a la Comisión a la mayor brevedad de la adopción de medidas con arreglo al apartado 1.

3. Asimismo, los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no garantice dicho cumplimiento.

4. Si la información recogida con arreglo a los apartados 1 a 3 demuestra que un organismo responsable del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no está ejerciendo su función, la Comisión lo notificará al Departamento de Comercio de Estados Unidos de América y, si procede, presentará un proyecto de medidas con arreglo al procedimiento que establece el artículo 31 de la Directiva, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.

Artículo 4

1. La presente Decisión podrá adaptarse en cualquier momento de conformidad con la experiencia resultante de su aplicación o si el nivel de protección establecido por los principios y las FAQ es superado por los requisitos de la legislación estadounidense.

La Comisión analizará en todo caso, basándose en la información disponible, la aplicación de la presente Decisión tres años después de su notificación a los Estados miembros e informará de cualquier resultado pertinente al Comité previsto en el artículo 31 de la Directiva 95/46/CE, en particular de toda prueba que pueda afectar a la evaluación de que las disposiciones del artículo 1 de la presente Decisión proporcionan protección adecuada a efectos del artículo 25 de la Directiva 95/46/CE y de toda prueba de que la presente Decisión se está aplicando de forma discriminatoria.

2. La Comisión presentará, si procede, proyectos de medidas de conformidad con el procedimiento establecido en el artículo 31 de la Directiva 95/46/CE.»

8 El anexo I de la Decisión 2000/520 tiene la siguiente redacción:

«Principios de puerto seguro (protección de la vida privada)

Publicados por el Departamento de Comercio de Estados Unidos de América el 21 de julio de 2000

[...]

[...] el Departamento Federal de Comercio publica el presente documento más las preguntas más frecuentes ("los principios"), o FAQ, en su calidad de autoridad competente para estimular, fomentar y desarrollar el comercio internacional. Dichos principios se formularon en consulta con la industria y la opinión pública para facilitar el comercio y las transacciones entre Estados Unidos de América y la Unión Europea. Son de utilización exclusiva de las entidades estadounidenses que reciben datos personales de la Unión Europea, al efecto de reunir los requisitos de "puerto seguro" y obtener la correspondiente presunción de "adecuación". Puesto que los principios se concibieron exclusivamente para lograr este objetivo concreto, resultaría impropia su utilización con otros fines.
[...]

La decisión de adherirse a los requisitos de "puerto seguro" es totalmente voluntaria, pero éstos pueden cumplirse de distintas maneras [...]

La adhesión a estos principios puede limitarse: a) [en] cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]; b) por disposición legal o reglamentaria, o jurisprudencia, que originen conflictos de obligaciones o autorizaciones [explícitas], siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar

los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables. A fin de ser coherentes con el objetivo de mejorar la protección de la vida privada, las entidades deberán esforzarse en aplicar estos principios de manera completa y transparente, lo que incluye indicar en sus políticas de protección de la vida privada cuándo se aplicarán de manera regular las limitaciones a los principios permitidas por la anterior letra b). Por esta misma razón, cuando se permita la opción a tenor de los principios y/o de la legislación de Estados Unidos de América, se espera que las entidades opten por el mayor nivel de protección posible.

[...]»

9 El anexo II de la Decisión 2000/520 está redactado como sigue:

«Preguntas más frecuentes (FAQ)

[...]

FAQ nº 6 — Autocertificación

P: *¿De qué modo una entidad autocertifica su adhesión a los principios de puerto seguro?*

R: Los beneficios del puerto seguro se garantizan desde la fecha en que una entidad autocertifica ante el Departamento de Comercio, o su representante, su adhesión a los principios de conformidad con las directrices que se indican a continuación.

Para proceder a la autocertificación, las entidades pueden proporcionar al Departamento de Comercio (o a su representante) una carta firmada por uno de los responsables de la empresa en nombre de la entidad que se adhiere al puerto seguro, que contendrá cuando menos la información siguiente:

1) nombre de la entidad, señas postales y de correo electrónico, teléfono y fax;

2) descripción de las actividades de la entidad en lo relativo a la información personal recibida de la Unión Europea; y

3) descripción de su política de protección de la vida privada respecto de dicha información personal, con indicación de: a) el lugar donde puede consultarla el público; b) la fecha de entrada en vigor de dicha política; c) una oficina de contacto para la tramitación de las quejas, las solicitudes de acceso y cualquier otra cuestión relacionada con los principios de puerto seguro; d) el organismo oficial concreto con jurisdicción para entender de cualquier queja contra la entidad por posibles prácticas desleales o fraudulentas y vulneraciones de las leyes o normas sobre la vida privada (y citado en el anexo de los principios); e) el nombre de los programas de protección de la vida privada a los que esté adscrita la entidad; f) el método de verificación (por ejemplo, interna, por terceros) [...]; y g) la instancia independiente de recurso que se ocupará de investigar las quejas no resueltas.

Si la entidad desea que los beneficios del puerto seguro se apliquen a la información sobre recursos humanos transferida desde la Unión Europea para usarla en el contexto de la relación laboral, puede hacerlo siempre que exista un organismo oficial con jurisdicción para entender de cualquier queja contra la entidad provocada por información sobre recursos humanos citado en el anexo de los principios. [...]

El Departamento (o su representante) llevará una lista de las entidades que presenten dichas cartas, dispensándoles por consiguiente los beneficios del puerto seguro. Asimismo, actualizará la lista con las cartas anuales y las notificaciones recibidas de conformidad con la FAQ nº 11. [...]

[...]

FAQ nº 11 — Resolución de litigios y ejecución

P: *¿Cómo deberán cumplirse los requisitos de resolución de litigios impuestos por el principio de aplicación y cómo se deberá actuar ante el caso de que una entidad incumpla sistemáticamente los principios?*

R: El principio de aplicación establece los requisitos en virtud de los cuales se regulan los mecanismos de aplicación del puerto seguro. La FAQ sobre verificación (FAQ nº 7) establece la forma de reunir los requisitos de la letra b) del principio. En la presente FAQ nº 11 se abordan las letras a) y c), que requieren instancias independientes de recurso. Dichas instancias pueden adoptar formas diversas, pero siempre deben reunir los requisitos exigidos por el principio de aplicación. Las entidades podrán cumplirlos de la manera siguiente: 1) conformidad con programas de protección de la vida privada concebidos por el sector privado que incorporen los principios de puerto seguro en sus normas y cuenten con mecanismos de aplicación eficaces, similares a los descritos en el principio de aplicación; 2) conformidad con lo dispuesto por las autoridades de control establecidas legal o reglamentariamente [encargadas de] la tramitación de las quejas individuales y la resolución de litigios; o 3) compromiso de colaboración con las autoridades de protección de datos establecidas en la Comunidad Europea o sus representantes autorizados. Esta lista se ofrece a título ilustrativo y no es de ninguna manera taxativa. El sector privado puede crear otros mecanismos de aplicación, siempre que reúnan los requisitos contemplados en el principio de aplicación y en las FAQ. Obsérvese que los requisitos del principio de aplicación se añaden al requisito expuesto en el apartado 3 de la introducción a los principios, en el sentido de que las iniciativas autorreguladoras deberán ser vinculantes con arreglo al artículo 5 de la Federal Trade Commission Act (Ley de la Comisión Federal de Comercio) o legislación similar.

Instancias de recurso

Se alentará a los consumidores a presentar cualquier queja que tengan ante la entidad correspondiente antes de acudir a las instancias de recurso independientes. [...]

[...]

Recurso ante la FTC

La FTC se ha comprometido a tramitar prioritariamente los casos presentados por los organismos de autorregulación privados, como BBBOnline y TRUSTe, y [por] los Estados miembros de la Unión Europea que aleguen el incumplimiento de los principios de puerto seguro, a fin de determinar si se ha vulnerado el artículo 5 de la Ley FTC, por la que se prohíben los actos o prácticas desleales o fraudulentos en el comercio. [...]

[...]»

10 A tenor del anexo IV de la Decisión 2000/520:

«Memorando sobre [indemnización] por violación de las reglas sobre protección de la [vida privada], autorizaciones explícitas y fusiones y absorciones en el Derecho estadounidense

Este documento viene a responder a las aclaraciones solicitadas por la Comisión Europea sobre la legislación estadounidense en materia de: a) demandas de indemnización de daños y perjuicios por violación del derecho [al respeto de la vida privada], b) "autorizaciones explícitas" para la utilización de datos personales sin atenerse a los principios [...] de puerto seguro y c) efectos de las fusiones y absorciones sobre las obligaciones contraídas en virtud de dichos principios.

[...]

B. Autorizaciones legales explícitas

Los principios de puerto seguro recogen una excepción cuando las normas legales o reglamentarias o la jurisprudencia crean "obligaciones en contrario o autorizaciones explícitas, siempre que en el ejercicio de tal autorización la entidad acredite que el incumplimiento de dichos principios se limita a lo necesario para satisfacer los intereses legítimos que tal autorización considera deben prevalecer". Es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro. Con respecto a las autorizaciones explícitas, aunque estos principios tienen como finalidad salvar las diferencias entre los regímenes estadounidense y europeo de protección de la [vida privada], debemos respetar las facultades legislativas de nuestros legisladores. Esta limitada excepción del cumplimiento estricto de los principios de puerto seguro trata de encontrar un equilibrio entre los intereses legítimos de cada parte.

La excepción se circunscribe a los casos en los que haya una autorización explícita. Por tanto, como cuestión de partida, la norma legal o reglamentaria o la resolución judicial en cuestión debe autorizar expresamente la conducta concreta de las entidades adheridas a los principios de puerto seguro. [Con otras palabras, la excepción no será aplicable si la ley guarda silencio]. [Además,] la excepción sólo será aplicable si la autorización explícita entra en conflicto con el cumplimiento de dichos principios. Aun en tal caso, la excepción "está limitada a lo necesario para satisfacer los intereses legítimos que tal autorización considera deben prevalecer". A modo de ejemplo, si la Ley se limita a autorizar a una empresa a proporcionar datos personales a las autoridades públicas, la excepción no sería de aplicación. Por el contrario, si la Ley autoriza expresamente a la empresa a proporcionar información personal a organismos oficiales sin el consentimiento del interesado, esto constituiría una "autorización explícita" para actuar de modo contrario a lo establecido en los principios de puerto seguro. Por su parte, las excepciones concretas a los requisitos expresos de notificar y prestar consentimiento caerían en el ámbito de la excepción (dado que sería equivalente a una autorización explícita a revelar los datos sin notificación ni consentimiento). Por ejemplo, una ley que autorice a los médicos a proporcionar los historiales médicos de sus pacientes a las autoridades sanitarias sin el previo consentimiento de éstos puede permitir una excepción de los principios de notificación y opción. Esta autorización no permitiría al médico entregar estos mismos historiales a las organizaciones de protección de la salud o los laboratorios farmacéuticos comerciales, que quedarían fuera del ámbito de los fines autorizados por la ley y, por tanto, de la excepción.[...]. La autorización legal en cuestión puede ser una autorización "aislada" para hacer determinadas cosas con los datos personales, pero, como ilustran los ejemplos siguientes, será probablemente una excepción a una norma más amplia que prohíba obtener, utilizar o revelar datos personales.

[...]»

Comunicación COM(2013) 846

11 El 27 de noviembre de 2013 la Comisión adoptó la Comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU» [COM(2013) 846 final; en lo sucesivo, «Comunicación COM(2013) 846 final»]. Acompañaba a esa Comunicación un informe, también de fecha 27 de noviembre de 2013, que contiene las «conclusiones de los copresidentes de la Unión Europea del grupo de trabajo *ad hoc* Unión Europea-Estados Unidos sobre protección de datos personales» («Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»). Como expone su punto 1, ese informe se había elaborado en cooperación con Estados Unidos a raíz de la revelación de la existencia en ese país de varios programas de vigilancia que comprendían la recogida y el tratamiento de información a gran escala de datos personales. Ese informe contenía, en particular, un análisis detallado del ordenamiento jurídico de Estados Unidos en lo que concierne especialmente a las bases legales que autorizan la existencia de programas de vigilancia y la recogida y el tratamiento de datos personales por autoridades estadounidenses.

12 En el punto 1 de la Comunicación COM(2013) 846 final la Comisión precisó que «los intercambios comerciales son objeto de la Decisión [2000/520]», y añadió que «dicha Decisión establece una base jurídica para la transferencia de datos personales desde la UE a las empresas establecidas en Estados Unidos que se han adherido a los principios del régimen de puerto seguro.» Además, en ese mismo punto 1 la Comisión puso énfasis en la creciente importancia de los flujos de datos personales, ligada en especial al desarrollo de la economía digital, que «ha dado lugar a un crecimiento exponencial de la cantidad, calidad, diversidad y naturaleza de las actividades de tratamiento de datos».

13 En el punto 2 de esa Comunicación la Comisión manifiesta que «ha aumentado la preocupación por el nivel de protección de los datos personales de los ciudadanos de la [Unión] transferidos a Estados Unidos en el marco del régimen de puerto seguro» y que «el carácter voluntario y declarativo del régimen ha centrado la atención en su transparencia y cumplimiento.»

14 Además, la Comisión expuso en el referido punto 2 que «las autoridades estadounidenses pueden acceder y seguir tratando los datos personales de los ciudadanos de la [Unión] enviados a Estados Unidos en el marco del régimen de puerto seguro de forma incompatible con los motivos por los que se recogieron inicialmente dichos datos en la [Unión] y con los fines por los que se transfirieron a Estados Unidos» y que «la mayoría de las empresas estadounidenses de internet relacionadas

más directamente con [los] programas [de vigilancia] están certificadas en el marco del régimen de puerto seguro.»

15 En el punto 3.2 de la Comunicación COM(2013) 846 final la Comisión señaló la existencia de diversas deficiencias en la aplicación de la Decisión 2000/520. Puso de manifiesto que algunas empresas estadounidenses certificadas no respetaban los principios enunciados en el artículo 1, apartado 1, de la Decisión 2000/520 (en lo sucesivo, «principios de puerto seguro»), y que, mediante mejoras de esa Decisión, «deben subsanarse las deficiencias estructurales relacionadas con la transparencia y la aplicación y deben reforzarse los principios sustantivos del régimen de puerto seguro y la aplicación de la excepción por motivos de seguridad nacional». Por otra parte, observó que «el régimen de puerto seguro sirve asimismo de interfaz para la transferencia de los datos personales de los ciudadanos [europeos] desde la [Unión Europea] a los Estados Unidos por parte de las empresas [a] las que se pide que suministren datos a los servicios de información de los Estados Unidos en el marco de los programas de recogida de información de los Estados Unidos».

16 La Comisión concluyó en ese mismo punto 3.2 que, «habida cuenta de las deficiencias halladas, no puede mantenerse la aplicación actual del régimen de puerto seguro. Sin embargo, su derogación afectaría negativamente a los intereses de las empresas de la [Unión Europea] y de los Estados Unidos que se han adherido al mismo.». Finalmente, la Comisión añadió también en el mismo punto 3.2 que «con carácter de urgencia, la Comisión debatirá con las autoridades de Estados Unidos las deficiencias detectadas».

Comunicación COM(2013) 847

17 El mismo día 27 de noviembre de 2013 la Comisión adoptó la Comunicación al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE [COM(2013) 847 final; en lo sucesivo, «Comunicación COM(2013) 847 final»]. Según resulta de su punto 1, esa Comunicación se basa en particular en las informaciones recibidas por el Grupo de trabajo *ad hoc* Unión Europea-Estados Unidos y constituye la continuación de los dos informes de evaluación de la Comisión, publicados respectivamente en 2002 y en 2004.

18 El punto 1 de esa Comunicación precisa que el funcionamiento de la Decisión 2000/520 «se basa en los compromisos y la autocertificación de las entidades que lo han suscrito» y añade que «si bien la firma de estos acuerdos es voluntaria, sus reglas son vinculantes para los que los suscriben».

19 Además, del punto 2.2 de la Comunicación COM(2013) 847 final resulta que, a 26 de septiembre de 2013, estaban certificadas 3 246 entidades de numerosas industrias y sectores de servicios. Esas empresas prestaban principalmente servicios en el mercado interior de la Unión, en particular en el sector de Internet, y algunas de ellas eran empresas de la Unión que tenían filiales en Estados Unidos. Parte de esas empresas trataban los datos de sus empleados en Europa, datos que transferían a Estados Unidos para la gestión de sus recursos humanos.

20 En ese mismo punto 2.2 la Comisión puso de relieve que «cualquier fallo en la transparencia o en la aplicación por parte estadounidense [hacía] que la responsabilidad [pasara] a las autoridades de protección de datos y las empresas europeas que utilizan el sistema».

21 De los puntos 3 a 5 y 8 de la Comunicación COM(2013) 847 final se deduce que en la práctica un número elevado de empresas certificadas no respetaban, o no lo hacían plenamente, los principios de puerto seguro.

22 Además, en el punto 7 de la misma Comunicación la Comisión manifiesta que «aparentemente todas las empresas involucradas en el programa PRISM [programa de recogida de informaciones a gran escala], y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro» y que ello «ha hecho de puerto seguro uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la [Unión]». En ese sentido, la Comisión constató en el punto 7.1 de la referida Comunicación que «diversas bases legales con arreglo al ordenamiento jurídico estadounidense permiten la recogida y el tratamiento a gran escala de datos personales almacenados o tratados de otra forma por entidades basadas en Estados Unidos» y que «al tratarse de programas a gran escala, puede ocurrir que las

autoridades estadounidenses accedan y procesen los datos transferidos al amparo del puerto seguro más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional, como reza la excepción prevista en la Decisión [2000/520].»

23 En el punto 7.2 de la Comunicación COM(2013) 847 final, titulado «Limitaciones y posibilidades de reparación», la Comisión puso de relieve que «las garantías previstas por la legislación estadounidense se refieren fundamentalmente a los ciudadanos estadounidenses o a los residentes legales», y que «es más, no está prevista la posibilidad de que los titulares de los datos, ya sean estadounidenses o de la [Unión], puedan acceder a sus datos, rectificarlos o suprimirlos, ni obtener reparación administrativa o judicial, en lo que respecta a la recogida y el tratamiento posterior de sus datos personales en virtud de los programas de vigilancia estadounidenses».

24 Según el punto 8 de la Comunicación COM(2013) 847 final, entre las empresas certificadas se encontraban «las empresas de la red, como Google, Facebook, Microsoft, Apple o Yahoo», que «tienen centenares de millones de clientes en Europa» y transfieren datos personales a Estados Unidos para su tratamiento.

25 La Comisión concluyó en ese mismo punto 8 que «el acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por entidades con certificación de puerto seguro suscita serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país».

LITIGIO PRINCIPAL Y CUESTIONES PREJUDICIALES

26 El Sr. Schrems, nacional austriaco residente en Austria, es usuario de la red Facebook (en lo sucesivo, «Facebook») desde 2008.

27 Toda persona residente en el territorio de la Unión que desee utilizar Facebook está obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento.

28 El 25 de junio de 2013 el Sr. Schrems presentó ante el comisario una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency (en lo sucesivo, «NSA»).

29 Considerando que no estaba obligado a investigar sobre los hechos denunciados por el Sr. Schrems en su reclamación, el comisario la desestimó por infundada. Apreció en efecto que no había pruebas de que la NSA hubiera accedido a los datos personales del interesado. El comisario añadió que las imputaciones formuladas por el Sr. Schrems en su reclamación no podían ser eficazmente aducidas, ya que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión 2000/520, en la que la Comisión había constatado que Estados Unidos garantizaba un nivel adecuado de protección.

30 El Sr. Schrems interpuso un recurso ante la High Court contra la decisión discutida en el litigio principal. Una vez examinadas las pruebas presentadas por las partes litigantes, ese tribunal apreció que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la Unión a Estados Unidos servían a finalidades necesarias e indispensables para el interés público. No obstante, el referido tribunal añadió que las revelaciones del Sr. Snowden habían demostrado que la NSA y otros organismos federales habían cometido «importantes excesos».

31 Ahora bien, según ese mismo tribunal, los ciudadanos de la Unión no disponen de ningún derecho efectivo a ser oídos. La supervisión de las acciones de los servicios de información se realiza a través de un procedimiento secreto y no contradictorio. Una vez transferidos los datos personales a Estados Unidos, la NSA y otros organismos federales, como el Federal Bureau of Investigation (FBI),

pueden acceder a ellos en el contexto de la vigilancia y de las interceptaciones indiferenciadas que ejecutan a gran escala.

32 La High Court constató que el Derecho irlandés prohíbe la transferencia de datos personales fuera del territorio nacional, excepto cuando el tercer país interesado asegura un nivel de protección adecuado de la vida privada y de los derechos y libertades fundamentales. La importancia de los derechos al respeto de la vida privada y a la inviolabilidad del domicilio, protegidos por la Constitución irlandesa, exige que toda injerencia en esos derechos sea proporcionada y ajustada a las exigencias previstas por la ley.

33 Ahora bien, el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa. Para que las interceptaciones de comunicaciones electrónicas puedan ser consideradas conformes con esa Constitución, debe aportarse la prueba de que esas interceptaciones tienen carácter selectivo, de que la vigilancia de determinadas personas o de determinados grupos de personas está objetivamente justificada en interés de la seguridad nacional o de la represión de la delincuencia y de que existen garantías adecuadas y comprobables. Así pues, según la High Court, si el asunto principal se tuviera que resolver con fundamento exclusivo en el Derecho irlandés, se debería apreciar que, dada la existencia de serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, el comisario habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente.

34 No obstante, la High Court estima que este asunto atañe a la aplicación del Derecho de la Unión, en el sentido del artículo 51 de la Carta, por lo que la legalidad de la decisión discutida en el asunto principal debe apreciarse a la luz del Derecho de la Unión. Ahora bien, según ese tribunal, la Decisión 2000/520 no se ajusta a las exigencias derivadas tanto de los artículos 7 y 8 de la Carta como de los principios enunciados por el Tribunal de Justicia en la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238). El derecho al respeto de la vida privada garantizado por el artículo 7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros quedaría privado de alcance alguno si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas se rodeen de garantías adecuadas y comprobables.

35 La High Court observa además que, en realidad, el Sr. Schrems impugna en su recurso la licitud del régimen de «puerto seguro» establecido por la Decisión 2000/520, de la cual deriva la decisión discutida en el litigio principal. Así pues, aunque el Sr. Schrems no haya impugnado formalmente la validez de la Directiva 95/46 ni de la Decisión 2000/520, según ese tribunal se suscita la cuestión de si, en virtud del artículo 25, apartado 6, de la Directiva 95/46, el comisario estaba vinculado por la constatación realizada por la Comisión en esa Decisión, según la cual Estados Unidos garantiza un nivel de protección adecuado, o bien si el artículo 8 de la Carta autorizaba al comisario a separarse, en su caso, de esa constatación.

36 En esas circunstancias, la High Court decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legislación y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?

2) En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520?»

SOBRE LAS CUESTIONES PREJUDICIALES

37 Con sus cuestiones prejudiciales, que es oportuno examinar conjuntamente, el tribunal remitente pregunta en sustancia si, y en qué medida, el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una decisión, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen, que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

Sobre las facultades de las autoridades nacionales de control, a las que se refiere el artículo 28 de la Directiva 95/46, ante una Decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva

38 Se debe recordar previamente que las disposiciones de la Directiva 95/46, en cuanto regulan el tratamiento de datos personales, que puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada, deben ser necesariamente interpretadas a la luz de los derechos fundamentales protegidos por la Carta (véanse las sentencias Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 68; Google Spain y Google, C-131/12, EU:C:2014:317, apartado 68, y Ryneš, C-212/13, EU:C:2014:2428, apartado 29).

39 Del artículo 1 y de los considerandos 2 y 10 de la Directiva 95/46 se deduce que ésta se propone garantizar no sólo una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas frente al tratamiento de los datos personales, sino también un elevado nivel de protección de esas libertades y derechos fundamentales. La jurisprudencia del Tribunal de Justicia destaca la importancia tanto del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta como del derecho fundamental a la protección de los datos personales que garantiza el artículo 8 de ésta (véanse las sentencias Rijkeboer, C-553/07, EU:C:2009:293, apartado 47; Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 53, y Google Spain y Google, C-131/12, EU:C:2014:317, apartados 53, 66 y 74 y la jurisprudencia citada).

40 En lo concerniente a las facultades de las que disponen las autoridades nacionales de control en materia de transferencia de datos personales a terceros países, se ha de señalar que el artículo 28, apartado 1, de la Directiva 95/46 impone a los Estados miembros la obligación de instituir una o varias autoridades públicas encargadas del control, con toda independencia, del cumplimiento de las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de datos personales. Esa exigencia deriva también del Derecho primario de la Unión, en particular del artículo 8, apartado 3, de la Carta y del artículo 16 TFUE, apartado 2 (véanse, en ese sentido, las sentencias Comisión/Austria, C-614/10, EU:C:2012:631, apartado 36, y Comisión/Hungría C-288/12, EU:C:2014:237, apartado 47).

41 La garantía de independencia de las autoridades nacionales de control pretende asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas frente al tratamiento de datos personales y debe interpretarse a la luz de dicho objetivo. Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades. La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales, como señala el considerando 62 de la Directiva 95/46 (véanse las sentencias Comisión/Alemania, C-518/07, EU:C:2010:125, apartado 25 y Comisión/Hungría C-288/12, EU:C:2014:237, apartado 48 y la jurisprudencia citada).

42 Para garantizar esa protección, las autoridades nacionales de control han de lograr un justo equilibrio entre el respeto del derecho fundamental a la vida privada y los intereses que exigen la libre circulación de datos personales (véanse, en ese sentido, las sentencias Comisión/Alemania, C-518/07, EU:C:2010:125, apartado 24, y Comisión/Hungría C-288/12, EU:C:2014:237, apartado 51).

43 A tal efecto, las autoridades nacionales de control disponen de una amplia gama de facultades, y éstas, enumeradas de forma no exhaustiva por el artículo 28, apartado 3, de la Directiva 95/46, constituyen otros tantos medios necesarios para el cumplimiento de sus funciones, como destaca el

considerando 63 de esa Directiva. Así pues, esas autoridades disponen, en particular, de facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control, de facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio.

44 Del artículo 28, apartados 1 y 6, de la Directiva 95/46 resulta ciertamente que las facultades de las autoridades nacionales de control abarcan los tratamientos de datos personales realizados en el territorio del Estado miembro de esas autoridades, de modo que éstas no disponen, con fundamento en ese artículo 28, de facultades respecto a los tratamientos de datos realizados en el territorio de un tercer país.

45 No obstante, la operación consistente en hacer transferir datos personales desde un Estado miembro a un tercer país constituye por sí misma un tratamiento de datos personales, en el sentido del artículo 2, letra b), de la Directiva 95/46 (véase, en ese sentido, la sentencia Parlamento/Consejo y Comisión, C-317/04 y C-318/04, EU:C:2006:346, apartado 56), realizado en el territorio de un Estado miembro. En efecto, esa disposición define el «tratamiento de datos personales» como «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales», y cita como ejemplo «la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos».

46 El considerando 60 de la Directiva 95/46 precisa que las transferencias de datos personales hacia terceros países sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la misma Directiva. En ese sentido, el capítulo IV de ésta, en el que figuran los artículos 25 y 26, estableció un régimen dirigido a garantizar un control por los Estados miembros de las transferencias de datos personales hacia terceros países. Es un régimen complementario del régimen general que establece el capítulo II de la misma Directiva, que enuncia las condiciones generales de licitud de los tratamientos de datos personales (véase, en ese sentido, la sentencia Lindqvist, C-101/01, EU:C:2003:596, apartado 63).

47 Como quiera que las autoridades nacionales de control, conforme al artículo 8, apartado 3, de la Carta y al artículo 28 de la Directiva 95/46, están encargadas del control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales, toda autoridad nacional de control está investida, por tanto, de la competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad hacia un tercer país respeta las exigencias establecidas por la Directiva 95/46.

48 Al mismo tiempo que el considerando 56 de la Directiva 95/46 reconoce que las transferencias de datos personales desde los Estados miembros a terceros países son necesarias para el desarrollo del comercio internacional, la Directiva 95/46 establece en su artículo 25, apartado 1, el principio de que esa transferencia sólo se puede realizar si esos terceros países garantizan un nivel de protección adecuado.

49 Además, el considerando 57 de la misma Directiva precisa que, cuando un tercer país no ofrezca un nivel de protección adecuado, debe prohibirse la transferencia al mismo de datos personales.

50 El artículo 25 de la Directiva 95/46 impone diversas obligaciones a los Estados miembros y a la Comisión para controlar las transferencias de datos personales a terceros países en función del nivel de protección atribuido a éstos en cada uno de esos países. De ese artículo resulta, en particular, que la constatación de que un tercer país garantiza o no un nivel de protección adecuado pueden realizarla bien los Estados miembros o bien la Comisión, como ha señalado el Abogado General en el punto 86 de sus conclusiones.

51 La Comisión puede adoptar con fundamento en el artículo 25, apartado 6, de la Directiva 95/46, una decisión que constate que un tercer país garantiza un nivel de protección adecuado. Conforme al párrafo segundo de esa disposición, los destinatarios de esa decisión son los Estados miembros, que deberán adoptar las medidas necesarias para atenerse a ella. En virtud del artículo 288 TFUE, párrafo cuarto, esa decisión tiene carácter obligatorio para todos los Estados miembros destinatarios y vincula por tanto a todos sus órganos (véanse, en ese sentido, las sentencias Albako/BALM, 249/85, EU:C:1987:245, apartado 17, y Mediaset, C-69/13, EU:C:2014:71, apartado 23), en cuanto tiene el efecto de autorizar transferencias de datos personales desde los Estados miembros al tercer país al que se refiere dicha decisión.

52 Así pues, mientras la decisión de la Comisión no haya sido declarada inválida por el Tribunal de Justicia, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden ciertamente adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciara con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado. En efecto, los actos de las instituciones de la Unión disfrutan en principio de una presunción de legalidad, y producen por tanto efectos jurídicos mientras no hayan sido revocados, anulados en virtud de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad (sentencia Comisión/Grecia, C-475/01, EU:C:2004:585, apartado 18 y la jurisprudencia citada).

53 No obstante, una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, como la Decisión 2000/520, no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos. De igual forma, una decisión de esa naturaleza no puede dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control por el artículo 8, apartado 3, de la Carta y por el artículo 28 de la referida Directiva, como ha expuesto el Abogado General en los puntos 61, 93 y 116 de sus conclusiones.

54 Ni el artículo 8, apartado 3, de la Carta, ni el artículo 28 de la Directiva 95/46 excluyen del ámbito de la competencia de las autoridades nacionales designadas a ese efecto el control de las transferencias de datos personales a terceros países a los que se refiera una decisión de la Comisión en virtud del artículo 25, apartado 6, de esa Directiva.

55 En particular, el artículo 28, apartado 4, párrafo primero, de la Directiva 95/46, que dispone que las autoridades nacionales de control entenderán de la solicitud que presente «cualquier persona [...] en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales», no prevé ninguna excepción en ese sentido, en el supuesto de que la Comisión hubiera adoptado una decisión en virtud del artículo 25, apartado 6, de esa Directiva.

56 Además, sería contrario al sistema establecido por la Directiva 95/46 y a la finalidad de sus artículos 25 y 28 que una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de dicha Directiva tuviera el efecto de impedir que una autoridad nacional de control examine la solicitud de una persona para la protección de sus derechos y libertades frente al tratamiento de sus datos personales que hayan sido o pudieran ser transferidos desde un Estado miembro a un tercer país al que se refiere esa decisión de la Comisión.

57 Por el contrario, el artículo 28 de la Directiva 95/46 se aplica por su propia naturaleza a todo tratamiento de datos personales. Por tanto, incluso habiendo adoptado la Comisión una decisión en virtud del artículo 25, apartado 6, de esa Directiva, las autoridades nacionales de control, a las que una persona haya presentado una solicitud de protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por la referida Directiva.

58 Si no fuera así, las personas cuyos datos personales hayan sido o pudieran ser transferidos al tercer país considerado quedarían privadas del derecho garantizado por el artículo 8, apartados 1 y 3, de la Carta de presentar a las autoridades nacionales de control una solicitud para la protección de sus derechos fundamentales (véase, por analogía, la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 68).

59 Une solicitud, prevista en artículo 28, apartado 4, de la Directiva 95/46, mediante la que una persona cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país alegue, como en el asunto principal, que el Derecho y las prácticas de ese país no garantizan un nivel de protección adecuado, no obstante lo constatado por la Comisión en una decisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva, debe entenderse como concerniente en sustancia a la compatibilidad de esa decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

60 Hay que recordar en ese sentido la reiterada jurisprudencia del Tribunal de Justicia según la cual la Unión es una Unión de Derecho en la que todos los actos de sus instituciones están sujetos al control de su conformidad, en particular, con los Tratados, con los principios generales del Derecho

y con los derechos fundamentales (véanse, en ese sentido, las sentencias Comisión y otros/Kadi, C-584/10 P, C-593/10 P y C-595/10 P, EU:C:2013:518, apartado 66; Inuit Tapiriit Kanatami y otros/Parlamento y Consejo, C-583/11 P, EU:C:2013:625, apartado 91, y Telefónica/Comisión, C-274/12 P, EU:C:2013:852, apartado 56). Por tanto, las decisiones de la Comisión adoptadas en virtud del artículo 25, apartado 6, de la Directiva 95/46 no pueden quedar excluidas de ese control.

61 Sin perjuicio de ello, el Tribunal de Justicia es exclusivamente competente para declarar la invalidez de un acto de la Unión, como una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, competencia exclusiva cuyo objeto es garantizar la seguridad jurídica preservando la aplicación uniforme del Derecho de la Unión (véanse las sentencias Melki y Abdeli, C-188/10 y C-189/10, EU:C:2010:363, apartado 54, y CIVAD, C-533/10, EU:C:2012:347, apartado 40).

62 Aunque los tribunales nacionales están ciertamente facultados para examinar la validez de un acto de la Unión, como una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, carecen sin embargo de competencia para declarar ellos mismos su invalidez (véanse, en ese sentido, las sentencias Foto-Frost, 314/85, EU:C:1987:452, apartados 15 a 20, e IATA y ELFAA, C-344/04, EU:C:2006:10, apartado 27). *A fortiori*, al examinar una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, concerniente a la compatibilidad de una decisión de la Comisión, adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, con la protección de la vida privada y de las libertades y derechos fundamentales de las personas, las autoridades nacionales de control no están habilitadas para declarar la invalidez de la referida decisión.

63 Atendiendo a esas consideraciones, cuando una persona, cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país que haya sido objeto de una decisión de la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, presenta a la autoridad nacional de control una solicitud para la protección de sus derechos y libertades frente al tratamiento de esos datos, e impugna con ocasión de esa solicitud, como en el asunto principal, la compatibilidad de dicha decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas, incumbe a esa autoridad examinar la referida solicitud con toda la diligencia exigible.

64 En el supuesto de que la referida autoridad llegue a la conclusión de que los datos alegados en apoyo de esa solicitud son infundados y la desestime por ello, la persona que haya presentado la solicitud debe disponer de recursos jurisdiccionales que le permitan impugnar esa decisión lesiva para ella ante los tribunales nacionales, según resulta del artículo 28, apartado 3, párrafo segundo, de la Directiva 95/46, entendido a la luz del artículo 47 de la Carta. Conforme a la jurisprudencia citada en los apartados 61 y 62 de la presente sentencia, esos tribunales están obligados a suspender el procedimiento y plantear al Tribunal de Justicia una cuestión prejudicial de validez si estiman que uno o varios de los motivos de invalidez alegados por las partes o, en su caso, suscitados de oficio son fundados (véase, en ese sentido, la sentencia T & L Sugars y Sidul Açúcares/Comisión, C-456/13 P, EU:C:2015:284, apartado 48 y jurisprudencia citada).

65 En el supuesto contrario, cuando esa autoridad considere fundadas las alegaciones expuestas por la persona que le haya presentado una solicitud para la protección de sus derechos y libertades frente al tratamiento de sus datos personales, la referida autoridad debe tener capacidad para comparecer en juicio, conforme al artículo 28, apartado 3, párrafo primero, tercer guion, de la Directiva 95/46, entendido a la luz del artículo 8, apartado 3, de la Carta. A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta.

66 Por las anteriores consideraciones se ha de responder a las cuestiones planteadas que el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

Sobre la validez de la Decisión 2000/520

67 Según resulta de las explicaciones del tribunal remitente sobre las cuestiones planteadas, en el asunto principal el Sr. Schrems alega que el Derecho y las prácticas de Estados Unidos no garantizan un nivel de protección adecuado, en el sentido del artículo 25 de la Directiva 95/46. Como ha señalado el Abogado General en los puntos 123 y 124 de sus conclusiones, el Sr. Schrems manifiesta dudas, que ese tribunal parece compartir en sustancia, sobre la validez de la Decisión 2000/520. Siendo así, por las consideraciones expuestas en los apartados 60 a 63 de la presente sentencia, y para dar una respuesta completa al referido tribunal, es preciso apreciar si esa Decisión se ajusta a las exigencias derivadas de dicha Directiva entendida a la luz de la Carta.

Sobre las exigencias derivadas del artículo 25, apartado 6, de la Directiva 95/46

68 Como ya se ha observado en los apartados 48 y 49 de la presente sentencia, el artículo 25, apartado 1, de la Directiva 95/46 prohíbe las transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado.

69 No obstante, a efectos del control de esas transferencias el artículo 25, apartado 6, párrafo primero, de esa Directiva dispone que la Comisión «podrá hacer constar [...] que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 [de ese artículo], a la vista de su legislación interna o de sus compromisos internacionales [...], a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

70 Es cierto que ni el artículo 25, apartado 2, de la Directiva 95/46 ni ninguna otra de sus disposiciones contienen una definición del concepto de «nivel de protección adecuado». En particular, el artículo 25, apartado 2, de esa Directiva se limita a enunciar que el carácter adecuado del nivel de protección que ofrece un tercer país «se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos», y enumera sin carácter exhaustivo las circunstancias que se deben considerar en esa apreciación.

71 No obstante, según resulta de los mismos términos del artículo 25, apartado 6, de la Directiva 95/46, esta disposición exige que un tercer país «garantice» un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales. Por otro lado, también conforme a esa disposición, el carácter adecuado del nivel de protección que ofrece un tercer país se ha de apreciar «a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

72 De esa forma, el artículo 25, apartado 6, de la Directiva 95/46 da cumplimiento a la obligación expresa de protección de los datos personales, prevista en el artículo 8, apartado 1, de la Carta, y pretende asegurar la continuidad del elevado nivel de protección en caso de transferencia de datos personales a un tercer país, como ha señalado el Abogado General en el punto 139 de sus conclusiones.

73 Es verdad que el término «adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo, como ha manifestado el Abogado General en el punto 141 de sus conclusiones, debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría. Además, el elevado nivel de protección garantizado por la Directiva 95/46 entendida a la luz de la Carta se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos.

74 De la redacción misma del artículo 25, apartado 6, de la Directiva 95/46 resulta que es el ordenamiento jurídico del tercer país al que se refiere la decisión de la Comisión el que debe garantizar un nivel de protección adecuado. Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión.

75 Siendo así, al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país, conforme al artículo 25, apartado 2, de la Directiva 95/46.

76 De igual modo, dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido.

77 Además, como ha expuesto el Abogado General en los puntos 134 y 135 de sus conclusiones, al apreciar la validez de una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46 también se han de tener en cuenta las circunstancias sobrevenidas después de su adopción.

78 En ese sentido es preciso observar que, dado el importante papel que cumple la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada, así como el gran número de personas cuyos derechos fundamentales pueden ser vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (véase por analogía la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48).

Sobre el artículo 1 de la Decisión 2000/520

79 La Comisión manifestó en el artículo 1, apartado 1, de la Decisión 2000/520 que los principios que figuran en el anexo I de ésta, aplicados de conformidad con la orientación que proporcionan las FAQ enunciadas en el anexo II de la misma Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos. De esa disposición resulta que tanto esos principios como las FAQ han sido publicados por el Departamento de Comercio estadounidense.

80 La adhesión de una entidad a los principios de puerto seguro se lleva a cabo conforme a un sistema de autocertificación, como resulta del artículo 1, apartados 2 y 3, de esa Decisión, en relación con la FAQ nº 6 que figura en el anexo II de ésta.

81 Aunque el recurso por un tercer país a un sistema de autocertificación no es por sí mismo contrario a la exigencia enunciada en el artículo 25, apartado 6, de la Directiva 95/46 de que el tercer país considerado garantice un nivel de protección adecuado «a la vista de su legislación interna o de sus compromisos internacionales», la fiabilidad de ese sistema en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales.

82 En el presente asunto, en virtud del anexo I, párrafo segundo, de la Decisión 2000/50, los principios de puerto seguro «son de utilización exclusiva de las entidades estadounidenses que reciben datos personales de la Unión Europea, al efecto de reunir los requisitos de "puerto seguro" y obtener la correspondiente presunción de "adecuación"». Por tanto, esos principios son aplicables únicamente a las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión, sin que se exija que las autoridades públicas estadounidenses se sometan a esos principios.

83 Además, en virtud del artículo 2 de la Decisión 2000/520, ésta «se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios [de puerto seguro] y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva [95/46]», sin contener no obstante las constataciones suficientes sobre las medidas con las que Estados Unidos garantiza un nivel de protección adecuado,

en el sentido del artículo 25, apartado 6, de esa Directiva, a la vista de su legislación interna o de sus compromisos internacionales.

84 A ello se añade que, conforme al anexo I, párrafo cuarto, de la Decisión 2000/520, la aplicabilidad de esos principios puede limitarse, en especial, por «las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]», así como por «disposición legal o reglamentaria, o jurisprudencia, que originen conflictos de obligaciones o autorizaciones [explícitas], siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones».

85 En ese sentido, en el título B de su anexo IV la Decisión 2000/520 pone de relieve, respecto a los límites a los que está sometida la aplicabilidad de los principios de puerto seguro, que «es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro».

86 Así pues, la Decisión 2000/520 reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]» sobre los principios de puerto seguro, primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten por tanto incompatibles con ellas.

87 Dado el carácter general de la excepción prevista en el anexo I, párrafo cuarto, de la Decisión 2000/520, ésta hace posibles así injerencias, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos, en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos. En ese sentido, para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 33 y la jurisprudencia citada).

88 Además, la Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional.

89 Se añade a ello el hecho de que la Decisión 2000/520 no pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza. Como ha expuesto el Abogado General en los puntos 204 a 206 de sus conclusiones, los mecanismos de arbitraje privado y los procedimientos ante la Comisión Federal de Comercio, cuyas facultades, descritas en particular en las FAQ nº 11 que figuran en el anexo II de esa Decisión, se limitan a los litigios comerciales, atañen al cumplimiento por las empresas estadounidenses de los principios de puerto seguro, y no se pueden aplicar en litigios concernientes a la legalidad de injerencias en los derechos fundamentales derivadas de medidas de origen estatal.

90 Por otro lado, el análisis precedente de la Decisión 2000/520 se confirma por la apreciación que la misma Comisión ha realizado sobre la situación resultante de la aplicación de esa Decisión. En efecto, en particular en los puntos 2 y 3.2 de la Comunicación COM(2013) 846 final y en los puntos 7.1, 7.2 y 8 de la Comunicación COM(2013) 847 final, cuyo contenido se expone respectivamente en los apartados 13 a 16, y 22, 23 y 25 de la presente sentencia, la Comisión constató que las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional. De igual modo, la Comisión apreció que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión.

91 En lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión, según reiterada jurisprudencia del Tribunal de Justicia, una normativa de ésta que haga

posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a ellos (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55 y la jurisprudencia citada).

92 Además, y sobre todo, la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 52 y la jurisprudencia citada).

93 Pues bien, no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización [véase en ese sentido, acerca de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, p. 54), la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 57 a 61].

94 En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta (véase, en ese sentido, la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 39).

95 De igual manera, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta. En efecto, el artículo 47, párrafo primero, de ésta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva, respetando las condiciones establecidas en dicho artículo. En ese sentido, la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho (véanse, en ese sentido, las sentencias Les Verts/Parlamento, 294/83, EU:C:1986:166, apartado 23; Johnston, 222/84, EU:C:1986:206, apartados 18 y 19; Heylens y otros, 222/86, EU:C:1987:442, apartado 14, y UGT-Rioja y otros, C-428/06 a C-434/06, EU:C:2008:488, apartado 80).

96 Como se ha apreciado en particular en los apartados 71, 73 y 74 de la presente sentencia, la adopción por la Comisión de una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46 requiere la constatación debidamente motivada por esa institución de que el tercer país considerado garantiza efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión, según resulta de los anteriores apartados de esta sentencia.

97 Ahora bien, se ha de observar que la Comisión no manifestó en la Decisión 2000/520 que Estados Unidos «garantiza» efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales.

98 En consecuencia, y sin que sea preciso apreciar el contenido de los principios de puerto seguro, se debe concluir que el artículo 1 de esa Decisión vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa.

Sobre el artículo 3 de la Decisión 2000/520

99 De las consideraciones expuestas en los apartados 53, 57 y 63 de la presente sentencia se sigue que, en virtud del artículo 28 de la Directiva 95/46, entendido a la luz del artículo 8 de la Carta, las autoridades nacionales de control deben poder examinar con toda independencia cualquier solicitud de protección de los derechos y libertades de una persona frente a un tratamiento de datos personales que la afecte. Así es, en particular, cuando esa persona suscite con ocasión de su solicitud interrogantes sobre la compatibilidad de una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

100 No obstante, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 establece una regulación específica de las facultades de las que disponen las autoridades nacionales de control ante una constatación realizada por la Comisión sobre el nivel de protección adecuado, en el sentido del artículo 25 de la Directiva 95/46.

101 De esa forma, a tenor de dicha disposición las referidas autoridades, «sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva [95/46], [...] podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios [de la Decisión 2000/520]», de manera restrictiva, ya que sólo es posible la intervención a partir de un alto umbral de condiciones. Aunque esa disposición no enerva las facultades de esas autoridades para tomar medidas encaminadas a asegurar el cumplimiento de las disposiciones nacionales adoptadas en aplicación de esa Directiva, excluye en cambio la posibilidad de que esas autoridades tomen medidas con objeto de asegurar el cumplimiento del artículo 25 de la misma Directiva.

102 Por tanto, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 debe entenderse en el sentido de que priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46, en el supuesto de que una persona alegue, con ocasión de una solicitud basada en esa disposición, factores que puedan afectar a la compatibilidad de una decisión de la Comisión, que haya constatado con fundamento en el artículo 25, apartado 6, de esa Directiva que un tercer país garantiza un nivel de protección adecuado, con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

103 Ahora bien, la facultad de ejecución atribuida a la Comisión por el legislador de la Unión en el artículo 25, apartado 6, de la Directiva 95/46 no confiere a esa institución la competencia para restringir las facultades de las autoridades nacionales de control a las que se refiere el anterior apartado de esta sentencia.

104 Siendo así, es preciso apreciar que, al adoptar el artículo 3 de la Decisión 2000/520, la Comisión excedió los límites de la competencia que le atribuye el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y que dicho artículo 3 es inválido por esa causa.

105 Toda vez que los artículos 1 y 3 de la Decisión 2000/520 son indisociables de los artículos 2 y 4 y de los anexos de ésta, su invalidez tiene el efecto de afectar a la validez de esa Decisión en su conjunto.

106 Por todas las consideraciones precedentes se debe concluir que la Decisión 2000/520 es inválida.

COSTAS

107 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante el órgano jurisdiccional nacional, corresponde a éste resolver sobre las costas. Los gastos efectuados por quienes, no siendo partes del litigio principal, han presentado observaciones ante el Tribunal de Justicia no pueden ser objeto de reembolso.

En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara:

1) El artículo 25, apartado 6, de la de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29

de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

2) La Decisión 2000/520 es inválida.

Firmas

DICTÁMENES

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
16/010	092/2009

Montevideo, 20 de agosto de 2010

Ref. Consulta sobre DATOS SENSIBLES y REFERENCIAS PERSONALES DE EMPRESAS DE SEGURIDAD

VISTO: La consulta formulada referente a recolección y tratamiento de datos de personal empleado en empresas de seguridad, o aspirantes a llenar vacantes.

RESULTANDO:

I) Que se consulta sobre la procedencia o improcedencia de registrar diferentes especies de datos personales pertenecientes a trabajadores de este ramo o aspirantes a serlo, todo lo cual es analizado y evacuado en circunstanciado informe jurídico que luce agregado al expediente (Informe N O 63/2009 de 22 de enero de 2010).

II) Que compartiendo este Consejo lo informado, se habrán de dictaminar aquellas conclusiones de carácter más general, sin perjuicio de remitir al mencionado informe jurídico por el detalle.

CONSIDERANDO:

I) Que la recolección de datos personales no es una actividad desregulada sino, por el contrario, se trata de una actividad reglada, acotada normativamente por una serie de principios y criterios jurídicos de obligatorio respeto, entre otros el de finalidad, y el de proporcionalidad (adecuación, ecuanimidad, ponderación).

II) Que tratándose de datos relativos a experiencia y referencias laborales para el cargo, estamos ante datos personales comunes, cuya recolección aparece justificada y necesaria para el establecimiento de vínculos laborales.

III) Que en la recolección y tratamiento de "datos sensibles", e incluso, en sentido más amplio, de los llamados por ley "datos especialmente protegidos" (que incluyen varias categorías, como son datos de salud, publicidad, actividad comercial o crediticia y transferencias internacionales), se deben observar criterios más severos que cuando se trata de datos personales comunes.

IV) Que sin perjuicio del derecho a recabar y obtener asesoramientos como el que moviliza la emisión de este dictamen, resulta difícil -por no decir imposible- ofrecer un dictamen completo destinado a cubrir todas y cada una de las hipótesis que plantea la realidad, por definición vasta y dinámica, dependiente de factores diversos que hacen que no siempre la recolección de un dato personal tenga la misma trascendencia o consecuencias.

V) Que por esta razón es, en definitiva, el responsable de la base de datos quien debe resolver en cada caso, del modo más objetivo y justificado posibles, qué datos recabar y cómo recabarlos, a la luz del contexto, la finalidad perseguida y los restantes principios y deberes que rigen la materia.

VI) Que la seguridad pública es un derecho fundamental a cuya defensa y garantía contribuyen diversos actores de la sociedad, entre los que figuran empresas privadas especializadas como la consultante, debiendo ponderarse esta importancia y alcances en relación a los restantes derechos fundamentales eventualmente afectados (art. 7 de la Constitución de la República)

ATENTO: A lo expuesto, a lo dispuesto en el art. 7, 8, 9 D), 12, 13, 18, 19 y 34 A) de la Ley N O 18.331 de 11 de agosto de 2008, y en los arts. 4 B), 5, 6 y 23 A) del Decreto N O 414/009 de 31 de agosto de 2009.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Los datos personales referidos a experiencia y referencias laborales son datos comunes destinados a un inicio de relacionamiento contractual, cuya recolección y tratamiento no requieren consentimiento del titular sin perjuicio de mantenerse su tratamiento reservado y responsable, destinado exclusivamente a la finalidad perseguida en su recolección.

2.- Tratándose de Empresas de Seguridad, y en función del derecho fundamental a cuya garantía y defensa este tipo de empresas contribuyen, se considera dentro de lo ponderado o adecuado, que recaben datos de sus trabajadores, o aspirantes a serlo, relativos a impedimentos físicos o enfermedades crónicas, antecedentes policiales, y deudas, todo ello bajo las más severas garantías de seguridad y reserva.

3.- En el mismo contexto empresarial, no aparece justificado -salvo prueba en contrario- tratar las siguientes especies de datos personales: calidad de inquilino o propietario; marcas o tatuajes; color de ojos y pelo; ciertos datos familiares (ocupación de padre, madre, hijo, otros); actividades deportivas, recreativas y religiosas.

4.- La recolección y tratamiento de datos sensibles en el marco de una relación contractual, no abaten la necesidad de obtener el consentimiento expreso y escrito del titular, ni supone dejar de cumplir con los restantes principios y preceptos de la Ley NO 18.331.

5.- Los datos personales de los trabajadores deben conservarse mientras dure el vínculo laboral, sin perjuicio de la facultad del responsable de llevar luego del cese, y en forma bloqueada para otro tipo de accesos y usos, un registro histórico a los efectos jubilatorios.

6.- Puede resultar oportuno, y así se recomienda, incluir opciones de respuestas facultativas en aquellos cuestionarios que recolectan datos personales, en especial tratándose de datos sensibles. Se recomienda a tales efectos informar a los titulares de los datos este carácter opcional, mediante leyendas precisas y claras en tal sentido, avisando también el compromiso del responsable de la base de datos de no utilizar la información recabada con sentido o fines discriminatorios.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

m.b.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
18/010	1300/010

Montevideo, 20 de agosto de 2010

VISTO: La consulta formulada respecto a la procedencia de integrar datos de salud provenientes de los actos médicos que practican las "Emergencias Móviles", en las Historias Clínicas de los respectivos pacientes que obran en sedes de los prestadores originales de servicios de salud.

RESULTANDO:

I) Que la consultante aclara que la medida o proyecto no incluiría la comunicación de datos comerciales ni financieros de tipo alguno.

II) Que la consulta merece dictamen positivo, en la línea que propone el asesoramiento letrado producido en el expediente, a cuyos argumentos y conceptos cabe remitirse sin perjuicio de incorporar otros fundamentos que completan el dispositivo jurídico aplicable en la especie.

CONSIDERANDO:

I) Que todo paciente tiene derecho a que se lleve una historia clínica completa, escrita o electrónica, donde figure la evolución de su estado de salud desde el nacimiento hasta la muerte (art. 18 lit. D de la Ley N O 18.335 de 1508-2008).

II) Que el carácter de completitud que prescribe la citada norma presupone más que la facultad la pertinencia, de contar con aquellos datos provenientes de atenciones sanitarias, cuyos asientos documentales están radicados originariamente en los servicios de Emergencia Móvil.

III) Que las Emergencias Móviles forman parte de un sistema sanitario integrado, y como tales recolectan y tratan datos personales de salud de sus pacientes, perfecta y totalmente habilitadas por la ley de la materia (art. 19 de la ley N O 18.331 de 1 1-08-2008).

IV) Que medidas como las propuestas contribuyen, en definitiva, al mejor cumplimiento del principio de finalidad que preside la confección de un instrumento documental tan esencial en el área como es la Historia Clínica, favoreciendo con ello la mejor práctica del servicio de salud por medio de distintos facultativos que se apoyan sucesiva e históricamente en dicho instrumento, para observar y atender al paciente a lo largo de su ciclo vital.

V) Que la Historia Clínica posee un régimen jurídico particular, que encuentra fundamento en una ley especial de interés general y de fecha posterior a la que rige la materia tutelada por esta Unidad, como es la Ley N O 18.335, lo que hace inaplicable el requisito de disociación dispuesto por el art. 17 inc. 3 lit. C) de la Ley N O 18.331, y habilita a prescindir del consentimiento del titular de los datos, al tenor lo dispuesto por el inc. A del mismo artículo ante citado.

VI) Que a la luz del especial carácter de la materia abordada (datos sensibles) cabe advertir sobre la importancia y consecuencias que tendrá la elección de la fuente formal en que terminará plasmándose esta iniciativa (ley, decreto, resolución ministerial), así como atender lo preceptuado por el art. 20 de la Ley N O 18.335.

ATENTO: A lo dispuesto por los arts. 18, 19, 34 lit. A) de la Ley N O 18.331 de 1 1 de agosto de 2008; y el art. 18 lit. D de la Ley N O 18.335 de 15 de agosto de 2008,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Declarar procedente y conveniente la integración de la información asistencial de salud proveniente de los registros de las Emergencias Móviles, a las Historias Clínicas de los respectivos pacientes radicadas en los prestadores integrales del servicio, respetando los principios y deberes contenidos en las Leyes Nros. 18.331 y 18.335.

2.- Atento a la naturaleza de la materia en juego, recomendar que la fuente formal donde termine plasmándose esta medida sea la de mayor rango jurídico.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

m.b.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
19/010	2851/010

Montevideo, 27 de agosto de 2010

Ref. Consulta DGI sobre si CLEARING DE INFORMES DEBE PROPORCIONARLE DATOS PERSONALES

VISTO: La consulta formulada por la Dirección General Impositiva (DCI) sobre si Clearing de Informes debe -en caso de serle requerido- proporcionar a la DGI los números de teléfonos celulares que ésta le solicite, en tanto disponga de ellos en sus bases de datos.

RESULTANDO:

En síntesis, DGI alude a la función que cumple como encargada de la recaudación de los tributos internos del país, al amplio deber de colaboración que tienen los particulares con la Administración y a la facultad de ésta a requerir informaciones a terceros ajenos a la relación jurídico tributaria, a la vez que refiere a la normativa aplicable que a su entender habilitaría la comunicación de datos que se solicita.

Se expidió el informe jurídico Nº 2456 de 13 de agosto de 2010 (fs. 3-4).

CONSIDERANDO:

I) Que la comunicación de datos que se pretende se encuentra regulada en el artículo 17 de la Ley N O 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 1 1 de agosto de 2008 (LPDP) y exige para su legitimidad la conjunción simultánea de los siguientes requisitos, el interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, salvo las excepciones establecidas en la norma.

El interés legítimo solo podría vislumbrarse desde la órbita de la DCI, (destinatario) no así del Clearing de Informes (emisor). La ausencia de este requisito, por sí solo bastaría para desestimar la comunicación de datos.

II) Que no obstante lo anterior, tampoco se verifican en el presente las excepciones enunciadas en el artículo 17 para validar la comunicación de datos sin el previo consentimiento del titular.

1. No existe una ley de interés general que establezca el deber de comunicar los datos por parte de un particular, como en este caso lo es el Clearing de Informes, cuya función es la de brindar informes objetivos de carácter comercial. Las previsiones legales a las que alude la consultante no son aplicables en la especie, en tanto atienden o bien a la obligación de aportar datos por parte de entidades públicas estatales o no, o bien al deber de colaboración de los particulares, esencialmente contribuyentes. En el presente caso, en cambio, se pretende que un particular brinde información no sobre sí, sino sobre terceras personas. Por otra parte, la consideración acerca de que la información en poder de la DGI resulta amparada en el secreto tributario (artículo 47 Código Tributario), no resulta fundamento de peso para legitimar la comunicación de datos que se solicita.

2. Tampoco se cumplen los supuestos del artículo 9 0 al que remite el artículo 17 de la LPDP:

a) Los datos no provienen de fuentes públicas de información.

b) La comunicación no implica el ejercicio de funciones propias de los poderes del Estado como entidades bilaterales de cooperación, sino que la entidad emisora, en este caso, es un particular con una finalidad comercial claramente definida. Tampoco existe una obligación legal que habilite la comunicación de marras, como lo analizáramos en el párrafo precedente.

c) tampoco se cumple el literal c) en la medida que el dato requerido por parte de Clearing de Informes es el número de teléfonos celulares que le solicite la DGI y que aquella disponga en sus bases de datos. Tal disposición enumera taxativamente los datos que no requieren el previo consentimiento informado. Para las personas físicas, ellos son el nombre, apellido, documento de identidad, nacionalidad, domicilio y fecha de nacimiento; y para las personas jurídicas, razón social, nombre de fantasía, RUT, domicilio, teléfono e identidad de las personas a cargo de la misma. El número de teléfono celular no resulta contemplado en la previsión legal, para ninguna de las dos categorías.

d) El literal d) alude a la existencia de una relación contractual, científica o profesional del titular de los datos, situación en la que no se encuentra DGI ni Clearing de Informes respecto a los titulares de los datos.

e) Finalmente, no se verifica la última hipótesis en tanto alude a un uso exclusivo, personal o doméstico.

3. Las restantes hipótesis contempladas en los literales c y del artículo 17 (datos relativos a la salud y datos disociados), tampoco se aplican en la especie.

ATENTO: A lo expuesto y a lo dispuesto por las normas legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que no se deben comunicar los datos referidos a números de teléfono celular, por parte de Clearing de Informes a la Dirección General Impositiva.

2.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

m.j.r.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
13/011	171/011

Montevideo, 9 de setiembre de 2011

VISTO: La consulta formulada por las Obras Sanitarias del Estado (O.S.E), a través del Sr. Enrique Balestrino, integrante de la comisión multidisciplinaria que pretende adecuar y alinear el Organismo a las Leyes Nos. 18.331 y 18.381, de Protección de Datos Personales y Acción de Habeas Data, y de Acceso a la Información Pública, respectivamente.

RESULTANDO:

I) Que el solicitante consulta si es válido el acceso del usuario de los servicios de agua potable y saneamiento a través del Portal de OSE, introduciendo su número de documento de identidad, cuando ese dato conduce a otros que pueden ser de índole privada.

II) Que se expidió el informe jurídico N O 5934, el 3 de junio de 2011.

CONSIDERANDO:

I) Que conforme lo dispuesto en el artículo 4 0 , literales D y M de la Ley N O 18.331, de Protección de Datos Personales y Acción de Habeas Data (LPDP) que definen dato personal y tratamiento de datos, respectivamente, y de acuerdo con lo previsto por los artículos 70 y 90 del mismo cuerpo normativo que regulan los principios de veracidad y previo consentimiento informado, no resulta recomendable la incorporación del dato personal cédula de identidad del usuario, en forma única, para acceder a la información que el Organismo brinda al usuario.

II) Que una persona que no sea el usuario consultante y que conozca el número de cédula de identidad de otra, podría acceder fácilmente a la factura del consultado, tomando conocimiento del nombre completo del titular del servicio, domicilio, tipo de tarifa de que se trata (familiar u otro), unidad, así como el detalle del consumo con el monto a pagar y deudas si las tuviere.

ATENTO: A lo expuesto y lo dispuesto por las disposiciones legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Expedirse en el sentido que sería correcta la utilización del número de cédula de identidad, si en forma complementaria se incluye un password de carácter personal del usuario.

2.- Notifíquese, publíquese y oportunamente archívese.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

m.j.r.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
18/011	2011-2-10-00587

VISTO: La consulta presentada por el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

RESULTANDO:

I) Que la consulta refiere a la posibilidad de que el Ministerio de Ganadería, Agricultura y Pesca comunique datos al Ministerio del Interior en el marco de proyecto presentado como Fondo Concursable de AGESIC denominado "Fortalecimiento de la Seguridad del Movimiento de Semovientes".

II) Que el Ministerio de Ganadería, Agricultura y Pesca trasferiría los siguientes datos al Ministerio del Interior: número de DICOSE, número de caravana, número de padrón de campo, cédula de identidad del propietario (eventualmente puede requerirse también el nombre), identificación de la marca y razón social.

III) Que el expediente pasó a informe jurídico, el cual se realizó con fecha 19 de setiembre de 2010.

CONSIDERANDO:

I) Que estamos ante la presencia de datos personales, algunos determinados como el nombre, la cédula de identidad, el RUT, y otros determinables, por lo que es aplicable al caso concreto la LPDP

II) Que la consulta presentada refiere a una comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

III) Que según el artículo 17 de la LPDP, los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

IV) Que en el caso de marras sería aplicable la excepción relativa a que no es necesario recabar el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17 de la LPDP.

V) Que el Sistema Nacional de Información Ganadera (SNIG) es un sistema de información que tiene como objetivo principal asegurar la trazabilidad del ganado vacuno desde el establecimiento de origen del animal hasta el frigorífico, tanto individualmente como por grupos de animales, de acuerdo con las disposiciones y reglamentaciones del MGAP.

VI) Que el Ministerio de Interior tiene como cometido asegurar la seguridad nacional y para ello debe prevenir y combatir el delito.

VII) Que en la presente consulta se verifica la excepción contenida en el artículo 9 0 literal B) de la Ley, por lo que la comunicación de datos es legítima ya que el Ministerio de Interior está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el consentimiento de los titulares.

VIII) Que igualmente se hace aplicable el resto de la normativa vigente, sobre todos los principios que regulan la protección de datos.

ATENTO: A lo expuesto y lo dispuesto por las disposiciones legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Establecer que es legítima la comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

2.- Indicar que no es necesario recabar el consentimiento de los titulares porque se verifica la excepción relativa al ejercicio de las funciones propias de los organismos.

3.- Recomendar que se aplique las demás disposiciones relativa a la protección de datos.

4.- Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

f.b.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
26/011	2011-2-100000646

Montevideo, 4 de noviembre de 2011

VISTO: La consulta presentada por la Dirección General de Bomberos.

RESULTANDO:

I) Que la consulta refiere a la posibilidad de que el Ministerio de Trabajo y Seguridad Social comunique datos contenidos en las planillas de trabajo llevadas por aquél, a la Dirección Nacional de Bomberos con el objetivo de controlar que las empresas que cuentan con habilitación de Bomberos mantengan personal capacitado en el marco de los cursos de capacitación externa que brinda dicha Institución.

II) Que el expediente pasó a informe jurídico, el cual se realizó con fecha 12 de octubre de 2011.

CONSIDERANDO:

I) Que estamos ante la presencia de datos personales contenidos en las planillas de trabajo llevadas por el Ministerio de Trabajo y Seguridad Social, por lo que es aplicable al caso concreto la Ley N O 18.331 de 11 de agosto de 2008 de Protección de Datos Personales.

II) Que la consulta presentada refiere a una comunicación de datos entre el Ministerio de Trabajo y Seguridad Social y la Dirección General de Bomberos.

III) Que según el artículo 170 de la Ley, los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos.

IV) Que el artículo mencionado establece además los casos, en forma taxativa, en que no será necesario el consentimiento del titular de los datos para su comunicación. Entre las hipótesis previstas se encuentran los supuestos determinados por el artículo 90 de la Ley.

V) Que en el caso consultado sería aplicable la excepción relativa a que no es necesario el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17 0 de la Ley.

VI) Que la Dirección Nacional de Bomberos solicita al Ministerio de Trabajo las planillas de trabajo presentadas por las empresas con el objetivo de controlar que éstas cumplan con la obligación legal que establece la Ley N O 15.896. Por lo tanto, solicita los datos en virtud del cumplimiento de cometidos específicos que le son asignados por la Ley.

VII) Que en la presente consulta se verifica la excepción contenida en el artículo 9 0 literal B) de la Ley, por lo que la comunicación de datos es legítima ya que la Dirección General de Bomberos está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el consentimiento de los titulares.

VIII) Que igualmente se hace aplicable el resto de la normativa vigente, sobre todos los principios que regulan la protección de datos.

ATENTO: A lo establecido en la LPDP y a lo precedentemente expuesto,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Establecer que es legítima la comunicación de datos entre el Ministerio de Trabajo y Seguridad Social y la Dirección General de Bomberos.

2.- Indicar que no es necesario recabar el consentimiento de los titulares porque se verifica la excepción relativa al ejercicio de las funciones propias de los organismos.

3.- Recomendar que se tengan presentes las demás disposiciones relativas a la protección de datos.

4.- Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
14/012	2012-2-10-0000448

Montevideo, 28 de junio de 2012

VISTO: La consulta formulada por el Instituto Nacional de las Mujeres (INMUJERES) - Departamento de las Mujeres Afrodescendientes, del Ministerio de Desarrollo Social (MIDES), sobre la formación e inscripción de una base de datos territorial de profesionales y/o técnicos de origen afrodescendiente.

RESULTANDO:

I) Que dicho Departamento será el encargado de gestionar y recolectar los datos a través de un formulario digital auto-gestionado que se ubica en el sitio Web del MIDES, pero la gestión del espacio físico del soporte (el hosting y operación) de la Web MIDES la realiza la Empresa InnovaAge, mediante contrato celebrado con este ministerio.

II) Que el fundamento para la creación está en el mandato legal que se expresa en los Cometidos y Misión Institucional del MIDES y sus objetivos son fundamentalmente dos: a) obtener una base que sirva de justificación y fundamento para las Políticas Públicas, en especial las de Acción Afirmativa, y b) evaluar los posibles avances que se han producido en dichas políticas y su influencia en el colectivo afrodescendiente.

III) Que se consulta acerca de si es legítima o no la recolección y tratamiento de estos datos, -considerados datos sensibles-, por parte de este Departamento del MIDES, a la luz de lo establecido en el art. 18 de la Ley Nº 18.331.

CONSIDERANDO:

I) Que por regla, los datos de origen racial o étnico, -datos sensibles-, sólo pueden ser objeto de recolección y tratamiento con consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo (art. 18).

II) Que la especial tutela adjudicada a los datos sensibles, tiene por objeto evitar la discriminación, no obstante ello, también existe obligación de los Estados de actuar mediante políticas públicas adecuadas para favorecer el desarrollo de grupos y sectores de la sociedad que no tienen objetivamente las mismas posibilidades o propendiendo a la consolidación de una política social redistributiva de carácter progresivo, tal como se expresa en el DEC N O 286/006 de 22 de agosto de 2006)

III) Que por ello determinadas entidades públicas, de acuerdo con sus fines y cometidos, podrán mantener registro de este tipo de datos personales pues como en el caso, la finalidad de la base es la justificación y fundamento para las Políticas Públicas que se adoptan, evaluar los avances que se han producido y su influencia en el colectivo afrodescendiente.

IV) Que además, atento a los cometidos asignados al MIDES por Ley de creación N O 17.866 y normas posteriores, no sería exigible recabar el consentimiento informado de los titulares, en tanto éstos sean efectiva o potencialmente beneficiarios de sus programas, por resultar de aplicación el inciso B) del artículo 9 0 de la Ley N O 18.331.

V) Que la referida base deberá ser inscripta en el Registro de la URCDP, en el plazo de 90 días desde su creación, así como contar con medidas de seguridad acordes.

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Establecer que se considera legítima la creación de la base referida a la luz de lo establecido en el art. 18 de la Ley NO. 18.331.

2.- Indicar que deberá ser inscripta en el Registro de la URCDP dentro del plazo de 90 días contados desde la fecha de su creación, así como contar con medidas de seguridad acordes.

3.- Notifíquese, publíquese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
19/012	2011-2-10-0000818

Montevideo, 6 de setiembre de 2012

VISTO: La consulta referida a las eventuales consecuencias jurídicas que tendría contratar servicio de videovigilancia ofrecido por ANTEL, (http://www.antel.com.uy/antel/personas-yhogares/movil/servicios/con-costo/Videovigilancia), a efectos de instalar la cámara en la cocina-comedor del domicilio particular donde realiza su tarea la niñera contratada para el cuidado de los hijos menores de edad.

RESULTANDO:

I) Que el servicio de ANTEL refiere a un sistema de vigilancia y seguridad para el hogar, la oficina o el comercio a través del cual se puede monitorear en tiempo real desde el PC, laptop o celular.

II) Que el consultante pretende contratar este servicio para monitorear el ámbito de su hogar, concretamente la cocina- comedor del mismo, que si bien es considerado como ámbito doméstico, no sería tal para la persona que desempeña funciones cuidando a sus hijos menores de edad.

CONSIDERANDO:

I) Que la evolución producida en materia de derecho a la intimidad y a la privacidad, ha llevado a que el "derecho a estar solo" adquiera una dimensión más social y colectiva, llegándose así al derecho a tener el control y protección adecuada de los datos personales, por lo cual corresponde analizar aquellos casos, -como éste-, donde se entrecruzan varios derechos de raigambre constitucional, desde una perspectiva que enfatice en esta nueva concepción.

II) Que de acuerdo con el Documento "Repertorio de recomendaciones prácticas de la OIT", adoptado en la reunión de expertos en Ginebra en 1996 sobre la protección de la vida privada de los trabajadores, entre los principios generales se señala que el tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.

III) Que por otra parte la Guía de INTECO sobre Videovigilancia y PDP en su sección "Control laboral en entornos domésticos", establece que "es legítima la utilización de cámaras en entornos domésticos para el control laboral de personas ajenas contratadas, por ejemplo para el desempeño de tareas de mantenimiento, cuidado de niños o cualquier otro servicio prestado en el interior del domicilio".

IV) Que no sería necesario obtener el consentimiento de la persona afectada por el sistema de videovigilancia pues el art. 9 de la Ley N O 18.331 establece una serie de excepciones entre las cuales encontramos en el Numeral D), que si esos datos derivan de una relación contractual y son necesarios para su desarrollo o cumplimiento de la misma, no se exige recabar dicho consentimiento en forma expresa. En el caso analizado, puede considerarse que este tratamiento es necesario para el adecuado desenvolvimiento de la relación laboral referida al cuidado de los niños.

V) Que sin perjuicio de lo anterior, la instalación de cámaras tendrá que respetar los demás requisitos exigidos por la legislación vigente en la materia, especialmente el deber de informar expresamente y en forma anticipada a la trabajadora pues de esta forma la videovigilancia pasa a formar parte de la propia relación laboral y el tratamiento de los datos pasa a ser necesario para su adecuado desenvolvimiento de la misma (art. 13 de la Ley N O 18.331).

VI) Que las imágenes sólo pueden ser utilizadas para la finalidad para la cual han sido recabadas (art. 8 de la Ley Nº 18.331), así como deben eliminarse una vez cumplida la finalidad para la cual se han obtenido, salvo que se justifique su conservación, por ejemplo en caso de constatarse un delito.

VII) Que también deberán respetarse los espacios privados de la trabajadora (baños, dormitorios o vestuarios), pues la videovigilancia en estos casos afecta su intimidad y privacidad y no se ajusta al principio de proporcionalidad (adecuación del medio utilizado al fin que se persigue), que debe contemplarse para que la misma sea legítima (art. 1º y 6º num. 2 de la Ley Nº 18.331), así como garantizar la seguridad y confidencialidad de las imágenes que se obtienen (art. 1.1 de la Ley N O 18.331).

ATENTO: A lo dispuesto por los arts. 1º, 6º Numeral 2º, 8º , 9º Numeral D), 11, 13 y demás pertinentes de la Ley N O 18.331 de 11 de agosto de 2008;

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que no sería necesario obtener el consentimiento de la persona afectada por el sistema de videovigilancia de acuerdo a lo establecido en el art. 9 de la Ley NO 18.331 Numeral D).

2.- Que a efectos de cumplir con la ley deberá estarse a las demás exigencias indicadas.

3.- Notifíquese, publíquese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

g.r.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
25/012	2012-2-10-0000687

Montevideo, 12 de octubre de 2012

VISTO: La consulta formulada en obrados respecto a los casos de interoperabilidad o intercambio de información entre Organismo públicos (art. 157 ley 18719), que implican comunicación de datos personales y donde aplica la excepción del literal b del art. 9 (al cual remite el art. 17), ello también implica el relevo del control de los fines vinculados con el interés legítimo (art. 17) o solo refiere al consentimiento. Formula la misma consulta para cuando opera la excepción del literal c del art. 9 en referencia al control del interés legítimo".

CONSIDERANDO:

I) Que el art. 158 de la Ley Nº 18.719 de 27 de diciembre de 2010, establece que a los efectos del intercambio de información entre Entidades Públicas, estatales o no, una de las obligaciones consiste en recabar el consentimiento, de acuerdo con lo previsto en la Ley Nº 18.331, cuando el objeto de intercambio refiere a información privada o de particulares que requiere el previo consentimiento informado.

II) Que el art. 159 establece que las Entidades Públicas deberán ajustar su actuación a una serie principios, como por ejemplo el de previo consentimiento informado, el de finalidad, el de confidencialidad y seguridad, por lo cual, aún respecto a aquellos datos que no requieren previo consentimiento informado, también se deberán observar el resto de los principios que estructuran la Ley Nº 18.331.

III) Que debido a ello, cuando se intercambia determinada información entre organismos debe considerarse especialmente el marco de las competencias que le han sido asignadas legalmente a cada uno de ellos, a efectos de determinar si es posible o no aplicar algunas de las excepciones establecidas en la Ley.

IV) Que en definitiva, aunque no sea necesario recabar el consentimiento sí deberá atenderse a la finalidad, al marco legal y a los cometidos de cada organismo interviniente, las cuales deben corresponderse con el interés que subyace, tanto en las gestiones que atañen a los propios usuarios, como en los servicios que debe brindar el Estado para cumplir con sus funciones.

V) Que para complemento de lo anterior se considera que el art. el art. 159 de la Ley Nº 18.719, establece un marco de actuación cuyo procedimiento debe ser iniciado con la presentación de una solicitud fundada y firmada por el jerarca del organismo emisor, ante el jerarca del organismo receptor, y que los acuerdos además deberán establecer las condiciones, protocolos y criterios funcionales o técnicos con los que se llevaran a cabo dichos intercambios, todo lo cual debe ser interpretado como parte del control de la finalidad y el interés legítimo, más allá de que no se requiera obtener el previo consentimiento informado en las hipótesis previstas en la Ley N O 18.331 art. 9 B) y C).

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que si bien en los casos comprendidos dentro de las excepciones, no debe recabarse el previo consentimiento informado, si deberá atenderse a la finalidad e interés legítimo, así como a los cometidos específicamente establecidos por Ley a los organismos intervinientes.

2.- Notifíquese, publíquese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
29/012	2012-2-10-0000755

Montevideo, 13 de diciembre de 2012

VISTO: La consulta formulada el Fondo de Solidaridad en cuanto a si se encuentra habilitada para obtener cierta clase de datos personales que disponen los organismos tributarios recaudadores, para el mejor cumplimiento de sus cometidos.

RESULTANDO:

I) Que el órgano consultante es una persona de derecho público no estatal creada por la Ley N O 16.254 con el cometido de gestionar un sistema de becas de ayuda para la educación terciaria, mediante los fondos obtenidos de los organismos de recaudación tributaria en concepto de una contribución especial creada por la misma ley.

II) Que en orden al cumplimiento de estos cometidos, se alega no disponer de información actualizada acerca de los sujetos pasivos del tributo que administra, fundamentalmente por lo que hace al domicilio y otros datos de contacto.

III) Que la carencia anotada proviene de la circunstancia de que los registros que utiliza hasta este momento son los provenientes de la Universidad de la República, en su gran mayoría correspondientes a la época en que el profesional culminara sus estudios.

IV) Que ello ocasiona que el consultante no disponga de datos de contacto actualizados, que le permitan ejercitar sus cometidos legales con efectividad, vale decir promover el cumplimiento voluntario y sucedáneamente por medio de medidas administrativas y judiciales, de las obligaciones de los contribuyentes.

V) Que por el contrario, una información de este tenor actualizada es la que se encuentra en poder de la Caja de Jubilaciones y Pensiones de Profesionales Universitarios (CJPPU), la Caja Notarial de Seguridad Social (CNSS), la Dirección General Impositiva (DCI) y el Banco de Previsión Social (BPS).

CONSIDERANDO:

I) Que el art. 6 del Decreto N O 325/002 en redacción dada por el art. 1 0 del Decreto N O 477/011, al reglamentar la Ley N O 16.254, precisa las facultades del órgano consultante para obtener la información que pretende.

II) Que el intercambio de información entre entidades públicas, estatales o no, está regulado por los arts. 157 a 160 de la Ley Nº 18.719, entre cuyas obligaciones figura la de recabar el consentimiento de acuerdo con lo previsto en la Ley Nº 18.331.

III) Que de su parte la comunicación de datos personales está regulada en el art. 17 de la Ley Nº 18.331, y tiene como exigencias de regla o principio dos requisitos, a saber la existencia de un interés legítimo en emisor y receptor, y el previo consentimiento del titular de los datos.

IV) Que en el ocurrente, el interés legítimo en la comunicación aparece explicado y justificado, mientras que el requisito del consentimiento es abatible a través de algunas de las hipótesis que admite el régimen, y que para el caso son los "listados limitados" (art, 90 inc. 30 lit. C de la Ley), y "el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal" (art. 90 inc. 30 lit. B de la Ley).

V) Que aún cuando no se recabe el consentimiento de los titulares de los datos, procede de todos modos atenerse al cumplimiento de los restantes preceptos del régimen, en especial el respeto de la finalidad perseguida (contacto y facilitación para la adopción de medidas tendientes al cumplimiento voluntario o forzado de las obligaciones a cargo del contribuyente), limitación de la comunicación a aquellos datos estrictamente necesarios a esa finalidad, mantener la reserva y seguridad de los datos obtenidos, e inscribir la base de datos en el Registro que lleva la Unidad.

ATENTO: A lo precedentemente expuesto, lo dispuesto por la normativa citada en el cuerpo, el art. 34 lit. F de la Ley N O 18.331 de 11 de agosto de 2008, y el Informe Letrado N O 515/2012,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

Que el Fondo de Solidaridad está habilitado para requerir la comunicación de datos personales de los sujetos pasivos del tributo que administra, a los organismos y con el alcance planteado en los **CONSIDERANDOS** del presente Dictamen.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

m.b.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
31/012	2012-2-10-0000855

Montevideo, 20 de diciembre de 2012

VISTO: La consulta formulada en cuanto a la legalidad de la comunicación de las imágenes almacenadas en videocámara, a solicitud de terceros.

RESULTANDO:

I) Que un cliente habría olvidado su aparato telefónico celular en el mostrador de la consultante, y existen elementos de sospecha de que el mismo podría habérselo apropiado otra persona que se hubiera aproximado luego al mismo mostrador.

II) Que la consultante dispone de videocámara en el lugar, ubicado dentro de un shopping center, en la que podrían haber quedado registradas las imágenes correspondientes a este insuceso.

III) Que el personal de seguridad del shopping center le ha solicitado a la consultante la comunicación de dichas imágenes, lo que motiva la presente consulta.

CONSIDERANDO:

I) Que las imágenes de personas constituyen datos personales a los que se aplica el régimen jurídico de protección de datos personales según lo ha edictado ya la Unidad a través de su Dictamen N O 10 de 16-04-2010.

II) Que sin perjuicio de otros, existen en la materia dos principios o reglas esenciales, que son el de reserva y el de consentimiento.

III) Que en virtud de la aplicación y juego armónico de ambos principios, la respuesta a la consulta formulada será negativa ya que no se observa que existan en el caso ninguna de las condiciones o hipótesis legales en las que procede comunicar datos personales a terceros, por parte de quien dispone de ellos.

IV) Que en casos como el ocurrente, corresponde que el propio responsable de la base de datos de videovigilancia, a través de personal autorizado, verifique si se cumplen las sospechas existentes, y en su caso de trámite a la intervención policial y judicial correspondientes.

V) Que en cuanto al personal de seguridad del shopping center se le puede brindar un informe objetivo de lo que arroje la visualización de las imágenes, siempre que no permita identificar ni hacer identificable al presunto autor del delito, labor que -como ya se expresara- es de cargo de las autoridades competentes.

VI) Que toda base de datos pública o privada debe inscribirse en el Registro habilitado al efecto por la Unidad, deber que el consultante no ha cumplido y deberá hacerlo.

ATENTO: A lo precedentemente expuesto, lo dispuesto por los arts. 40 lit. D, 90 inc.3º lit. B, 17 inc. 30 lit. B, 29 y 34 lit. A de la Ley Nº 18.331 de 11 de agosto de 2008, el Dictamen Nº 10 de 16-04-2010 y el Informe Letrado Nº 508/2012.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Ratificar lo resuelto en este órgano por Dictamen Nº 10 de 16 de abril de 2010, en cuanto a que las imágenes almacenadas en videocámaras colocadas en lugares de uso público, constituyen una especie de datos personales abarcada, como tal, por la Ley NO 18.331 y sus normas complementarias.

2.- En consecuencia, salvo consentimiento del titular, o ejercicio de funciones propias de los poderes del Estado, u obligación legal, u orden de la justicia competente, no procede revelar dichas imágenes ni comunicarlas a terceros.

3.- Intímese a AA Uruguay S.R.L. el registro de su base de datos personales de videovigilancia y toda otra de la que sea responsable, en el plazo de treinta (30) días, y bajo apercibimiento.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

m.b.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
05/013	2013-2-10-000096

Montevideo, 14 de marzo de 2013

VISTO: La consulta conjunta formulada por el Banco de Previsión Social (BPS), el Ministerio de Educación y Cultura (MEC) y las Asociaciones que vinculan a las Instituciones de Enseñanza Privada (EIHU-IAHU y AUDEC), respecto a si resulta acorde al régimen de protección de datos personales solicitarle a las Instituciones de Enseñanza Privada los datos de escolares y liceales que se especifican en la consulta, con la finalidad de facilitar el otorgamiento y control del beneficio de Asignación Familiar que sirve el Ente.

RESULTANDO:

I) Que el planteo se basa en razones de buena administración, en la medida que, como se sostiene, la comunicación redundará en beneficio de los propios beneficiarios y se cumplirá real y efectivamente la legislación vinculada a dicha prestación, al tiempo de evitar tener que citar a cada interesado para volver a requerirle una información que ya está disponible.

II) Que los datos cuya comunicación se pretende son: cédula de identidad, nombre completo, fecha de nacimiento, fecha de matriculación, indicador de permanencia en los estudios (o asistencia regular, o progreso educativo) que justifica ser acreedor de la prestación, indicador de recibo o postulación a recibir el beneficio.

CONSIDERANDO:

I) Que la comunicación en los términos planteados, se enmarca en los principios que rigen la materia de protección de datos personales, en particular los de legalidad, veracidad (por lo que refiere a su adecuación, ecuanimidad y no excesividad), y finalidad.

II) Que de acuerdo con el régimen legal vigente no resulta necesario contar con el consentimiento de los titulares de los datos (o de sus representantes legales en el caso), para comunicaciones del orden de las que plantea la consulta, circunscripta a datos de personas y grupos familiares atributarios del régimen de Asignación Familiar, no así a todos los alumnos.

ATENTO: A lo precedentemente expuesto, al Informe Letrado que antecede, y a lo dispuesto por los artículos 60 70 80 y 90 lits. B y C, y 17 lit. B de la Ley 18.331 y sus modificativas, así como en las Leyes Nros. 15.084 y 18.227.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

Se considera lícita la comunicación de datos personales que plantea la consulta, en poder de las Instituciones de Enseñanza Privada al Banco de Previsión Social, no requiriendo el consentimiento de los titulares respecto, específicamente, a personas y grupos familiares que son atributarios o gestionantes del beneficio de Asignación Familiar, a los efectos de facilitar y controlar el otorgamiento y mantenimiento de éste; para otros casos, se tendrá por lícita la comunicación solamente con consentimiento del titular de los datos, o sus representantes legales, en los términos que prevé la Ley Nº 18.331.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

m.b.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
08/013	2013-2-10-0000051

Montevideo, 21 de marzo de 2013

VISTO: La consulta formulada por la Dirección General de Registro de Estado Civil referida al alcance que posee la Ley N O 18.331 respecto a la información contenida en Acta y Certificado de Defunción del Mtro. Julio Castro.

RESULTANDO:

I) Que a pedido expreso de un familiar se incluye en el Acta de Defunción la causa de su muerte que ha sido determinada por el Equipo de Médicos Forenses, como resultado del "disparo de arma de fuego en contexto de tortura y malos tratos".

II) Que sin embargo, la Dirección General del Registro de Estado Civil dictó una circular (Circular N O 2/2012 de 2 de marzo de 2012), en la que se establece que al labrar el acta de defunción, ya sea en certificado electrónico o en papel, no deberá dejarse constancia de la causa de la muerte si en el certificado no viene establecida. En caso de que se haya indicado, deberá dejarse constancia de que es reservada de acuerdo a la normativa de datos personales.

CONSIDERANDO:

I) Que corresponde analizar los fundamentos legales de dicha reserva establecida en el Decreto del Poder Ejecutivo de 8 de diciembre de 2011 sobre Certificado de Defunción Electrónica, recogidos en la Circular Nº 2/2012 de la Dirección General de Registro: Ley Nº 18.335 sobre Derechos de los Pacientes y Usuarios y su Decreto Nº 274/010 y Ley Nº 18.331 de Protección de Datos y Acción de Habeas Data.

II) Que de la Ley Nº 18.335 y su Decreto, no surge en forma expresa que la causa de la muerte deba ser considerada, por sí sola, un dato clínico reservado, sino que esas normas refieren al tratamiento de la información que consta en la historia clínica (propiedad del paciente), CONSIDERANDO que es reservada y que debe ser tratada de acuerdo a lo previsto en su art. 18. Además según lo indica el art. 10, regula los derechos y obligaciones de los pacientes y usuarios de los servicios de salud, con respecto a los trabajadores de la salud y a los servicios de atención de la salud, en virtud de ello no corresponde su aplicación al caso que se consulta.

III) Que respecto a la Ley N O 18.331, cabe considerar que si bien se establece la reserva como uno de sus principios, también hay excepciones que deben ser debidamente armonizadas con los demás derechos que se contraponen en cada caso concreto.

IV) Que el art. 17 establece que los datos personales objeto de tratamiento podrán ser comunicados sin previo consentimiento cuando así lo disponga una ley de interés general, por ello en este caso, deberían considerarse especialmente tanto la Ley N O 18.381 de Acceso a la Información Pública (arts. 9, 10 y 12), como la Ley N O 18.596 de Actuación Ilegítima del Estado entre el 13 de junio de 1968 y el 28 de febrero de 1985 y Reconocimiento y Reparación a las Víctimas, además de la normativa de derecho internacional de los DD.HH que nuestro país a ratificado y que garantiza derechos a las víctimas de terrorismo de Estado.

V) Que el art. 17 a su vez señala, que no será necesario el consentimiento, cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. En el caso del Mtro. Julio castro, la causa de la muerte es un dato que ha sido publicado en

diversos medios de información, así como ya es parte de libros o informes oficiales que tienen circulación pública y masiva.

VI) Que para finalizar, corresponde la aplicación de la modificación introducida al art. 9 de la Ley Nº 18.331, por el art. 43 de la Ley Nº 18.996 de 7 de noviembre de 2012, estableciendo que se consideran como fuentes públicas o accesibles al público, entre otras, a las publicaciones oficiales y las publicaciones en medios masivos de comunicación, en cualquier soporte, así como a todo registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos, puedan ser consultados, difundidos o utilizados por parte de terceros.

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que desde el punto de vista de la protección de datos personales, la Dirección General de Registro de Estado Civil se encuentra habilitada para incluir la causa de la muerte en el Acta y en la Partida de Defunción del Mtro. Julio Castro.

2.- Notifíquese, publíquese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
17/013	2013-2-10-0000050

Montevideo, 29 de mayo de 2013

VISTO: La consulta del Sr. Arturo Toscano, acerca de la legalidad del procedimiento de respaldo de la información personal e institucional que guardaba en la computadora que utilizaba en el trabajo.

RESULTANDO:

Que se trata de un funcionario que utiliza una PC institucional y un servidor de correo Outlook, tanto para sus actividades personales como laborales.

CONSIDERANDO:

I) Que corresponde analizar el derecho del funcionario a la privacidad y a protección de sus datos personales en el ámbito laboral, así como de la potestad de control y de discrecionalidad que posee la administración pública en el ámbito de sus funciones, con relación a las actividades desarrolladas por éste, así como de sus recursos.

II) Que el respaldo de la información de su PC ha sido realizado por la Dirección Nacional de Innovación, Ciencia y Tecnología (DICyT), dirección dependiente del MEC, creada por la Ley N O 17.930 con el cometido de elaborar e impulsar las políticas, lineamientos, estrategias y prioridades del Ministerio en materia de innovación, ciencia y tecnología.

III) Que respecto a la pertenencia del correo otorgado al trabajador, es clara la jurisprudencia laboral en cuanto a considerar que es una herramienta y un recurso propio del empleador, entregado en tal carácter para que se cumpla con las tareas asignadas.

IV) Que además hay que tener presente que los tribunales laborales han entendido que, más allá de la debida protección de la intimidad y la privacidad de los trabajadores, hay un margen de control al que tienen derecho los empleadores.

V) Que por otra parte, si bien no ha existido un consentimiento expreso se puede inferir que el mismo está implícito en la relación laboral que se mantiene con el organismo, además de que el art. 9º B) de la Ley establece que no se requiere el consentimiento cuando los datos se recaben para el ejercicio de las funciones propias de los poderes del Estado o en virtud de una obligación legal.

VI) Que no obstante ello, cada responsable de base de datos o de tratamiento de datos, está obligado a adoptar medidas de seguridad para proteger adecuadamente los datos personales que posee (arts. 10, 11 y 12 de la Ley N O 18.331).

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que no se ha vulnerado la Ley NO 18.331, ya que la actuación del Ministerio de Educación y Cultura se enmarca en los principios de finalidad, necesidad y proporcionalidad en el cumplimiento de sus funciones (art. 9º B).

2.- Establecer que el consentimiento del consultante es parte de la relación contractual según lo expresado en el art. 9º D).

3.- Establecer asimismo que es obligación del organismo utilizar esa información sólo para la finalidad para la cual ha sido recabada según lo establecido en el art. 8 de la Ley, así como que deberá garantizar su seguridad y confidencialidad.

4.- Notifíquese, publíquese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
21/013	2013-2-10-0000219

Montevideo, 4 de julio de 2013

VISTO: La consulta formulada por el Sr. Guillermo Winkler sobre adecuación de la base de datos de recomendaciones empresariales al marco legal establecido por la Ley N O 18.331.

RESULTANDO:

Que se trata de un sistema de referencias empresariales, donde cada empresa afiliada, podrá ingresar cédula y nombre del empleado y una evaluación numérica que indique si lo recomienda o no lo recomienda.

CONSIDERANDO:

I) Que para poder consultar las referencias incluidas en el sistema, las empresas deberán estar afiliadas y obtener el consentimiento previo de las personas, que les proveerán con cédula de identidad para que se pueda realizar la búsqueda. Además el sistema no permite emitir listados ni navegar la información de personas que no hayan brindado el consentimiento para la consulta.

II) Que el art. 17 de la Ley establece que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos.

III) Que en el caso, si bien existe interés legítimo del emisor y del destinatario, no se puede inferir el consentimiento del trabajador del contexto de la relación laboral o contractual, ni por la entrega de la Cl, pues el sistema que instituye la Ley no se basa en el consentimiento tácito sino en el consentimiento expreso (art. 90 primera parte).

IV) Que en este sentido, si bien el art. 90 D) de la Ley establece la excepción al consentimiento cuando los datos deriven de una relación laboral o contractual, y sean necesarios para su desarrollo o cumplimiento, en el caso hay que diferenciar entre la relación en sí, y la posibilidad de ser incluido en esta base de datos de referencias empresariales, pues esto último no es necesario para el desarrollo o cumplimiento de la relación de que se trate, -exigencia prevista en el art. 90 D)-, por ende, debe solicitarse el consentimiento en forma expresa, ya sea mediante un formulario o una cláusula específica.

V) Que por otra parte, los trabajadores cuyos datos van a ser ingresados en el sistema y eventualmente comunicados, deben ser informados de la finalidad de la base y de esa eventual comunicación, en los términos establecidos en el art. 13 de la Ley.

VI) Que **CONSIDERANDO** lo establecido en el art. 70 de la Ley, la recomendación en sí deberá ser lo más objetiva posible, sin juicios de valor que puedan vulnerar la integridad de las personas, y sin la inclusión de datos sensibles que puedan constituirse en una forma de discriminación, así como la recolección de estos datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a la Ley.

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que debe recabarse el consentimiento en forma expresa mediante un formulario o cláusula específica que debe ser firmada por los trabajadores, conforme lo establecido en el art. 9 0 de la Ley 18.331.

2.- Establecer además que deberán ser informados en los términos previstos en el art. 13 de la Ley, así como el responsable de la base deberá adoptar las medidas de seguridad adecuadas, e inscribir la base de datos en el registro de la URCDP, dentro de los 90 días siguientes a su creación.

3.- Notifíquese, publíquese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
22/013	2013-2-10-0000130

Montevideo, 4 de julio de 2013

VISTO: La consulta de la Intendencia de Montevideo sobre inclusión en sitio web datos índice de archivo de Registro Civil.

RESULTANDO:

Que se considera la posibilidad de publicar en la web institucional el índice de archivo del Servicio de Registro de Estado Civil, con carácter de "dato abierto", pues los datos a los que podría accederse con esta publicación, no son datos que requieren previo consentimiento informado.

CONSIDERANDO:

I) Que los datos serían los siguientes: nombre completo de la persona y su fecha de nacimiento, matrimonio o defunción, con referencia al Año, Sección y Número de Acta, sin asociar la imagen de la partida de que se trate.

II) Que respecto al carácter de "dato abierto", corresponde mencionar que el criterio aplicado por la IM, -y plenamente compartido-, siempre ha consistido en asegurarse que los datos que publica con este carácter sean efectivamente públicos, en definitiva que no se trate de información reservada, confidencial o secreta, según lo establecido en la Ley N O 18.381 de Acceso a la Información Pública y en la Ley N O 18.331 de Protección de Datos Personales y Acción de Habeas Data. 18.331).

III) Que en nuestro país, de acuerdo con la Ley N O 18.331, cualquier iniciativa de datos abiertos debe considerar el anonimato de personas tanto físicas como jurídicas, pues el art. 4 o de esta Ley establece que dato personal se trata de información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

IV) Que el art. 9 Literal C) de esta norma indica que el tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse, agregando que éste será necesario el previo consentimiento cuando: C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, por lo tanto algunos de los datos que se van a publicar no están incluidos en este listado.

V) Que la función del Registro de Estado Civil es anotar los hechos o actos que atañen al estado civil, con la intervención de un funcionario público competente (Oficial del Estado Civil) en los libros correspondientes y con las formalidades que la ley prescribe.

VI) Que por ende esto debe estar en consonancia con lo establecido en el art. 17 de la Ley que indica que la comunicación de datos personales objeto de tratamiento, sólo podrá realizarse para cumplir con los fines directamente relacionados con el interés legítimo del emisor y del destinatario, con el previo consentimiento del titular, salvo que así lo disponga una ley de interés general o en los dispuestos del art. 9 0 (por ejemplo los listados), o los datos sean disociados (anonimizados).

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que la publicidad de determinados datos personales, como los datos de matrimonio o de defunción, sin el consentimiento del titular, vulneran las disposiciones de la Ley NO 18.331.

2.- Establecer que el tratamiento de estos datos debe ajustarse a los principios de proporcionalidad (art. 70) y de finalidad (art. 8 0), así como a lo establecido en los arts. 90 y 17 A), por lo que el índice debería publicarse sin los datos antes indicados o sin identificar a los titulares de los mismos (art. 17 D).

3.- Notifíquese, publíquese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
29/013	2013-2-10-0000391

Montevideo, 24 de octubre de 2013

VISTO: La consulta formulada por la Ing. Sabrina Trotta Mouriño de la Secretaría del Departamento de Informática del Ministerio del Interior (Ml).

RESULTANDO:

I) Que el Ml trabaja en la elaboración del pliego de un proyecto que comprende la inclusión de una cédula de identidad electrónica (CIE), con el objetivo de que la misma sea un documento de viaje conforme al ICAO 9303.

II) Que dicha CIE presentará información visible (como hasta ahora) e información digital almacenada en chips de dos tipos: uno con contacto y otro sin contacto. El chip con contacto para ser leído requiere de un dispositivo de lectura, mientras que el chip sin contacto puede ser leído con un dispositivo de lectura autorizado a una distancia máxima de 10 cm entre lector y Cl.

III) Que se consulta acerca de que datos se pueden o no, almacenar en el chip sin contacto, **CONSIDERANDO** que el ICAO 9303 ha determinado como obligatorios los siguientes: tipo de documento, Estado u organismo expedidor, nombre (del titular), número de documento, dígito de control número de documento, nacionalidad, fecha de nacimiento, dígito de control - fecha de nacimiento, sexo (de nacimiento (N) y sexo actual (A), en formato N/A), fecha de expiración o válido hasta y rostro. Las principales dudas surgen con los datos relativos al sexo y al rostro.

CONSIDERANDO:

I) Que de acuerdo con la Ley N O 18.331, arts. 18 y 19, hay datos personales que requieren de una protección especial para ser tratados y almacenados, por considerarse datos sensibles.

II) Que no obstante ello corresponde tener presente que existen obligaciones a cargo de los Estados, que implican instrumentar las medidas necesarias y adecuadas, para garantizar y proteger los derechos humanos de todas las personas, incluyendo la seguridad pública.

III) Que en este sentido el art. 18 que establece que los "datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo."

IV) Que se infiere de la consulta que se trata de cumplir con las funciones que posee el Ml en materia de seguridad pública, para lo cual es necesario identificar en forma certera y precisa, a todas las personas, especialmente en lugares de entrada y salida del país como los aeropuertos.

V) Que se indica en la consulta que los datos solicitados se enmarcan en el Documento ICAO 9303 que se trata de un material elaborado por la Organización de Aviación Civil Internacional, que recomienda las características que deben tener los documentos de viaje de lecturas mecánicas.

VI) Que en cuanto al rostro, cabe destacar que se trata de un dato biométrico así como el reconocimiento facial, se trata es una aplicación dirigida por un programa informático, destinado a identificar automáticamente a una persona en una imagen digital, mediante la comparación de determinadas características faciales existentes en una base de datos, por lo cual se recomienda su uso al sólo efecto de dicha verificación.

VII) Que en razón de ello, los elementos biométricos en los pasaportes, en otros documentos de viaje o en los carnés de identidad son muy sensibles, por lo cual debe garantizarse que sólo las autoridades competentes pueden acceder a los datos almacenados en el chip.

VIII) Que lo delicado del tema obliga a utilizar sistemas seguros, que entre otras cosas, impidan que se memoricen los rostros por parte de terceros no autorizados, que el acceso a las imágenes de reconocimiento facial esté restringido sólo a las autoridades competentes, así como debe utilizarse una arquitectura de seguridad que proporcione un nivel adecuado para el intercambio de dicha información, como por ejemplo, una Infraestructura de Clave Pública Global (PKI), que afortunadamente Uruguay ya posee (Ley N O 18.600 de Documento y Firma Electrónica y su Decreto 436 de 8 de diciembre de 2011.

IX) Que en definitiva, si bien el art. 3 0 de la Ley N O 18.331, indica que las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado, quedan excluidas de su ámbito de aplicación, corresponde que desde la perspectiva de un derecho humano como lo es la protección de datos personales, se consideren las recomendaciones formuladas por la URCDP.

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Establecer que solamente corresponderá el acceso a datos de sexo y de rostro, de la cédula de identidad electrónica (Cl) a las autoridades competentes y que su recolección y almacenamiento, se realicen a los exclusivos efectos de la seguridad pública, en el marco del cumplimiento de las funciones y cometidos que posee el Ministerio del Interior, en consonancia con los principios de finalidad y proporcionalidad previstos en la Ley Nº 18.331.

2.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
30/013	2013-2-10-000029

Montevideo, 24 de octubre de 2013

VISTO: La consulta formulada por el Sr. Luis Edgardo Olivera, acerca de la existencia de mecanismos de control sobre plazos de conservación de los datos de carácter objetivo, así como lo que sucede en caso de que existan inscripciones sucesivas en diferentes bases de datos de este tipo.

RESULTANDO:

Que las bases de datos que brindan información comercial de carácter objetivo, se nutren con los datos informados por las entidades adheridas a determinadas empresas especializadas en el tema, responsables de las mismos y que brindan ese servicio, así como también se pueden conformar con datos obtenidos de fuentes de acceso público.

CONSIDERANDO:

I) Que la legalidad, respecto a los datos, objeto de recolección y tratamiento, se encuentra regulada en forma explícita en la Ley Nº 18.331, art.22.

II) Que el contenido de dichas bases, debe estar únicamente referido a la "solvencia patrimonial o crediticia", de forma tal que se pueda determinar la solvencia económica actual del interesado, por ello es muy importante que se ajusten a los principios de finalidad, proporcionalidad y calidad de la información.

III) Que sólo existen dos formas de control: a) el que puede realizar el interesado o titular perjudicado por este tipo de registro, a través del ejercicio de los derechos que se consagran en la Ley (arts. 14 y 15), y b) el control que realiza la URCDP, como Órgano Regulador que tiene a su cargo la tuición del tratamiento de los datos personales en sentido amplio, incluido el control de lo establecido en el artículo 22 con plena competencia para ello.

IV) Que respecto al control de la URCDP, cabe tener presente que toda persona física o jurídica que posea una base de datos de este tipo tiene la obligación de inscribirla en el registro (art. 28 de la LPDP), por ende la Unidad realiza el control correspondiente cuando la base se inscribe, contrastando la información que se proporciona con lo establecido en la Ley, así como también cuando se reciben consultas o denuncias de particulares.

V) Que por otra parte, el Consejo Ejecutivo de la URCDP tiene potestades sancionatorias ante el incumplimiento de la LPDP, pudiendo imponer sanciones de apercibimiento, multa de hasta quinientas mil unidades indexadas y clausura de las bases de datos por un plazo de hasta seis días hábiles (artículo 35 de la LPDP).

VI) Que respecto a la posibilidad de inscripción sucesiva, el acreedor puede inscribir en diferentes bases al deudor, pero si ello no se ajusta a la realidad o si es incorrecto incurrirá en responsabilidad, por lo cual tiene obligación de controlar la veracidad de los datos y los plazos, así como tener presente el derecho a inscribir sólo por una vez más, si pasado el plazo de 5 años inicial, la deuda se mantiene impaga.

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Informar al consultante que la legalidad respecto al objeto de la recolección y tratamiento de estos datos se encuentra regulada en forma explícita en art. 22 de la Ley 18.331, así como existen mecanismos de control, tanto a cargo de los propios interesados a través del ejercicio de los derechos que se consagran en la Ley (arts. 14 y 15), y b), como a cargo de la URCDP.

2.- Notifíquese, publíquese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
01/014	01/014

Montevideo, 05 de febrero de 2014

VISTO: Las modificaciones introducidas por la Ley NO 18.996, de 7 de noviembre de 2012, al agregar el artículo 9 bis a la Ley N O 18.331, de 11 de agosto de 2008.

RESULTANDO:

I) Que el artículo 9 bis de la Ley NO 18.331, establece que se consideran como públicas o accesibles al público, las siguientes fuentes o documentos:

A. El Diario Oficial y las publicaciones oficiales, cualquiera sea su soporte de registro o canal de comunicación.

B. Las publicaciones en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que figuren o el canal a través del cual se practique la comunicación.

C. Las guías, anuarios, directorios y similares en los que figuren nombres y domicilios, u otros datos personales que hayan sido incluidos con el consentimiento del titular.

D. Todo otro registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros. En caso contrario, se podrá hacer uso del registro o publicación mediante técnicas de disociación u ocultamiento de los datos personales.

II) Que dicha disposición refiere a datos que ya se encuentran en fuente pública relacionados a la identidad de su titular.

CONSIDERANDO:

I) La necesidad de interpretar el tratamiento de datos personales no vinculados a la identidad de su titular.

II) Que los datos personales que no requieren previo consentimiento informado deben estar contenidos en listados.

III) Que por dictamen NO 26/2013, esta Unidad ha entendido que la palabra "listados" al no haber sido definida expresamente por el legislador, debe ser entendida en su sentido natural y obvio, según el uso general; y que de acuerdo con La Real Academia Española, listado viene del participio listar, que significa formar o tener listas, enumeración, generalmente en forma de columna, de personas, cosas, cantidades, que se hace con determinado propósito.

IV) Que toda interpretaci6n sistemática y contextual de la Ley Nº 18.331, debe realizarse de acuerdo con los principios rectores. Esta posición fue sostenida tanto por la URCDP como por la Unión Europea durante el trámite de adecuación, quedando plasmado así en la Decisión de Ejecución de la Comisión Europea de 21 de agosto de 2012, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales

ATENTO: A lo expuesto, a lo previsto en las normas legales citadas y en el articulo 34 literales A) y B) de la Ley Nº 18.331,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que el artículo 9 bis de la Ley refiere a datos que ya se encuentran en fuente pública relacionados a la identidad de su titular.

2.- Que conforme a lo dispuesto en el Dictamen NO 26/2013, los datos personales que no requieren previo consentimiento informado deben estar contenidos en "listados" al momento de su recolección.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

c.e.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
02/014	2012-2-10-0000937

Montevideo, 13 de febrero de 2014

VISTO: : La consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones (URSEC), respecto a la procedencia de publicar sanciones aplicadas a funcionarios públicos en su sitio web, sin vulnerar las disposiciones de la Ley N O 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data y su decreto reglamentario Nº 414/009 de 31 de Agosto de 2009.

CONSIDERANDO:

I) Que de acuerdo con lo estipulado en el principio de finalidad, previsto en el artículo 8 de la Ley Nº 18.331, los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles a aquellas que motivaron su obtención, debiendo ser eliminados una vez que hayan dejado de ser pertinentes a los fines para los cuales hubieren sido recolectados, evitando una perpetuidad en la sanción aplicada y consecuentemente perjuicios tales como los derivados del derecho al olvido.

II) Que será el responsable del contenido del sitio web, quien decida qué información será publicada, y por cuánto tiempo permanecerán esos datos disponibles en Internet, así como la aplicación de posibles controles o filtros a efectos de evitar la indexación por diversos motores de búsqueda, respecto a las resoluciones que contengan información personal, evitando una prolongación indeterminada en el tiempo y el espacio lo que naturalmente podría producir perjuicios al titular de los datos en cuestión.

III) Que salvo que exista interés público en conocer la identidad de los involucrados, correspondería aplicar a las resoluciones que contengan información de carácter personal un procedimiento de disociación de los datos, tal como se establece en el art. 17 literal D) de la Ley Nº 18.331.

ATENTO: A lo expuesto por las disposiciones de la Ley Nº 18.331, de 11 de Agosto de 2008 y en su decreto reglamentario Nº 414/009 de 31 de Agosto de 2009.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Señalar que la publicación de resoluciones que imponen sanciones a funcionarios públicos en el marco de las obligaciones de transparencia activa del organismo, no vulnera las disposiciones de la Ley Nº 18.331, en tanto se hayan considerado los principios y excepciones previstas en la norma.

2.- Salvo que exista interés público en conocer la identidad de los involucrados, caso en que deberá atenderse a lo detallado en los considerandos I y ll, se recomienda aplicar a las resoluciones que contengan información personal un procedimiento de disociación de los datos, tal como se establece en el art. 17 inc. D) de la Ley Nº 18.331.

3.- Notifíquese, publíquese y oportunamente archívese

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

f.a.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
08/014	2014-2-10-0000233

Montevideo, 23 de julio de 2014

VISTO: La consulta formulada por el Ing. Rafael Méndez de Integración AFAP sobre tratamiento de datos en la nube.

RESULTANDO:

I) Que Integración AFAP está en proceso de selección de un CRM y una de sus opciones es el software RightNow de la firma Oracle en modalidad SaaS, por tanto la aplicación y los datos contenidos en ella estarán en la nube de Oracle.

II) Que según el proveedor esa nube tiene varios Datacenter en distintas partes del mundo para asegurar la disponibilidad del servicio.

III) Que Integración AFAP tiene cerca de 200.000 afiliados, cuyos datos personales serán accedidos desde el CRM, y se almacenarán como mínimo: nombre, dirección, teléfono, sueldo, lugar de trabajo, fecha de nacimiento.

CONSIDERANDO:

I) Que la situación encuadra dentro del ámbito de aplicación definido por la Ley Nº 18.331 (art. 3º) y en las hipótesis previstas en los Literales A y B del artículo 3 0 del Decreto Nº 414/009, reglamentario de la Ley.

II) Que corresponde determinar si se está o no ante una transferencia de datos en el sentido establecido en el art. 40 Literal H) de dicho Decreto.

III) Que en la consulta se indica que los datos "se subirán" a la nube, por lo cual habría transferencia ya que la base se encuentra en un servidor ubicado en el exterior del país aunque sea a modo de respaldo.

IV) Que es fundamental destacar que se está ante una transferencia internacional de datos, **CONSIDERANDO** especialmente en este sentido, la importancia que tiene que, tanto el servicio como los respaldos, se encuentren ubicados en países adecuados en materia de protección de datos personales.

ATENTO: A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Indicar que en la situación planteada en la consulta formulada por Integración AFAP en estos obrados existe transferencia internacional de datos en el sentido de lo establecido en la Ley 18.331 y su decreto reglamentario 414/009, en especial su art 4 0 Literal H).

2.- Hacer saber que en virtud de la legislación citada en el numeral anterior, tanto el servicio como los respaldos, deberán ubicarse en países adecuados en materia de protección de datos personales.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
12/014	2014-2-10-0000281

Montevideo, 04 de setiembre de 2014

VISTO: La consulta presentada por el Ministerio de Salud Pública en relación con el certificado de defunción y el certificado de defunción resumido en cuanto a su publicación en la web.

CONSIDERANDO:

I) Que tanto el certificado de defunción como el certificado de defunción resumido contienen datos personales y datos personales sensibles (artículo 41 literales D) y E) de la Ley N O 18.331).

II) Que para ambos tipos de datos es necesario el consentimiento libre, previo, expreso, informado y documentado de su titular, agregándose como requisito para los datos sensibles estar por escrito.

III) Que el Ministerio de Salud Pública y el Instituto Nacional de Estadística están realizando un trabajo de colaboración para la publicación de los certificados de defunción y de nacido vivo en la página web. Dicha publicación podrá ser realizada si se tiene el consentimiento del titular del, dato, en el caso de las defunciones aquél de sus herederos, con la excepción prevista en el artículo 90 literal C) de la Ley N O 18.331 y si se disocian los datos.

IV) Que los certificados de defunción no están comprendidos dentro del concepto de fuente pública establecido en el artículo 91 bis, de la Ley, por lo que la entidad pública que podría proporcionarlos es la Dirección General del Registro de Estado Civil en su carácter de registro público y no el Ministerio de Salud Pública.

ATENTO: A lo expuesto, y a lo previsto en la Ley N O 18.331, arts. 41 literales D) y E), 16 y 18 y al Decreto NO 431/011, de 4 de diciembre de 201 1 y normas concordantes.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Para la publicación de los certificados de defunción en la página web, el Ministerio de Salud Pública debe solicitar el consentimiento libre, previo, expreso, informado de los herederos del titular. En el caso de los datos sensibles se necesita además, que sea por escrito.

2.- No se requerirá el consentimiento para su publicación si los datos están dentro de los enumerados en el artículo 90 literal C) de la Ley N O 18.331 0 si están disociados.

3.- No es de aplicación al certificado de defunción y al certificado de defunción resumido el artículo 9 0 bis de la Ley N O 18.331, por no estar comprendido dentro de sus enunciados. Solo la Dirección General del Registro de Estado Civil es la que puede proporcionar estos certificados como fuente pública.

4.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
11/015	2008-28-1-0010024

Montevideo, 05 de junio de 2015

VISTO: La consulta presentada por la Unidad Nacional de Seguridad Vial (UNASEV) sobre la procedencia de permitir a la Compañía Uruguaya de Transportes Colectivos Sociedad Anónima (CUTCSA), acceso a los registros sobre personas "a quienes se les ha retirado la libreta de conducir a consecuencia de espirometrías positivas (o análisis análogos)".

CONSIDERANDO:

I) Que la puesta a disposición de datos consultada se enmarca en la definición legal de comunicación de datos personales dada por la Ley N O 18.331, de 11 de agosto de 2008.

II) Que la referida comunicación requiere el consentimiento informado de sus titulares, por no resultar aplicables en la especie ninguna de las excepciones previstas en el artículo 17 de la Ley N O 18.331, ni advertirse el interés legítimo requerido por la norma.

III) Que, asimismo, una cesión de esta índole no se estima acorde con el principio de veracidad al ser desproporcionada en relación con la finalidad perseguida por CUTCSA de "optimizar los controles relativos al personal que diariamente desempeña funciones de conductor en las unidades de nuestra Empresa".

ATENTO: A lo expuesto e informado, y lo previsto por los arts. 31 y 34 de la Ley N O 18.331,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- La comunicación de datos consultada requiere previo consentimiento informado de sus titulares, por no resultar aplicables ninguna de las excepciones previstas en el artículo 17 de la Ley N O 18.331, ni advertirse el interés legítimo requerido por la norma.

2.- Notifíquese, publíquese

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
12/015	2015-2-10-0000066

Montevideo, 07 de julio de 2015

VISTO: La solicitud formulada con fecha 2 de julio de 2015, por el Centro Ceibal para el Apoyo a la Educación de la Niñez y la Adolescencia (Centro Ceibal), a los efectos que la Unidad Reguladora y de Control de Datos Personales "se expida en los temas de su competencia acerca de la utilización de las herramientas "Google Apps For Education" por parte de docentes y estudiantes, mediante usuarios registrados los dominios docente.ceibal.edu.uy y estudiante.ceibal.edu.uy", que son administrados por el Centro".

RESULTANDO:

I) Que el dominio para docentes ya se encuentra disponible, y se planea poner a disposición el de estudiantes para enseñanza media a la brevedad.

II) Que el Centro Ceibal adjunta la documentación en la cual se detallan los acuerdos de servicio a los que ha adherido con Google Inc. (Google) - "Google Apps for Education (online) Agreement" y "Data Processing Amendment to Google Apps Agreement" (el Acuerdo) -.

III) Que se ha realizado un pormenorizado análisis de compatibilidad entre el Acuerdo y las disposiciones normativas vigentes en materia de protección de datos personales.

CONSIDERANDO:

I) Que el Acuerdo no condiciona temporalmente a las partes, que serán las que fijen el plazo inicial de prestación de los servicios, renovable automáticamente por períodos adicionales de doce meses, pudiendo ser terminado en cualquier momento, mediando un pre aviso de 15 días al plazo inicial o cualquiera de sus prórrogas, a la otra parte.

II) Que expresamente se señala que el alcance del tratamiento para la provisión de los Servicios (detección, prevención y resolución de incidentes técnicos y de seguridad), así como la respuesta a los requerimientos en general, es fijado por el Centro Ceibal y Google debe cumplir con las instrucciones; solamente tratará los datos en el marco del Acuerdo, no pudiendo utilizar los datos de los usuarios de este servicio con fines publicitarios de tipo alguno.

III) Que el Centro Ceibal se compromete a la obtención del consentimiento parental — padres, tutores o curadores - en relación con la recopilación de información personal de los estudiantes para la provisión y el uso de los Servicios objeto del Acuerdo.

IV) Que el Centro Ceibal es el responsable de obtener y conservar los consentimientos de los usuarios finales a los efectos de permitir que Google proporcione los Servicios. El Centro Ceibal en su carácter de administrador de las cuentas puede acceder, supervisar y comunicar estos datos, sin perjuicio que le es de aplicación la excepción prevista en los artículos 17 y 90 literal B), de la Ley N O 18.331, de 11 de agosto de 2008.

V) Que Google se compromete a que todas las instalaciones utilizadas para almacenar y procesar los datos del Centro Ceibal, cumplirán con los estándares razonables de seguridad para el sector y en ningún caso podrán ser inferiores a los mantenidos para las instalaciones de almacenamiento y procesamiento de la información que le es propia, estableciendo medidas técnicas, administrativas y organizacionales para proteger los datos de incidentes de seguridad.

VI) Que finalizado el acuerdo, Google borrará de sus sistemas la información en un máximo de ciento ochenta días. Durante la vigencia del Acuerdo, la información borrada por el Centro Ceibal o cualquiera de sus usuarios finales, será eliminada en igual plazo.

VII) Que las partes se comprometen a proteger la información proporcionada o conocida en el marco del Acuerdo y a adoptar las medidas necesarias para ello, responsabilizándose por terceros a su cargo que la infrinjan. Google se compromete a proteger y mantener la confidencialidad de los datos personales conocidos mediante el Acuerdo. Esta obligación subsiste aún en caso de terminación del contrato.

VIII) Que el Centro Ceibal y los usuarios finales tienen la posibilidad de corregir, bloquear, exportar y borrar definitivamente su información.

IX) Que en materia de comunicación de datos, la regla está fijada por el principio de reserva indicado en el **CONSIDERANDO** VII.

X) Que en relación con la transferencia internacional de datos, se acuerda que Google puede transferir, alojar o procesar los datos en territorio de los Estados Unidos de Norteamérica, o en cualquier otro país en que éste o sus subencargados de tratamiento definan, con el compromiso de Google de mantener su certificación al Programa de Puerto Seguro (Safe Harbor) del Departamento de Comercio de los Estados Unidos o adoptar una alternativa que cumpla con las exigencias de la Directiva 95/46/CE para la transferencia internacional de datos. XI) Que la normativa aplicable al Acuerdo Centro Ceibal — Google es acorde a la normativa nacional vigente, en mérito a que es de aplicación la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva) y la Ley Federal de Suiza, de 19 de junio de 1992.

ATENTO: A lo precedentemente expuesto y a las Leyes Nos. 18.331, de 11 de agosto de 2008 y 19.030, de 12 de diciembre de 2012, Decreto N O 414/009, de 31 de agosto de 2009, normas modificativas, concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- El Acuerdo entre Centro Ceibal y Google - "Google Apps for Education (online) Agreement" y "Data Processing Amendment to Google Apps Agreement" - se adecua a las disposiciones normativas vigentes en materia de protección de datos personales.

2.- Hacer saber al Centro Ceibal la conveniencia de adoptar las siguientes recomendaciones:

A. informar claramente a los docentes, estudiantes, padres, tutores o curadores sobre el contenido y alcance del Acuerdo y los Servicios a prestarse;

B. publicar los documentos denominados "Google Apps for Education (online) Agreement" y "Data Processing Amendment to Google Apps Agreement", traducidos al idioma español por traductor público;

C. publicar en forma separada y en lenguaje sencillo la información relativa al consentimiento, finalidad, tiempo de conservación, reserva, seguridad y destino de los datos tratados, así como los derechos que tienen los titulares a su respecto y la forma de ejercerlos, estableciendo un procedimiento claro;

D. recabar el consentimiento de los padres, tutores o curadores de los estudiantes menores de edad destinatarios de los servicios, mediante la elección de dos opciones claramente identificadas que no se encuentren premarcadas en favor o en contra, sin perjuicio de la excepción señalada en el CONSIDERANDO IV);

E. inscribir las bases de datos de su titularidad ante el Registro de Bases de Datos que lleva esta Unidad.

3.- Comuníquese, publíquese, etc.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
18/015	2015-2-10-0000405

Montevideo, 02 de diciembre de 2015

VISTO: La consulta presentada por la ADMINISTRACIÓN NACIONAL DE CORREOS (en adelante ANC) con referencia a las cuestiones atinentes a la protección de datos personales en el marco de la contratación e implementación por el propio organismo de un sistema informático de evaluación de personal.

RESULTANDO:

I) Que la ANC tiene ingresada ante el registro de bases de datos que lleva esta Unidad, la denominada "RRHH"

II) Que la empresa proveedora del servicio referido en el **VISTO**, realizará por cuenta de la ANC, titular de la base de datos, el tratamiento de la misma, y almacenará los datos en un servidor ubicado en los Estados Unidos de América, el cual cuenta con la certificación "Safe Harbor".

CONSIDERANDO:

I) Que el art. 4 Lit. H) de la Ley N O 18.331 dispone que encargado del tratamiento es aquella persona física o jurídica, pública privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

II) Que el art. 23 de la propia norma regula la transferencia internacional de datos personales, indicando que la misma se encuentra prohibida cuando los destinatarios de los datos sean países u organismos internacionales que no proporcionen niveles de protección adecuados, de acuerdo con los estándares del Derecho Internacional o regional en la materia, salvo las excepciones en ella numeradas.

III) Que el propio artículo 23 en su Lit. B) consagra como una de las excepciones previstas, que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado. Por su parte, su Lit. C) refiere a que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero.

IV) Que el art. 4 Lit. H) del Decreto Nº 414/009 define a la transferencia internacional de datos como aquel tratamiento de datos que supone una transmisión de éstos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.

V) Que el art. 17 de la Ley Nº 18.331 regula la comunicación de datos, indicando que esta debe respetar el interés legítimo del emisor y del destinatario de los datos, además de requerir el consentimiento previo e informado del titular, sin perjuicio de las excepciones allí previstas y las dispuestas en el art. 9.

VI) Que el art. 9 Lit. D) prevé que no será necesario el consentimiento previo del titular cuando los datos deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

VII) Que por Resolución Nº 17/009 de fecha de 12 de junio de 2009, el Consejo Ejecutivo de la URCDP, entendió como países adecuados a los efectos de las transferencias internacionales de datos, a los países de la Unión Europea y aquellos que la Comisión Europea considere garantizan las condiciones antes indicadas.

VIII) Que los arts.34 y 35 del Decreto Nº 414/009 regulan el procedimiento para solicitar ante esta Unidad la autorización para realizar transferencias internacionales a aquellos destinos que no se consideren adecuados, en función de lo dispuesto por el art 23 de la Ley Nº 18.331.

ATENTO: A lo expuesto, y a lo previsto en la Ley N O 18.331, su decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que la ADMINISTRACIÓN NACIONAL DE CORREOS deberá informar en el marco del registro de su base de datos denominada "RRHH" que aloja datos de evaluación de sus funcionarios, así como la existencia de un encargado de tratamiento y de transferencias internacionales de datos con destino a Estados Unidos de América.

2.- Que deberá solicitar a esta Unidad la autorización para la referida transferencia internacional en función de lo dispuesto por el art 23 de la Ley N O 18.331 y en la forma prevista en los arts.34 y 35 del Decreto N O 414/009.

3.- Que de resultar autorizada la transferencia antes referida, la misma no requerirá consentimiento previo del titular de los datos, con motivo de ser necesaria para la ejecución o desarrollo de un contrato, en función de lo dispuesto por los arts. 23, 17 Lit. B) y art. 9 Lit. D) de la Ley Nº 18.331.

4.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
04/016	2016-2-10-0000105

Montevideo, 02 de marzo de 2016

VISTO: La consulta realizada por la División Epidemiología del Ministerio de Salud Pública (MSP) con referencia a la implementación de un software de registro único de usuarios que padecen VIH, el cual vincula la información clínica, epidemiológica y de laboratorio, con la finalidad de dar tratamiento a la enfermedad y aumentar su vigilancia.

RESULTANDO:

I) Que las características de la epidemia de infección por VIH/SIDA se han modificado con el transcurso del tiempo, pasando a ser un evento transmisible, pero de comportamiento crónico.

II) Que la generalización del tratamiento antirretroviral, el inicio del tratamiento en la etapa no sida de la infección, el mayor acceso a programas de prevención de la transmisión materno infantil y a servicios de consejería y pruebas voluntarias, han permitido incrementar el número de personas que realizan la prueba del VIH, y obtener diagnósticos más tempranos en la historia natural de la infección, por lo que la vigilancia de la enfermedad se ha transformado en un gran desafío para los países.

III) Que el software relacionado en el VISTO permite el acceso a la información de los pacientes al MSP, a los laboratorios de análisis clínicos, y a los médicos tratantes.

CONSIDERANDO:

I) Que el artículo 44 de la Constitución de la República dispone que el Estado legislará en todas las cuestiones relacionadas con la salud e higiene públicas, procurando el perfeccionamiento físico, moral y social de todos los habitantes del país, disponiendo también, que todos los habitantes tienen el deber de cuidar su salud, así como el de asistirse en caso de enfermedad.

II) Que el art. 22 de la Ley N O 18.335, de fecha 15 de agosto de 2008 dispone que las personas tienen la obligación de someterse a las medidas preventivas o terapéuticas que se le impongan, cuando su estado de salud, a juicio del MSP, pueda constituir un peligro público, tal como lo dispone el artículo 224 del Código Penal.

III) Que el art. 1 0 de la Ley Orgánica de Salud Pública, Ley N O 9202 de fecha 12 de enero de 1934, dispone que compete al Poder Ejecutivo por intermedio del MSP, la organización y dirección de los servicios de Asistencia e Higiene.

IV) Que el art. 2 0 de la Ley N O 18.211 de 13 de diciembre de 2007 que regula la creación, funcionamiento y financiación del Sistema Nacional Integrado de Salud (SNIS) establece como competencia del MSP la implementación de dicho sistema y la articulación de los prestadores públicos y privados.

V) Que el art. 4 0 Lit. B de la referida norma, consagra como objetivos del SNIS la implementación de un modelo de atención integral basado en una estrategia sanitaria común, políticas de salud articuladas, programas integrales y acciones de promoción, protección, diagnostico precoz, tratamiento oportuno, recuperación y rehabilitación de la salud de sus usuarios, incluyendo los cuidados paliativos.

VI) Que el art. 4 0 Lit. E), de la Ley N O 18.331, de 11 de agosto de 2008, define a los datos sensibles como aquellos datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

VII) Que el art. 18 de esta Ley prevé que ninguna persona puede ser obligada a proporcionar datos sensibles, los cuales solo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Asimismo, indica que los mismos, pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo.

VIII) Que el artículo 17 de dicha Ley N O 18.331 regula la comunicación de datos personales exigiendo que la misma deba contar con el interés legítimo del emisor y del destinatario de los datos, sin perjuicio del previo consentimiento del titular de los mismos.

IX) Que el Lit. C) del propio artículo 17 prevé que no será necesario el consentimiento del titular cuando se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente.

X) Que por su parte, el art. 19 de la Ley Nº 18.331 indica que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la propia Ley N O 18.331.

XI) Que la Ley Nº 19.286, de fecha 25 de setiembre de 2014 (Código de Ética Médica), dispone en su artículo 22 que el respeto a la confidencialidad es un deber inherente a la profesión médica el cual podrá ser relevado en los casos establecidos por una ley de interés general o cuando exista justa causa de revelación.

ATENTO: A lo expuesto, y a lo previsto en la Ley Nº 18.331, su Decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que el proyecto objeto de esta consulta prevé el tratamiento de datos de salud, los cuales son datos sensibles en virtud de lo dispuesto por el art. 4 0 de la Ley 18.331, por lo cual se exhorta al MSP a adoptar todas las medidas de seguridad adecuadas para garantizar la seguridad de la información personal de los usuarios en el sistema.

2.- Que se entiende que la decisión del MSP de solicitar que la información cargada en el sistema sea comunicada sin disociarla de su titular resulta acorde a derecho, ya que la pertinencia exigida por el art. 17 Lit. C de la Ley N O 18.331, debe ponderarse a la luz de las normas jurídicas que regulan el punto objeto de este proyecto y así como el interés general a las que ellas responden, como son los Art. 44 de la Constitución, 22 de la Ley N O 18.335, y el Decreto N O 409/993, en la redacción dada por el Decreto Nº 255/008, así como las disposiciones internacionales aplicables.

3.- Que la titularidad del sistema y de la base de datos generada por parte del MSP también se entiende acorde a derecho, en función de su calidad de órgano integrante del sistema orgánico Poder Ejecutivo, en ejercicio de los cometidos referentes a la sanidad nacional en cumplimiento de lo dispuesto en el art. 1º de la Ley Orgánica de la Salud NO 9202.

4.- Que el acceso a la información alojada en el sistema sin restricciones por parte del MSP se entiende legitima, con motivo de ajustarse a lo dispuesto por el inc. 2 del art. 18 de la Ley Nº 18.331, en virtud de mediar razones de interés general por aplicación de lo dispuesto en los arts. 10, 20, 40 Lit. B), 1 1 y 49 de la Ley Nº 18.211 que regula el SNIS.

5.- Que la comunicación de datos realizada por los laboratorios de análisis clínicos con la carga de la información del paciente en el sistema también es legítima por encontrarse precedida de interés legítimo del laboratorio como emisor de los mismos, en virtud de la necesidad de dar cumplimiento a la normativa vigente, como son los arts. 40 Lit. B) y 1 1 de la Ley Nº 18.211; y por el MSP como destinatario de los mismos, en función de lo dispuesto en el art. 4 0 de la Ley Orgánica de la Salud N O 9202 y el art. 2 0 de la Ley N O 18.21 1, y no será necesario el consentimiento previo del titular, por aplicación del art. 17 Lit. C).

6.- Que la solicitud de acceso a la información del paciente que solicitan los propios laboratorios de análisis clínicos, se entiende acorde a lo previsto por el art. 19 de la Ley Nº 18.331, con motivo de que aquel ya ha sido usuario de la entidad, por lo que éstas ya poseen tal información, accediendo en este caso por otra vía. Igualmente corresponde exhortar al MSP extremar las medidas de seguridad y los accesos para que los laboratorios de análisis clínicos no accedan a información que exceda el marco de su actuación.

7.- Que la comunicación de datos realizada por parte de los médicos tratantes del paciente con destino al MSP, también es legítima ya que se encuentra revestida de interés legítimo para ambos: para los médicos, por aplicación de la Ley Nº 19.286 (Código de Ética Médica), y para el MSP por mandato del art. 44 de la Constitución, art. 1º de La ley Orgánica de la Salud Nº 9202 y el art. 2º de la Ley Nº 18.211 y tampoco será necesario el consentimiento del titular por aplicación de la excepción prevista en el art. 17 Lit. C).

8.- Que la comunicación de la información médica del paciente por parte del médico tratante con destino al MSP y a otros médicos tratantes que pudieren acceder al sistema en otras instancias del tratamiento, también se realiza acorde a derecho ya que reviste el interés general exigido y no requiere consentimiento previo del titular por aplicación del art. 17 Lit. C) de la Ley Nº 18.331, sin perjuicio de la aplicación del art. 22 de la Ley Nº 19.286 (Código de Ética Médica).

9.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
09/016	2016-2-10-0000067

Montevideo, 13 de abril de 2016

VISTO: La consulta formulada por MSC MEDITERRANEAN SHIPPING COMPANY S.A. y MEDITERRANEAN SHIPPING COMPANY URUGUAY S.A. referida a transferencia de datos personales.

RESULTANDO:

Que las empresas han proyectado la migración del servicio de correo empresarial a nivel global utilizando servidores con servicio exclusivo para ellas, establecidos en los Países Bajos (el primario) y en Irlanda (el secundario), en Virginia, Estados Unidos (el primario) y en Texas, Estados Unidos (el secundario), Singapur (el primario) y (Hong-Kong).

CONSIDERANDO:

I) Que no sería necesario tramitar la autorización para efectuar la transferencia internacional de datos proyectada si se cumple con la migración a los "países adecuados" (Países Bajos e Irlanda).

II) Que se debe tener presente que cuando sea a países no adecuados se necesita la autorización de la Unidad, o tener inscripto un código de conductas para la transferencia entre las empresas y sus filiales.

ATENTO: A lo expuesto, y a lo previsto en los artículos 23 de la Ley Nº 18.331, 34 y 35 del Decreto 414/009 y el Dictamen N O 8/014, de 23 de julio de 2014 de esta Unidad.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que corresponde se inscriba ante esta Unidad un código de conducta de datos personales para la utilización entre las consultantes (por MSC MEDITERRANEAN SHIPPING COMPANY S.A. y MEDITERRANEAN SHIPPING COMPANY URUGUAY S.A.) y sus filiales y efectuar las transferencias internacionales.

2.- Que en lo relativo a estas transferencias para el caso de que se cambiara de servidor a alguno de los ubicados en "países no adecuados", será necesario solicitar autorización a esta Unidad.

3.- Notifíquese, publíquese y posteriormente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

NOTA *de* INTERÉS

MARÍA VERÓNICA
PÉREZ ASINARI

MARÍA VERÓNICA
PÉREZ ASINARI

Jefa de Unidad, Supervisión y Aplicación de la ley, oficina del Supervisor Europeo de Protección de Datos.

IMPACTO EN URUGUAY DEL NUEVO REGLAMENTO DE LA UNIÓN EUROPEA SOBRE PROTECCIÓN DE DATOS PERSONALES

El 4 de mayo de este año se publicó en el Diario Oficial de la Unión Europea el Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Este texto será aplicable a partir del 25 de mayo de 2018. También se adoptó la Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

La protección de las personas físicas en relación al tratamiento de datos personales es un derecho fundamental en la Unión Europea (UE). Es claro que los cambios tecnológicos y la globalización traen aparejados nuevos desafíos para este derecho y otros que se encuentran conectados, como el derecho a la intimidad, sobre todo si se considera el impacto en la vida cotidiana de las personas del uso de Internet y el tratamiento de nuestros datos personales tanto por el Estado como por las empresas.

Se trata de una reforma emblemática que trae aparejada cambios sustanciales, como por ejemplo: refuerza los derechos de los individuos, facilita del ejercicio de los mismos, refuerza la responsabilidad de los organismos públicos y empresas de documentar internamente las medidas adoptadas para cumplir con la legislación, refuerza el poder de las autoridades independientes de protección de datos, incluyendo multas que pueden ir hasta el 4% de la facturación global de una empresa.

Dentro de las reformas que presenta el nuevo Reglamento hay dos aspectos que tienen un impacto directo en Uruguay: (a) el relativo a la adecuación para la transferencia internacional de datos personales, y (b) la nueva delimitación del ámbito de aplicación territorial (y la implicancia extraterritorial del mismo).

1. LA ADECUACIÓN Y LOS FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES

La legislación europea en materia de protección de datos establece que la información relativa a los individuos (datos personales) sólo puede ser transferida a un país no miembro de la UE cuando ese país asegure un nivel de protección adecuado. Se considera que un país otorga un nivel de protección adecuado cuando su sistema legal y el modo en que éste es aplicado en la práctica garantiza determinados derechos y obligaciones que son considerados esenciales en la UE (entre ellos: principio de limitación de finalidad, proporcionalidad, calidad de los datos, transparencia, seguridad, derechos de acceso, rectificación y oposición, restricciones respecto de transferencias sucesivas a otros terceros países, mecanismos adecuados de procedimiento y control –autoridad independiente de protección de datos, nivel satisfactorio de cumplimiento, apoyo y asistencia a los interesados, vías adecuadas de recurso-). Si el país de destino

de los datos no es adecuado habrá que evaluar si alguna excepción es aplicable (ej.: consentimiento del titular, necesidad para un contrato, interés vital, razones importantes de interés público). En caso de que las excepciones no procedan la transferencia solo podrá tener lugar si la organización presenta garantías suficientes sobre el nivel de protección que ofrece el destinatario de los datos (ej.: firma de cláusulas contractuales).

La Comisión Europea puede adoptar una decisión que declare que un país no miembro de la UE garantiza un nivel adecuado de protección. Cuando ello sucede se establece el libre flujo de datos personales entre la UE y ese país no miembro (o un sector de un tercer país). Ello incluye un análisis pormenorizado de la letra de la ley y de la realidad en su aplicación. Hasta la fecha muy pocos países han obtenido tal decisión por parte de la Comisión Europea. Uruguay se encuentra entre ese pequeño grupo de países que han sido declarados "adecuados".[1] Los otros son los siguientes: Suiza, Argentina, Israel, Nueva Zelanda, Andorra, Guernsey, Jersey, Isla de Man, Islas Feroe, un sector de Canadá (sector privado). Estados Unidos contaba con un sistema, conocido como Safe Harbor, que cubría solo a las empresas que auto-certificaban el cumplimiento de determinados principios. No obstante, un fallo de la Corte de Justicia de la UE de 2015 anuló la decisión de la Comisión que declaraba el Safe Harbor "adecuado"[2].

La decisión de adecuación no significa un "cheque en blanco", sino que la Comisión siempre estuvo facultada para revisar el sistema del país no miembro, su aplicación y la incidencia en la decisión de adecuación. No obstante, hasta el momento, no se han realizado revisiones formales respecto de los países declarados adecuados. Con la adopción del nuevo Reglamento se produce un cambio importante,[3] ya que la Comisión Europea deberá realizar revisiones periódicas, al menos cada cuatro años, que tengan en cuenta los desarrollos acaecidos en los países declarados adecuados. Si la revisión revelara que alguno de esos países no siguen asegurando un nivel adecuado de protección, la Comisión deberá decidir en ese sentido, y, hasta donde fuese necesario, repeler, enmendar o suspender la decisión de adecuación. La Comisión deberá consultar al país de que se trate con el objeto de remediar una situación tal. Es por ello que los países que quieran conservar la adecuación deberán asegurarse que el nivel de protección continúe siendo satisfactorio y que se adecue a los desarrollos "esenciales" de la materia en la UE. De ese modo se deberá considerar el impacto de la adopción de la Carta de Derechos Fundamentales y del nuevo Reglamento, así como la jurisprudencia europea, como el caso Schrems, en el cual la Corte de Justicia de la Unión Europea refuerza el concepto de adecuación al requerir que el nivel de protección sea "esencialmente adecuado".

2. ÁMBITO DE APLICACIÓN TERRITORIAL

El nuevo Reglamento se aplicará a las organizaciones y empresas que se encuentren establecidas en el territorio de la UE y a aquellas que no se encuentren establecidas en el territorio de la UE cuando las actividades de tratamiento estén relacionadas con:

- la oferta de bienes o servicios a individuos en la UE, independientemente de si a estos se les requiere su pago, o
- el control de su comportamiento, en la medida en que este tenga lugar en la Unión.[4]

Es por ello que una empresa uruguaya (ej.: una app, un sitio web) que ofrezca bienes o servicios a individuos en la UE, o controle su comportamiento, deberá cumplir con el nuevo Reglamento de protección de datos (no sólo cumplir con las obligaciones y respetar los derechos de los individuos, sino también designar un representante en la UE, salvo que la actividad de tratamiento de datos personales sea ocasional).

1 *En Uruguay, la materia es regulada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data.*

2 *La Corte consideró que tal decisión no garantizaba la protección de los derechos fundamentales a la intimidad y a la protección de datos personales (se trata del caso Schrems –C-362/14- basado en las transferencias realizadas por Facebook desde la UE a EEUU, considerando el impacto de las revelaciones de Snowden en la protección de los derechos fundamentales).*

3 *Artículo 41 del Reglamento.*

4 *Artículo 3.2 del Reglamento.*

ENTREVISTA

JACOB KOHNSTAMM

Fue designado Presidente de la Autoridad Holandesa de Protección de Datos (Dutch DPA) en 2004. Entre 2010 y 2014 también fue Presidente del Grupo de Trabajo en Protección de Datos del Articulo 29 (WP29). Este cuerpo consultivo independiente se compone de representantes de varios supervisores de protección de datos en la Unión Europea. Además, fue Presidente del Comité Ejecutivo de la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad entre 2011 y 2014.

1. HOW LONG WERE YOU CHAIRMAN OF THE DUTCH DATA PROTECTION AUTHORITY?

I was appointed as Chairman of the Dutch Data Protection Authority (Dutch DPA) in 2004. On the 1st of August 2016 I will resign, so in total I have been 12 years Chairman of the Dutch DPA. Between 2010 and 2014 I also served as Chairman of the Article 29 Data Protection Working Party (WP29). This independent advisory body is composed of representatives of the various data protection supervisors in the European Union. Furthermore, I served as Chairman of the Executive Committee of the International Data Protection and Privacy Commissioners Conference between 2011 and 2014.

2. WHAT HAVE BEEN THE MOST INTERESTING CHALLENGES DURING YOUR TENURE? WHAT HAVE BEEN THE DIFFICULTIES YOU HAD TO FACE?

To keep up with technological developments is a true challenge. Take for example our own lives that have changed dramatically over the last 5 years with smartphones, the internet and the development of the Internet of Things. The consequence of this change is that people cannot escape from leaving behind vast quantities of digital personal data traces on a daily basis. Money as a means of exchange is slowly being replaced by personal data, which is less visible and their re-use stays outside everyone's view or control. I hope with the new GDPR our personal data in Europe will be better protected with data protection impact assessments, data protection officers and class actions. Furthermore I think the budget for all European DPAs has to increase dramatically to keep up with all the work. This will be an interesting challenge in the near future!

1. ¿POR CUÁNTO TIEMPO FUE UD. PRESIDENTE DE LA AUTORIDAD DE PROTECCIÓN DE DATOS HOLANDESA?

Fui designado como Presidente de la Autoridad de Protección de Datos holandesa (APD holandesa) en 2004. Renunciaré el 1º de agosto de 2016, por lo que en total he sido Presidente de la APD holandesa por 12 años. Entre 2010 y 2014 también he sido Presidente del Grupo de Trabajo en Protección de Datos del Artículo 29 (WP29). Este cuerpo consultivo independiente se compone de representantes de varios supervisores de protección de datos de la Unión Europea. Además, he sido Presidente del Comité Ejecutivo de la Conferencia Internacional de Protección de Datos y Comisionados de Privacidad entre 2011 y 2014.

2. ¿CUÁLES HAN SIDO LOS DESAFÍOS MÁS INTERESANTES DURANTE SU PERÍODO? ¿QUÉ DIFICULTADES HA TENIDO QUE ENFRENTAR?

Mantenerse al día con los desarrollos tecnológicos es un verdadero desafío. Tomen por ejemplo cómo nuestras vidas han cambiado dramáticamente en los últimos 5 años con los celulares inteligentes, internet y el desarrollo del Internet de las Cosas. La consecuencia de este cambio es que las personas no pueden escapar a dejar tras de sí enormes cantidades de rastros digitales de datos personales en forma diaria. El dinero como medio de cambio está siendo lentamente reemplazado por datos personales, que son menos visibles y su re-utilización se mantiene fuera de la vista o control de todos. Espero que con el nuevo Reglamento General en Protección de Datos, nuestros datos personales en Europa se mantengan mucho mejor protegidos con evaluaciones de impacto en protección de datos, oficiales en protección de datos y el establecimiento de litigios. Además, pienso que el presupuesto para todas las autoridades en protección de datos de Europa debe ser incrementado dramáticamente para continuar con todas las tareas. ¡Este será un interesante desafío en el futuro cercano!.

3. WHAT DO YOU CONSIDER IS THE INFLUENCE OF THE DUTCH DATA PROTECTION AUTHORITY HAS HAD ON THE DEVELOPMENT OF DATA PROTECTION IN EUROPE AND LATIN AMERICA?

I hope we can inspire Latin American countries to cooperate in order to obtain better data protection for their citizens, like we do within the Article 29 Working Party on a European level. Furthermore I have tried to create (transatlantic) bridges with the Building Bridges project. During the International Privacy Conference in Amsterdam in October 2015 we published the Privacy Bridges report, in which we presented ten privacy bridges that will both foster stronger transatlantic collaboration and advance privacy protection for individuals. In this context I think it is not only about transatlantic bridges to the United States of America, but to countries worldwide.

4. WHAT IS THE PERCEPTION THAT DUTCH CITIZENS HAVE REGARDING THEIR RIGHT TO DATA PROTECTION?

I think they become more aware of their rights every day. We also try to promote this by pro-65viding citizens with useful information on our website. We have telephone hours for citizens who have questions regarding the Dutch Data Protection Act. People can call us on their right to redress for example. Via our website they can file a complaint when they suspect a breach of the Dutch Data Protection Act.

5. WHAT ARE THE MOST IMPORTANT ASPECTS IN RELATION TO THE BIRTH AND EVOLUTION OF THE "RIGHT TO BE FORGOTTEN" IN THE EUROPEAN UNION? DO YOU THINK THAT THERE IS ANY EVENT THAT THERE SHOULD BE AN EXCEPTION TO THE "RIGHT TO BE FORGOTTEN"?

The "right to be forgotten" is a concept discussed and put into practice in the European Union. Because of the European Court of Justice ruling against Google in Costeja in May 2014, the debate is very much alive. On its first day of compliance (30 May 2014) Google received 12,000 requests to have personal details removed from its search engine. Of course there are concerns about the impact on the right to freedom of expression and whether creating a right to be forgotten would decrease the quality of the Internet through censorship and a rewriting of history. I think it is very important to always have a balanced approach, but not lose sight of the importance of privacy.

3. ¿CUÁL CONSIDERA HA SIDO LA INFLUENCIA DE LA AUTORIDAD DE PROTECCIÓN DE DATOS HOLANDESA EN EL DESARROLLO DE LA PROTECCIÓN DE DATOS EN EUROPA Y AMÉRICA LATINA?

Espero que podamos inspirar a los países de América Latina a cooperar para obtener una mejor protección de datos para sus ciudadanos, como hemos hecho en el seno del Grupo de Trabajo del Artículo 29 a nivel europeo. Además, he tratado de crear puentes (transatlánticos) con el Proyecto Construyendo Puentes. Durante la Conferencia Internacional de Privacidad de Amsterdam en octubre 2015 publicamos el Reporte Construyendo Puentes, en el que presentamos diez puentes de privacidad que fomentarán tanto una colaboración transatlántica más fuerte y cómo el avance de la protección de la privacidad para los individuos. En este contexto pienso que no sólo se trata de puentes transatlánticos a los Estados Unidos de América sino a países de todo el mundo.

4. ¿CUÁL ES LA PERCEPCIÓN QUE LOS CIUDADANOS HOLANDESES TIENEN RESPECTO A SU DERECHO A LA PROTECCIÓN DE DATOS?

Pienso que cada día se están haciendo más conscientes de sus derechos. Tratamos de promover esto mediante la provisión a los ciudadanos de información útil en nuestro sitio web. Tenemos horarios telefónicos para ciudadanos que tienen preguntas respecto del Acta de Protección de Datos holandesa. Las personas pueden llamarnos por ejemplo respecto a su derecho de reparación. A través de nuestro sitio web pueden realizar una queja cuando sospechan de una violación al Acta de Protección de Datos holandesa.

5. ¿CUÁLES SON LOS ASPECTOS MÁS IMPORTANTES EN RELACIÓN CON EL SURGIMIENTO Y EVOLUCIÓN DEL "DERECHO AL OLVIDO" EN LA UNIÓN EUROPEA? ¿PIENSA UD. QUE EXISTE ALGÚN CASO EN EL QUE DEBERÍA DE EXISTIR UNA EXCEPCIÓN AL "DERECHO AL OLVIDO"?

El "derecho al olvido" es un concepto discutido y puesto en práctica en la Unión Europea. Debido a la sentencia de la Corte Europea de Justicia contra Google en Costeja en mayo de 2014, el debate está muy vigente. En su primer día de cumplimiento (30 de mayo de 2014) Google recibió 12.000 solicitudes de remoción de datos personales de su motor de búsqueda. Por supuesto que existe preocupa-

6. THE DUTCH DATA PROTECTION AUTHORITY WAS INCREASED FLOW OF THEIR WORK AFTER THE JUDGMENT OF THE SUPREME COURT ON THE "RIGHT TO BE FORGOTTEN"?

Yes, since the debate is very much alive our work considering the "right to be forgotten" has indeed increased.

7. HOW IT HAS AFFECTED THE EUROPEAN UNION WITH THE JUDGMENT OF THE SUPREME COURT ON THE ANNULMENT OF THE DECISION OF SAFE HARBOR?

Safe Harbor and its successor are now the talk of the town in privacy minded Europe! The Article 29 Working Party has adopted a statement at its last plenary in April. We note the improvements the Privacy Shield offers compared to the invalidated Safe Harbor decision. But, given the concerns expressed and the clarifications asked, we urge the Commission to resolve these concerns and provide the requested clarifications in order to improve the draft adequacy decision and ensure the protection offered by the Privacy Shield is indeed essentially equivalent to that of the EU.

ción respecto del impacto en el derecho a la libertad de expresión y respecto a si crear un derecho al olvido podría disminuir la calidad de internet a través de la censura y una reescritura de la historia. Pienso que es muy importante tener siempre una aproximación balanceada, pero no perder de vista la importancia de la privacidad.

6. ¿TUVO LA AUTORIDAD DE PROTECCIÓN DE DATOS HOLANDESA UN INCREMENTO EN SU FLUJO DE TRABAJO LUEGO DE LA SENTENCIA DE LA CORTE RESPECTO AL "DERECHO AL OLVIDO"?

Si, desde que el debate ha cobrado más vigencia nuestro trabajo considerando el "derecho al olvido" se ha efectivamente incrementado.

7. ¿CÓMO SE HA VISTO AFECTADA LA UNIÓN EUROPEA CON LA SENTENCIA DE LA CORTE ANULANDO LA DECISIÓN DE "SAFE HARBOR (PUERTO SEGURO)"?

¡Safe Harbor (Puerto Seguro) y su sucesor son el tema del día en la Europa preocupada por la privacidad! El Grupo de Trabajo del Artículo 29 ha adoptado una declaración en su último plenario de abril. Destacamos las mejoras ofrecidas por el "Privacy Shield" (Escudo de Seguridad) en comparación con la decisión invalidada de "Safe Harbor" (Puerto Seguro). Pero, atento a las preocupaciones expresadas y las clarificaciones soliciadas, instamos a la Comisión a resolver estas preocupaciones y proveer las clarificaciones solicitadas a fin de mejorar el borrador de decisión de adecuación y asegurar que la protección ofrecida por el "Privacy Shield" (Escudo de Seguridad) es efectivamente y esencialmente equivalente a la de la Unión Europea.

8. DO YOU KNOW IF THERE HAS BEEN A BEFORE AND AFTER THE ADEQUACY OF URUGUAY TO DIRECTIVE 96/45 / EC AS REGARDS THE ECONOMIC IMPACT BETWEEN THIS COUNTRY AND THE EU?

In terms of economic activity I would not know if there has been a change after the European Commission adequacy decision on Uruguay in 2012. In fact, it would be interesting to investigate whether after 2012 there has been an increase (or decrease) in economic activity.

9. THE DATA PROTECTION AGENCIES HAVE ACHIEVED A BALANCE IN THE RIGHTS OF USERS AGAINST LARGE CORPORATIONS (FB, GOOGLE, UBER, ETC.) AND DATABASES? WHAT IS YOUR OPINION?

I think this is a very good development. Users should be back in the driver's seat and in control over their own personal data. Improving user control is one of the most important tasks for big companies, hopefully in the near future there will be more data protection officers (DPOs) on the work floor to assist with this pivotal task. With the new Regulation DPOs will be mandatory in some cases, so I guess we will see an increase in DPOs the coming years.

10. DO YOU CONSIDER IT IS REALISTIC TO THINK THAT ALL THE PRINCIPLES THAT STRUCTURE THE PROTECTION OF PERSONAL DATA IN THE CONTEXT OF THE FIGHT AGAINST TERRORISM STILL APPLY?

Recent acts of terrorism have spurred European governments to push for new monitoring powers, however I think privacy should always be taken into account by government officials.

8. ¿SABE SI HA EXISTIDO UN ANTES Y UN DESPUÉS DE LA ADECUACIÓN URUGUAYA A LA DIRECTIVA 95/46/ EC EN LO QUE RESPECTA AL IMPACTO ECONÓMICO ENTRE ESTE PAÍS Y LA UNIÓN EUROPEA?

En términos de actividad económica, no sabría decir si han existido cambios luego de la decisión de adecuación de la Comisión Europea respecto de Uruguay en 2012. De hecho, sería interesante investigar si luego de 2012 ha existido un incremento (o disminución) de la actividad económica.

9. ¿LAS AGENCIAS DE PROTECCIÓN DE DATOS HAN ALCANZADO UN BALANCE EN LOS DERECHOS DE LOS USUARIOS RESPECTO DE GRANDES CORPORACIONES (FB, GOOGLE, UBER, ETC.) Y BASES DE DATOS? ¿CUÁL ES SU OPINIÓN?

Pienso que este es un muy buen desarrollo. Los usuarios deberían de estar nuevamente tras del volante y en control de sus propios datos personales. Mejorar el control del usuario es una de las tareas más importantes para grandes compañías, ojalá en el futuro cercano haya más Oficiales de Protección de Datos (OPD) en los lugares de trabajo para ser un apoyo en esta tarea fundamental. Con la nueva regulación los OPD serán obligatorios en algunos casos, por lo que supongo que veremos un incremento en los OPD en los próximos años.

10. ¿CONSIDERA UD. QUE ES REALISTA PENSAR QUE TODOS LOS PRINCIPIOS QUE FORMAN LA ESTRUCTURA DE LA PROTECCIÓN DE DATOS PERSONALES SON APLICABLES EN EL CONTEXTO DE LA LUCHA CONTRA EL TERRORISMO?

Los recientes actos de terrorismo han llevado a los gobiernos europeos a presionar por nuevos poderes de supervisión, no obstante lo cual pienso que la privacidad debería ser siempre tenida en cuenta por los agentes gubernamentales.

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

agesic
Desarrollando el Uruguay Digital

PRESIDENCIA
República Oriental del Uruguay