Desafíos inducidos por la tecnología en el ámbito de la intimidad y la protección de los datos en Europa

Informe del
Grupo de trabajo *ad hoc* sobre intimidad y tecnología
de la ENISA

Julio de 2008

Redactado por:

Mema Roussopoulos, FORTH (Presidenta del GT)
Laurent Beslay, SEPD
Caspar Bowden, Microsoft
Giusella Finocchiaro, Universidad de Bolonia
Marit Hansen, ULD Kiel
Marc Langheinrich, ETH Zurich
Gwendal Le Grand, CNIL
Katerina Tsakona, FORTH

Revisado por:

Marc Langheinrich, ETH Zurich
Mema Roussopoulos, FORTH

Índice

1. Introducción

Hoy en día, la intimidad y la protección de los datos personales plantean desafíos cruciales en el desarrollo de los sistemas y aplicaciones de las tecnologías de la información y las comunicaciones (TIC). Este extremo se reconoce expresamente en el Reglamento (CE) nº 2004/460, por el que se creó la ENISA en marzo de 2004 (considerando 8). El desarrollo de sistemas de comunicaciones móviles e inalámbricas, las aplicaciones que fundamentan su fiabilidad en protocolos de Internet de extremo a extremo y la aparición de la RFID (identificación por radiofrecuencia), entre otras cuestiones, crean nuevos riesgos de tratamiento ilícito de los datos personales. Se explotan las posibles amenazas derivadas de las vulnerabilidades tanto técnicas como humanas (a saber, un correo basura [*spam*] agresivo, el software malintencionado [*malware*] o los sitios web de suplantación de identidad [*phishing*]) para la realización de ataques delictivos organizados. La prevista proliferación de redes de sensores que recojan información sobre la vida cotidiana de las personas someterá a tensión la capacidad para aplicar con efecto significativo los principios de protección de los datos, a menos que se descubran métodos adecuados para garantizar el cumplimiento de la normativa.

El Grupo de trabajo de la ENISA sobre intimidad y tecnología se creó con objeto de analizar los problemas que plantean estas tendencias tecnológicas y sus consecuencias para el marco jurídico vigente de la UE. Su principal tarea es proponer acciones para atender estos desafíos. En este informe, identificamos las principales **lagunas inducidas por la tecnología** entre la normativa sobre protección de datos y la realidad del entorno socioeconómico en continua evolución. Consideramos las potenciales amenazas y las oportunidades que ofrecen las tecnologías de punta y proponemos prioridades para colmar las lagunas más urgentes.

Los principios de la protección de datos están rigurosamente formulados en términos tecnológicamente neutrales, pero es fundamental comprender cómo pueden aplicarse eficazmente a unas innovaciones que sustenten el cumplimiento del objetivo de Lisboa de hacer de la UE «la economía basada en el conocimiento más competitiva y dinámica del mundo». **Para que los ciudadanos sigan confiando en que sus derechos fundamentales están protegidos y en que el marco de la UE es relevante para su experiencia cotidiana, deben tener la posibilidad de ejercer su derecho a la intimidad de modo práctico y útil.** Nos preocupa que estos principios acaben convirtiéndose en una mera abstracción jurídica que facilite tan sólo remedios teóricos para casos excepcionales. Para evitar una situación tan precaria, tal vez sean necesarios un modo de pensar original y una actuación resuelta.

En el resto del informe facilitamos una descripción preliminar de los distintos problemas identificados, damos una lista de sus características específicas y ofrecemos una serie de recomendaciones que consideramos esenciales para colmar las lagunas citadas. Nuestro análisis tiene en cuenta la función de los organismos públicos y privados competentes a escala europea y de los Estados miembros, donde proceda.

2. Resumen de recomendaciones

Esta sección contiene un resumen de las lagunas identificadas y las soluciones recomendadas. Para un examen más pormenorizado, consúltese la descripción de las distintas lagunas en el cuerpo del documento.

Inclusión digital en relación con la protección de la intimidad

Una laguna fundamental es la falta de sensibilización y de comprensión del tema de la intimidad en las relaciones entre las personas, así como la falta de capacidad para obrar adecuadamente. Esta laguna podría dar lugar a una división de la sociedad entre quienes gozan de intimidad y quienes no gozan de ella. Si la sociedad de la información ha de abordar el problema de la inclusión digital en lo que respecta a las tecnologías de la información y las comunicaciones (TIC), es decir, el problema de cómo hacerlas más accesibles a los usuarios, ha de procurarse capacitar a los ciudadanos para proteger y aplicar su intimidad en las TIC. A este respecto exigen una atención especial no sólo los grupos desfavorecidos en materia de TIC, como las personas mayores o con discapacidad, sino también los jóvenes con un bajo umbral de uso de las TIC.

Recomendamos que la Comisión inicie programas de inclusión digital que lleguen a la población a través de ejemplos relevantes para su situación vital, ya sea en la escuela, en la guardería, en la empresa o en cualquier otro lugar. Esto no sólo exige el desarrollo de nuevas herramientas de asistencia al usuario y sistemas de gestión de la identidad, sino también una mejora de los medios de comunicación (por ejemplo, folletos sobre intimidad, programas educativos en las escuelas, etc.).

Herramientas de asistencia al usuario

Las mejores tecnologías y leyes no ayudan al ciudadano si éste es incapaz de hacer uso de ellas de la mejor forma para sus intereses. Por ejemplo, no son muchos los usuarios finales que han adaptado para su uso tecnologías de seguridad tales como las herramientas de cifrado o de «anonimización», pese a su sofisticación tecnológica. Los responsables del tratamiento de datos cuyo modelo de negocio depende de la monetización de flujos de datos personales no tienen actualmente incentivos suficientes para ofrecer interfaces de control de fácil manejo para los interesados.

Recomendamos que las agencias de investigación y la industria destinen recursos al desarrollo de interfaces de usuario más sencillas de utilizar y asistentes de configuración automática («wizards») de los sistemas y del control de los datos personales. Para que los interesados puedan comprender mejor las consecuencias del tratamiento de sus datos, los Estados miembros, las autoridades de protección de datos y las

organizaciones de consumidores deben aumentar sus iniciativas educativas, ajustándolas en lo posible a las necesidades de los grupos de ciudadanos concretos (por ejemplo, jóvenes, padres, etc.).

Acceso en línea a los datos personales

Uno de los aspectos más característicos del marco comunitario de protección de datos es la existencia de un inequívoco derecho de las personas a averiguar qué organizaciones tienen información sobre ellas: el derecho de acceso a los datos personales. Sin embargo, y a pesar de haber aumentado la importancia y la urgencia de las razones que justificaron el establecimiento inicial de este derecho, su aplicación en la práctica no ha seguido el ritmo de evolución de otros aspectos de la sociedad de la información, con lo que se ha impedido su ejercicio de un modo apropiado y eficaz. Lo primero que ha de considerarse para mejorar esa aplicación es garantizar una autenticación satisfactoria de la persona que formula la petición.

Recomendamos a la ENISA y al Grupo de trabajo del artículo 29 que hagan un análisis detallado de cómo podría reencuadrarse este derecho de acceso a los datos personales, con objeto de garantizar el acceso en línea de las personas a la cantidad máxima de sus datos personales, en el caso ideal de manera gratuita y, en la medida de lo posible, en consonancia con el marco jurídico vigente. Las herramientas de asistencia al usuario y los sistemas de gestión de la identidad pueden desempeñar una importante función en este marco.

Gestión de la identidad

Para garantizar la asunción de responsabilidades en el mundo en línea, los sistemas de TIC actuales suelen exigir a los usuarios que faciliten su verdadero nombre y otra información personal, acreditada por certificados digitales. Sin embargo, a menudo no es necesario el nombre del usuario. Las «credenciales privadas» o los «certificados de revelación mínima» contribuyen a la protección de la intimidad mediante la demostración de que se dispone de autorización al mismo tiempo que se controlan las condiciones que determinan la identificabilidad y la responsabilidad del usuario. La disponibilidad de tales tecnologías tiene consecuencias para la interpretación del principio de minimización de los datos y para el significado de proporcionalidad, es decir, para el hecho de que el tratamiento de datos personales no debe ser excesivo, sino que ha de limitarse a lo necesario.

Recomendamos que los legisladores y los responsables de la formulación de políticas a escala nacional y europea reevalúen el fundamento de la legitimidad del tratamiento de los datos personales a la luz de estas técnicas. Además, recomendamos que los interesados de los sectores público y privado contribuyan a la creación de la necesaria infraestructura de expedición e interoperabilidad de tales credenciales y que hagan uso de ellas en sus sistemas TIC cuando proceda.

Divulgación de los incidentes de seguridad

Una protección de la intimidad eficaz sólo será posible si la información sobre seguridad y los riesgos que afectan a la intimidad en el tratamiento de datos, así como los incidentes relativos a la seguridad y la intimidad que afecten a los datos personales, se comunican adecuada y oportunamente.

Recomendamos que la Comisión Europea adopte legislación completa sobre notificación de las infracciones de seguridad. En concreto, esa legislación debe permitir no sólo a las agencias protección de datos sino también a las personas identificar mejor tales incidentes y reaccionar adecuadamente ante ellos, de manera que los ciudadanos puedan comprender mejor cómo pueden afectarles y cómo reaccionar adecuadamente. Además, recomendamos que los organismos de normalización consideren la conveniencia de adoptar formatos y protocolos que favorezcan que los sistemas TIC de los usuarios interpreten tales notificaciones.

Certificación

Los esfuerzos por ofrecer incentivos exclusivamente económicos para fomentar el cumplimiento de la normativa han tenido escaso éxito hasta la fecha. Por ello, se debe trabajar en otros métodos. Por ejemplo, los Estados miembros deben desarrollar herramientas que permitan a las empresas aportar certificaciones o autocertificaciones del cumplimiento de la legislación sobre protección de datos al presentarse a una licitación pública. Los Estados miembros deben fomentar y regular los regímenes de certificación, contando asimismo con la participación de las asociaciones de consumidores: deben ofrecerse incentivos fiscales a las empresas que cumplan la normativa y han de considerar la conveniencia de liberar a las empresas de determinadas obligaciones en materia de información siempre que dispongan de un certificado de protección de la intimidad, tal como se establece en la Ordenanza de certificación en materia de protección de datos suiza, DPCO/VDSZ[1], que entró en vigor el 1 de enero de 2008. Deben asimismo establecerse sanciones (e indemnizaciones) para los casos de infracción de la legislación sobre protección de datos (a saber, sanciones diarias o indemnizaciones punitivas).

Recomendamos que la Comisión Europea fomente el desarrollo de procesos de certificación de la protección de la intimidad y adopte disposiciones fiscales y de otra índole para estimular dicha certificación. También recomendamos que los organismos de normalización contribuyan a normalizar las referencias de certificación de la protección de la intimidad. Las herramientas de supervisión y las buenas técnicas serán elementos importantes de un marco de certificación global.

[1] Véase http://www.admin.ch/ch/e/rs/235_13/.

Herramientas de supervisión

Las autoridades de protección de datos se enfrentan con auténticos desafíos al inspeccionar y auditar los sistemas que tratan datos personales. La industria tampoco dispone de las herramientas adecuadas para la realización de auditorías internas de protección de la intimidad. El estado tecnológico actual y el marco jurídico vigente no facilitan los medios para supervisar e inspeccionar con facilidad el tratamiento de los datos realizado por los responsables. Unas herramientas de supervisión normalizadas que permitieran un acceso automático y, acaso, remoto a las autoridades de protección de datos permitirían ejercer las competencias de inspección de manera adecuada y continua. Además, estas herramientas deben facilitar una trazabilidad incuestionable de los sistemas. De este modo, contribuirían a la mejora de los procesos de inspección y facilitarían el análisis de las vulneraciones de la intimidad; por último, potenciarían la transparencia y la información acerca del tratamiento que se facilite al usuario.

Recomendamos que la Comisión Europea financie herramientas eficientes de supervisión de la protección de la intimidad que permitan una auditoría fiable y contrastada; la aplicación de tales herramientas debe ser competencia de los responsables del tratamiento de datos, para garantizar una supervisión continua de la protección de la intimidad; las autoridades de protección de datos también las emplearían para automatizar sus inspecciones.

Buenas técnicas disponibles

Para hacer posible una auditoría y certificación oportunas y eficaces de los sistemas de recogida y tratamiento de datos, tanto la industria como las autoridades de protección de datos necesitan una serie buenas técnicas disponibles (BTD) sectoriales en materia de protección de la intimidad y seguridad. Podría optarse por el uso de una «lista de comprobación» para evaluar el cumplimiento de las normas de protección de la intimidad, estableciéndose una certificación básica en la que, a su vez, podrían basarse otras herramientas de análisis y supervisión.

Recomendamos que la Comisión proponga un instrumento jurídico que defina la estructura y los procedimientos necesarios para la identificación de tales BTD. Este instrumento debe prever la participación de todos los interesados relevantes, cuyas aportaciones deben ser consideradas orientaciones primarias por las autoridades de supervisión y las organizaciones públicas y privadas que ponen en práctica los sistemas de tratamiento.

Incentivos y sanciones

La falta de motivación adecuada de los responsables del tratamiento de datos para cumplir la legislación sobre protección de datos constituye una laguna de carácter general. Numerosas autoridades de protección de datos sólo pueden

verificar la actuación de una pequeña fracción de los responsables del tratamiento de datos, por lo que los incumplimientos de la normativa pasan, con frecuencia, desapercibidos. Asimismo, habida cuenta de la escasa entidad de buena parte de las sanciones, los incentivos económicos que se ofrecen para cumplir la normativa de protección de la intimidad son, a menudo, mínimos.

Recomendamos que la Comisión Europea y los Estados miembros fomenten un sistema de incentivos vinculado a un régimen de certificación y a un sistema de sanciones económicas eficaz basado en las BTD, así como en las adecuadas herramientas de auditoría y supervisión.

«Ser o no ser» datos personales

Pese a la reciente iniciativa del Grupo de trabajo del artículo 29 para aclarar el concepto de datos personales, con frecuencia se sigue discutiendo éste. Incluso en los casos en que la industria considere que no se están tratando datos personales, debe realizarse un análisis de los riesgos de vulneración de la intimidad y debe concebirse el sistema de modo que se minimicen tales riesgos. En algunos casos, los datos pueden volverse personales si evolucionan los medios que cabe esperar, razonablemente, que se utilicen para identificar a las personas a medida que aparezcan nuevas tecnologías. Por tanto, aunque no esté previsto que determinados datos vayan a convertirse en personales, habrá que aplicar las garantías adecuadas para evitar que ello suceda.

Recomendamos a la ENISA que desarrolle metodologías de evaluación de impacto sobre la intimidad y a la industria que incluya tales evaluaciones de impacto en la definición de su política de protección de la intimidad y de seguridad. También recomendamos a la industria que desarrolle garantías adecuadas para proteger adecuadamente los datos de las personas, sean éstos de carácter personal o no.

Clasificación social

La clasificación social que lleva a cabo, por ejemplo, el marketing conductual puede vulnerar la intimidad de las personas aunque los datos tratados no sean personales. La reglamentación en vigor está desperdigada en diversas leyes y no otorga una protección eficaz de la intimidad en tales casos.

Recomendamos que la Comisión elabore y establezca un marco jurídico global relativo a todos los tratamientos de datos que afecten a las personas, sean tales datos personales o no. En la práctica, ello podría traducirse en la exigencia de un historial de auditoría completo del tratamiento de los datos y de las fuentes de los mismos y en la obligación de una mayor transparencia para las personas afectadas. Por otra parte, recomendamos que los responsables del tratamiento de datos establezcan medidas organizativas y técnicas que garanticen que los interesados puedan ejercer sus derechos.

Intimidad, protección de datos y espacio

La sociedad de la información plantea desafíos para el mantenimiento de los datos personales de los ciudadanos en el ámbito territorial europeo. Al digitalizar el ámbito personal y, asimismo, sus fronteras, el concepto de territorio digital brinda la oportunidad de introducir la noción de territorio, propiedad y espacio en un entorno digital. El objetivo consiste en proporcionar herramientas que permitan a los usuarios gestionar la proximidad y la distancia con respecto al prójimo en este futuro espacio de inteligencia ambiental, tanto en el sentido jurídico como en el social, tal como sucede ahora en el mundo físico.

Recomendamos que el Grupo de trabajo del artículo 29 y la Comisión Europea exploren la posibilidad de aplicar el concepto de territorio a la sociedad de la información y de hacer extensivo al mundo en línea, por ejemplo, el principio de santuario jurídico que se aplica al domicilio.

Futura labor

Algunas de las lagunas identificadas se relacionan con riesgos de vulneración de la intimidad derivados de los nuevos modelos de negocio que seleccionan a los consumidores particulares a través de la *elaboración de perfiles conductuales*. El Grupo de trabajo señala que tales cuestiones se han tratado recientemente, sin ofrecerse una solución al respecto, en el contexto de ciertas investigaciones sobre competencia llevadas a cabo en los Estados Unidos de América y en la UE, y recomienda que la ENISA encargue la realización de un estudio exhaustivo de tales cuestiones en el que se haga especial hincapié en la economía conductual. El Grupo señala asimismo que, aunque ciertos órganos supervisores y el sector empresarial afirman que existen incentivos adecuados para garantizar una autorregulación satisfactoria, las investigaciones académicas llevadas a cabo[2,3] ofrecen escaso respaldo a tal opinión. Quizá haya que evaluar si se necesitan nuevos principios en materia de intimidad y nuevas estructuras de mercado para garantizar que las fuerzas de la competencia fomentan (en lugar de socavar) la protección de la intimidad. La ENISA se halla en una buena posición para fomentar esta investigación, en su calidad de «facilitador» independiente de la constitución de redes de ámbito comunitario y de análisis de información, y para garantizar que sus conclusiones hallen reflejo en las políticas de la UE.

Recomendamos a la ENISA que encargue la realización de investigaciones que continúen el trabajo emprendido en materia de protección de la intimidad y tecnología, con objeto de lograr una comprensión más profunda. En concreto, debe hacerse un análisis exhaustivo de la estructura de mercado de los servicios en línea sustentados publicitariamente y, en

[2] Véase http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.

[3] Tseng, Jimmy C: «An Economic Approach towards Privacy Enforcement», presentación en el taller *PRIME/ERIM Privacy for Business Workshop*, Rotterdam, diciembre de 2004. Véase https://www.prime-project.eu/events/external/ERIM%20Privacy%20for%20Business%20Workshop/Tseng3.ppt.

particular, de la influencia económica de la elaboración de perfiles conductuales, haciendo hincapié en la aplicación eficaz de los principios de protección de datos y en la autonomía de la persona a la que se refieren éstos. El estudio debe evaluar con imparcialidad la posible eficacia de la autorregulación y analizar si en el arbitraje reglamentario surgen diferencias en la definición de los datos personales[4,5] entre Estados miembros.

[4] Reidenberg, Joel R., Paul M. Schwartz: Data-Protection Law and On-Line Services: *Regulatory Responses*, Bruselas, 1998, http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf.

[5] Bohm, Nicholas, Richard Clayton: *Open Letter to the Information Commissioner*, *Foundation for Information Policy Research*, marzo de 2008, http://www.fipr.org/080317icoletter.html.

3. Una historia aleccionadora

En esta sección describimos una situación hipotética realista referida a un usuario en la que se ponen de manifiesto buena parte de las lagunas y los desafíos enumerados en la sección anterior y sobre los cuales se profundiza en la siguiente.

Sylvia ha experimentado recientemente una serie de problemas relacionados con su derecho a la intimidad. Desde hace un tiempo, su portal en línea y motor de búsqueda preferidos le muestran anuncios que parecen estar misteriosamente vinculados a ciertos aspectos de su vida privada; es más, algunos hacen referencia a una enfermedad sobre la que ha estado investigando por Internet. Sylvia está preocupada, ya que cree que tuvo cuidado de no iniciar sesión en ninguno de los sitios web de los que es usuaria mientras realizaba su investigación y no introdujo ninguna otra información personal que la identificara. Además, le intriga que, cuando hace clic en algún anuncio que le interesa, reciba una oferta menos favorable que la que aparece cuando hace uso del ordenador de un amigo. Cree que ello puede estar relacionado con las «cookies» pero, al tratar de conocer los diferentes tipos de «cookies» que existen y cómo controlarlos, la información correspondiente le parece muy confusa. Sin embargo, si se limita a borrar y desactivar todas las «cookies» de su navegador, el uso de la mayoría de sus sitios web preferidos se vuelve muy incómodo.

Sabe que las leyes sobre protección de datos de su país le conceden el derecho de averiguar qué sabe de su persona cualquier organización, pero está desconcertada porque, cuando analiza la política de protección de la intimidad de los sitios webs que visita, parece que, a menos que se registre e inicie una sesión, todos le indican que no están recopilando información personal alguna. Por lo tanto, no sabe cómo empezar a ejercer el derecho que le otorga la ley para averiguar qué está sucediendo.

En ocasiones, Sylvia facilita su dirección de correo electrónico y su número de teléfono móvil en sitios web que prestan servicios en línea y en algunos establecimientos comerciales de su localidad en los que adquiere diversos productos. Se ha dado cuenta de que, cuando visita otras tiendas, no es raro que reciba gran cantidad de publicidad por correo electrónico y a través de mensajes SMS referida a productos del tipo de los que ha estado buscando. Empieza a preguntarse si tales anuncios podrían relacionarse con las pequeñas etiquetas electrónicas que ha percibido que llevan algunos de los productos que compra. Estos anuncios aparecen asimismo en el navegador web de su teléfono móvil conforme se desplaza por la ciudad y le resulta molesto tener que hacer uso del ancho de banda que está pagando para acceder a una página para declarar que no desea recibir información esta índole (opt-out). Sin embargo, por mucho que visite tales páginas para excluir su nombre de la lista de

destinatarios, parece que sigue recibiendo publicidad importuna de cada vez más empresas.

Sylvia es una activa defensora de una causa política controvertida y, aunque sus actividades son legítimas, su amigo Michael (a quien en ocasiones le deja hacer uso de su ordenador) ha sido parado por la policía de camino a alguna manifestación y ha tenido que responder multitud de preguntas al visitar un país extranjero. Sylvia se da cuenta de que sus hábitos de visita de sitios web, sus desplazamientos por la ciudad y los productos que compra parecen estar empezando a relacionarse de algún modo que no alcanza a comprender. Se pregunta durante cuánto tiempo se conserva esta información y si la legislación de su país permite a la policía acceder a ella y en qué condiciones. A ves, ha leído artículos en la prensa sobre nuevas leyes en este ámbito, pero los detalles que se ofrecen son contradictorios y parecen inducir a confusión de un modo casi deliberado. De camino a una nueva manifestación, la policía detiene su automóvil y le interroga sobre unas pinturas en spray y unas herramientas que adquirió (pagando en efectivo) en una ferretería para hacer ciertas reparaciones domésticas y, asimismo, sobre los motivos de sus visitas a cierto sitio web de carácter político. De vuelta a casa, comprueba que los artículos que compró llevan unas etiquetas de radiofrecuencia (RFID), aunque no tiene ni idea de cómo ha sabido la policía lo del sitio web.

Hace una llamada al servicio de información de la autoridad de protección de datos de su país. Resulta que el sitio web en que está interesada está alojado en otro Estado miembro de la UE, por lo que se le aconseja que se ponga en contacto con la autoridad de protección de datos de ese país. Después de enviar varios correos electrónicos a la APD extranjera, al final consigue respuesta de una persona que entiende su idioma y lo que quiere. Se le recomienda que se ponga en contacto con el sitio web correspondiente y así lo hace, pero sus mensajes son ignorados o reciben una respuesta automática de nula utilidad. Por fin, acaba escribiendo una carta a la dirección del sitio web, que no figuraba en línea pero que ha averiguado consultando el registro público de «responsables del tratamiento de datos». Sin embargo, tiene un problema: como en un principio el sitio web no le inspiraba mucha confianza, se había registrado en él con un nombre inventado. Tras intercambiar algunos mensajes más con la APD y con el sitio web, éstos acaban accediendo a su petición (aunque para ello tiene que remitirles la contraseña de su cuenta por correo). Sylvia no comprende muy bien por qué tiene que facilitar su nombre real y su dirección (ya que también ha tenido que proporcionar su nombre de usuaria y su contraseña), pero renuncia a discutir este punto con la APD y con el sitio web. Tras enviar un giro postal internacional por importe de 15 euros (el sitio web no aceptaba pagos en línea), el paquete de documentos que recibe un mes más tarde contiene información sobre el uso que ha hecho del servicio de correo electrónico del sitio web, pero no sobre las «cookies» o la navegación realizada por el sitio sin haber iniciado sesión. Ésta era la información que deseaba realmente recibir (incluida especialmente, una explicación de cómo se había transferido a otros sitios web o a las autoridades). «De nuevo se pone con

contacto con la APD, que le indica que, con arreglo a su interpretación de la legislación nacional de protección de datos, el sitio web no está obligado a facilitarle tal información. A estas alturas, Sylvia está realmente disgustada por los desafíos que le plantea el ejercicio de sus derechos de protección de datos y por la inutilidad de éstos para esclarecer las circunstancias que verdaderamente afectan a la protección de su intimidad en línea. Tiene una larga lista de empresas a las que podría escribir: las tiendas donde compró productos con etiquetas electrónicas, los otros sitios web que usa y, por supuesto, su proveedor de servicios de Internet y su empresa de telefonía móvil, pero para ello tendría que pagar mucho dinero en tasas de acceso y además piensa que la mayoría acabarían por decirle que «no saben quién es», por lo que teme obtener los mismos resultados insatisfactorios. Por fortuna, tiene un amigo que es abogado especializado en la protección de la intimidad y que decide hacerse cargo de su caso. Después de seis meses de paciente investigación y de un aluvión de correspondencia jurídica, acaba identificando los «identificadores RFID» y las «cookies» a las que se debe que la policía la interrogara de camino a la manifestación. No obstante, las únicas empresas a través de las cuales la policía pudo averiguar su verdadera identidad no le facilitan más información, si bien una de ellas, más solícita, le remite a la cláusula de la legislación sobre protección de datos en la que se dispone que no hay obligación de facilitar información a las «personas sospechosas».

Sylvia reconoce haber perdido enteramente el control de su vida privada y se siente preocupada además porque, después de todos los esfuerzos jurídicos emprendidos para ejercer sus derechos, pueda considerársela una persona «problemática» y se incluya su nombre en listas que le causen incluso más problemas en el futuro, cuando no dificultades con su empleo, su seguro médico o los créditos que solicite. Decide abandonar su actividad política, eliminar todas las etiquetas de prendas de ropa, adquirir un nuevo ordenador y cambiar de PSI, cancelar todas sus cuentas en línea y utilizar un teléfono móvil con tarjeta prepago, aunque no está segura de hasta qué punto sigue siendo posible rastrear sus movimientos. Cuenta a sus amigos sus surrealistas experiencias con la burocracia de la protección de la intimidad, aunque éstos no se creen en verdad su historia y piensan que se está volviendo algo excéntrica. Después de todo, saben que en Europa existe la legislación más estricta en materia de protección de la intimidad y no parece que se trate de un problema del que la mayoría de la gente, los medios de comunicación o los políticos se preocupen mucho.

Finalmente, Sylvia averigua que existe un nuevo paquete de programas informáticos que funciona con una serie de conocidos sitios web que gozan de una buena reputación en materia de protección de la intimidad. El paquete en cuestión le permite descargarse a su ordenador un catálogo completo de información sobre su interacción con los sitios web. Le sorprende la cantidad de detalles que se almacenan sobre sus hábitos de navegación por la red y también averigua que una parte de esta información se facilita —mediante las «cookies»— a otras empresas con fines publicitarios. Elige un PSI que participa

en este programa, el cual le permite averiguar qué «dirección IP» ha estado utilizando en un momento determinado. Haciendo uso de esta información, puede visitar otros sitios web y averiguar de manera automática de qué información disponen sobre la navegación por ellos (aunque sólo algunos Estados miembros de la UE consideran dicha información como «datos personales»). El paquete informático dispone incluso de una función de análisis que le permite comparar durante cuánto tiempo conservan los sitios web los datos sobre su conducta en línea y si ello cumple lo establecido en la política de protección de la intimidad (aunque, en su opinión, la política de la mayoría de los sitios es demasiado vaga para que el programa pueda desempeñar esta función). Además, este paquete sólo funciona con un número bastante reducido de sitios web y algunos de los que considera más útiles no participan en el servicio de descarga. Sorprendentemente, algunos de los sitios más innovadores de los Estados Unidos empiezan a habilitar este servicio de descarga de «datos de atención», aunque a estas alturas Sylvia ha aprendido a tener mucho cuidado con la letra pequeña, ya que ha comprobado que cualquiera que acceda a estos datos podría intuir algunos de sus pensamientos más íntimos.

Su abogado también tiene buenas noticias que darle. Después de más de dos años, un hermético «Tribunal de datos» se ha pronunciado por fin a su favor y la policía ha admitido que nunca debería haber considerado a Sylvia una «persona sospechosa»; además, por fin descubre que las empresas con las que trataba revelaron a la policía una completa serie de datos sobre su vida electrónica. Las malas noticias consisten en que esa información se reveló siguiendo procedimientos adecuados (se consideró «proporcionada» en su momento, a la luz de la información disponible y de las circunstancias), por lo no ha lugar a demandar a la policía o a las empresas exigiéndoles una indemnización de daños y perjuicios por todas las molestias y la burocracia (por expresarlo de un modo suave) que ha tenido que padecer. En apariencia, todos los estamentos «oficiales» consideran que todo se hizo tal como se debía.

Sylvia se pregunta por qué va a meterse nadie en actividades políticas para impulsar cambios sociales cuando las consecuencias pueden ser tan inquietantes. Sabe que la democracia es un sistema imperfecto y que, en ocasiones, la justicia puede ser algo arbitraria, pero, a su juicio, la moderna vida electrónica desalienta el activismo cívico y ha creado un siniestro Estado de control. Sea como fuere, ella ha acabado harta de política (y de vida en línea), aunque se pregunta qué tipo de democracia heredarían sus hijos si todo el mundo tomara la misma decisión. Es consciente de que jamás habría entendido lo sucedido sin la ayuda de su amigo el abogado especializado en la protección de la intimidad (cuya minuta no podría haber sufragado). Acaso el paquete informático de acceso y gestión de su propia información personal le habría ayudado, si hubiera dado con él antes, permitiéndole calibrar en qué medida su conducta en línea le exponía a riesgos de vulneración de su intimidad, aunque también ha leído que la empresa de software ha dejado de desarrollarlo. Al parecer, el número de personas lo bastante preocupadas por su intimidad en cada momento no era lo bastante elevado para garantizar la

rentabilidad del programa y los sitios web importantes, que a ella le gustaba visitar, no estaban, en verdad, interesados en participar.

Enlaces

Para conocer otras hipótesis mucho más pormenorizadas, consúltense los «Dark Scenarios» del proyecto SWAMI en http://is.jrc.es/pages/TFS/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf.

4. Lagunas y desafíos en materia de protección de la intimidad

A continuación se enumeran las doce principales lagunas en materia de protección de la intimidad que el Grupo de trabajo ha identificado entre la normativa de protección de datos y la realidad del entorno socioeconómico en continua evolución. Cada sección comienza con una descripción de la laguna identificada y enumera luego los desafíos identificados en materia de investigación y desarrollo (I+D), en materia jurídica y en materia de comunicación.

4.1 Inclusión digital en relación con la protección de la intimidad

Una laguna fundamental es la falta de sensibilización y de comprensión del tema de la protección de la intimidad en las relaciones entre las personas, así como la falta de capacidad para obrar adecuadamente.

Lagunas concretas

Las personas no son conscientes de los problemas referidos a la protección de la intimidad o bien son incapaces de proteger ésta en el marco actual de las TIC

Muchas personas desconocen por completo los importantes problemas de protección de la intimidad que resultan del uso de las nuevas tecnologías de recogida de datos, las redes sociales, las tecnologías omnipresentes, etc. Otras se sienten incómodas con algún tipo de tratamiento de datos, pero no acaban de comprender plenamente las posibles consecuencias de sus acciones en su propia intimidad. Otras acaso conozcan estos problemas de protección de la intimidad pero no saben qué hacer para evitarlos. Con frecuencia, el deseo de protección induce a rehusar toda participación en el mundo digital y, por tanto, a disfrutar de los beneficios de la sociedad de la información. Y quienes desean disfrutar de estos beneficios a menudo renuncian a la protección de su intimidad, considerando que no hay otra elección.

Las vías de recurso requieren mucho tiempo y, en ocasiones, resultan ineficaces

Para los usuarios que saben cómo proteger su intimidad, la adopción de las medidas necesarias puede ser demasiado costosa o engorrosa. Cabe decir lo mismo de las situaciones en las que se vulnera su derecho a la intimidad. Las vías de recurso suelen llevar mucho tiempo y, en ocasiones, los efectos de la vulneración de la intimidad ni siquiera son reversibles.

Existe el riesgo de que la falta de sensibilización y de capacidad para actuar de manera adecuada divida a la sociedad entre quienes gozan de intimidad y quienes no gozan de ella.

La «usabilidad» de las herramientas de protección de la intimidad es insuficiente«

La sociedad de la información ha de abordar el problema de la inclusión digital en lo que respecta a las TIC, es decir, el problema de cómo hacerlas más accesibles a los usuarios. Puesto que los efectos sobre la intimidad, en el ámbito de las TIC, suelen proceder de acciones de los usuarios, los desafíos que plantea la inclusión digital se hacen, si cabe, más apremiantes cuando lo que hay que proteger es la intimidad de los usuarios en las TIC, en particular de las personas mayores o con discapacidad. La «usabilidad» constituye una cuestión importante a la que, no obstante, no se ha dado una solución satisfactoria al diseñar herramientas para la protección de la intimidad personal.

Necesidad de incluir a los jóvenes

Un grupo concreto que muestra la necesidad de inclusión digital en el ámbito de la protección de la intimidad es el de los jóvenes, es decir, los niños y adolescentes. Los jóvenes presentan un umbral de uso de las TIC bajo. Sin embargo, en numerosas ocasiones representan un objeto de seducción más sencillo para determinados servicios que ofrecen juegos u otras aplicaciones de entretenimiento en los que se les pide que revelen información sobre ellos mismos y, posiblemente, sobre parientes y amigos.

Soluciones propuestas

La sensibilización del público general respecto a las cuestiones ligadas a la intimidad precisa planteamientos distintos según los destinatarios de que se trate. Por ejemplo, el planteamiento aplicado a los niños ha de ser distinto del aplicado a las personas mayores. Unos libros escolares desabridos y redactados en un estilo excesivamente didáctico no representan un método de sensibilización muy prometedor. En lugar de ello, hay que dirigirse a la población a través de ejemplos relevantes para su situación vital, ya sea en la escuela, en la guardería, en la empresa o en cualquier otro lugar.

Desafíos en materia de I+D

Integración de las necesidades éticas y relativas a la intimidad en las TIC

Al desarrollar sistemas TIC de cualquier tipo que puedan relacionarse con el tratamiento de datos personales, deben tenerse en cuenta, desde un inicio, las necesidades éticas y de protección de la intimidad. Los sistemas TIC deben permitir a las personas interesadas proteger su intimidad y ejercer sus derechos a la protección de los datos, en lugar de dejar de lado a grandes segmentos de población. En el ámbito de la inclusión basada en la edad, el proyecto SENIOR[6] está trabajando ya para facilitar un examen sistemático, haciendo uso del diálogo como instrumento fundamental para evaluar los aspectos sociales, éticos y de protección de la intimidad que plantean las TIC y el envejecimiento.

Necesidad de que los usuarios cuenten con herramientas de asistencia

El desarrollo de herramientas de asistencia de fácil manejo tales como «asistentes de protección de la intimidad» (*privacy wizard*) —ofrecidos acaso de manera gratuita por los Estados en apoyo de sus ciudadanos— podría ser beneficioso para lograr el fin de educar a los usuarios. Por ejemplo, un «asistente de protección de la intimidad» ofrecido como complemento para el navegador

[6] http://seniorproject.eu/

podría advertir al usuario de las consecuencias que tiene el suministro de información personal a un sitio web (por ejemplo, el nombre de soltera de la madre, el número de identificación, etc.). Asimismo, estas herramientas podrían utilizarse para establecer unos valores por defecto al configurar el software de acceso a Internet o los sistemas de gestión de la identidad. La incorporación de estos tipos de herramientas de ayuda directamente en los sistemas TIC convencionales supondría un método automático de educar a los usuarios acerca de las consecuencias de sus actos en la esfera de su intimidad personal.

Desafíos en materia jurídica

Tanto la Directiva 1995/46/CE sobre la protección en el tratamiento de los datos personales como la Directiva 2002/58/CE sobre la protección de la intimidad en el sector de las comunicaciones electrónicas exigen el suministro de información concreta a los interesados. Esta información no debe estar redactada en jerga jurídica, sino que ha de ser comprensible para todos los interesados. En cuanto a los servicios en línea, el Grupo de trabajo del artículo 29 ha publicado diversas opiniones sobre el modo de cumplir tal obligación, por ejemplo, en sus documentos WP43 y WP100. Además, en el documento WP147 se describen las obligaciones de información a los niños en materia de protección de datos.

Necesidad de armonización jurídica y aplicación de la normativa

Sin embargo, por desgracia, en la actualidad es infrecuente que se sigan tales recomendaciones y, en ocasiones, falta incluso información básica. De este modo, es necesario ser aún más claro al describir los requisitos obligatorios de información a los interesados, que en el mejor de los casos están armonizados a nivel europeo. Además, debe hacerse hincapié en el debate en las buenas prácticas en materia de notificación a los interesados y de suministro de información adicional. El proceso de información y sensibilización a los interesados también debe evaluarse en los regímenes de certificación de la protección de la intimidad.

Desafíos en materia de comunicación

Necesidad de educación y formación de la opinión pública

Es preciso que se emitan regularmente documentales que contengan descripciones gráficas de los aspectos concretos que puedan plantear problemas. Mediante folletos y otros soportes audiovisuales (tales como el material del proyecto «YOU decide») se podrían ilustrar los posibles peligros de las tareas de vigilancia que se llevan actualmente a cabo, para que las personas sean conscientes de dónde son objeto de control. Deben ofrecerse simulacros que muestren las consecuencias posibles del suministro de información personal en diversos contextos. La población podría así hacerse una idea de los riesgos a largo plazo que afectan a muchos tipos de información personal, en particular los más sensibles y relativos a la personalidad. En las escuelas, podrían organizarse juegos de rol para sensibilizar a los alumnos, por ejemplo, respecto a

las consecuencias que la divulgación de datos en las redes sociales podría tener en las entrevistas de trabajo realizadas varios años después.[7]

Es asimismo importante la educación convencional en el seno de la familia. Ya existe una serie de directrices en materia de protección de la intimidad en el mundo no digital que indican a los padres cómo inculcar ciertos mensajes a sus hijos, como el de decir «no» cuando se vulnera su esfera de intimidad física o el no acompañar a extraños. Se deben asimismo ofrecer a los padres las competencias necesarias para enseñar a sus hijos a protegerse en el mundo de las TIC. Y lo mismo puede ocurrir a la inversa, esto es, que los hijos enseñen a sus padres o abuelos a comprender los efectos de las TIC en su intimidad y a utilizar herramientas de protección.

Los profesores, las familias, los medios de comunicación y las instituciones del Estado deben participar en el proceso de educación y formación —posiblemente permanente— de todos los ciudadanos, el cual debe incluir el modo de interpretar la información relevante para la intimidad (políticas o certificados de protección de la intimidad) y de gestionar los riesgos de vulneración de ésta.

Enlaces

Grupo de trabajo del artículo 29: Recomendación 2/2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, 5020/01/EN/Final, WP 43, aprobada el 17 de mayo de 2001, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43es.pdf

Grupo de trabajo del artículo 29: Dictamen sobre una mayor armonización de las disposiciones relativas a la información, versión de 25 de noviembre de 2004, 11987/04/EN, WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_es.pdf

Grupo de trabajo del artículo 29: Documento de trabajo 1/2008 sobre la protección de los datos personales de los niños (Directrices generales y el caso especial de las escuelas), 00483/08/EN, WP 147, aprobado el 18 de de febrero de 2008, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

Inspección de Datos, en colaboración con la Dirección de Educación y Formación de Noruega y el Consejo Noruego de Tecnología: *YOU decide ... Thoughts and facts about protecting your personal data*, enero de 2007, http://www.dubestemmer.no/pdf/english-brochure.pdf

SENIOR – *Social Ethical and Privacy Needs in ICT for Older People*, proyecto del PM7 2008-2009, http://seniorproject.eu/

[7] Se emprendió esta iniciativa en varias escuelas durante la segunda edición del Día europeo de la protección de datos, el 28 de enero de 2008. Consúltese, asimismo, en línea: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Data_Protection_Day_default.asp.

4.2 Mejora de las herramientas de asistencia al usuario

Las herramientas de asistencia al usuario contribuyen a que las personas puedan inspeccionar, controlar y comunicar sus datos y sus preferencias.

En el caso ideal, los interesados deberían gozar de una «intimidad ubicua», es decir, de una intimidad que, por defecto, precisara una configuración y una gestión nulas y que les permitiera revelar libremente datos personales; asimismo, se les debería ofrecer una serie de opciones por defecto que les garantizaran la protección que deseen. Sin embargo, el mantenimiento de la intimidad y de la seguridad exigirá probablemente, en todos los casos, un esfuerzo por parte de la persona. Ello se debe a que la intimidad y la seguridad son estructuras complejas que dependen mucho de la situación individual y del contexto particular en el que se intercambian o se revelan datos. Las herramientas de asistencia al usuario ayudan a mantener la intimidad, ofreciendo recursos de inspección, control y comunicación.

Lagunas concretas

La naturaleza de las herramientas actuales es fragmentaria y dispersa

El mundo digital de hoy no ofrece un «paquete de protección de la intimidad» completo para usuarios finales que les ayude a gestionar todos los aspectos de su intimidad, sino únicamente una serie de herramientas dispersas que, por lo general, sólo permiten solucionar problemas concretos.

Precisan un considerable esfuerzo del consumidor para su uso

Además, la mayor parte de la tecnología actual de protección de la intimidad impone una pesada carga para el interesado, a quien se exige que gestione identidades, «ofusque» las consultas sobre localizaciones y «anonimice» el tráfico por Internet, no sólo frente al ordenador sino de manera constante, a lo largo de todo el día, en situaciones que van desde las comparecencias en público hasta los actos de índole empresarial y las reuniones privadas.

Si no se les impulsa a ello, la mayoría de las personas quizá no se molesten en el mantenimiento de su intimidad

Este simple modelo de notificación-elección puede dar lugar a una situación en la que la mayoría de las personas no se molesten en hacer el esfuerzo, de manera que la protección de la intimidad se convierta en un concepto elitista que cultiven unos pocos fundamentalistas de la misma. Incluso a quienes desean invertir recursos en la protección de su intimidad se les puede engañar para que revelen más información de la que pensaban dar o, simplemente, se sientan abrumados por la complejidad del mundo del tratamiento de datos.

Soluciones propuestas

La asistencia puede consistir en el ofrecimiento a las partes de herramientas tecnológicas mejor integradas y más fácilmente utilizables, o en la puesta a su disposición de esas herramientas en situaciones excepcionales, como cuando la persona desee averiguar los detalles de una recogida de datos concretos. Puede adoptar asimismo la forma de una mejora de la estrategia educativa dirigida a enseñar a los ciudadanos cómo controlar y gestionar adecuadamente su intimidad.

Desafíos en materia de I+D

Fomentar la facilidad de uso de las herramientas de asistencia

La facilidad de uso reviste una importancia especial en el caso de las herramientas de asistencia al usuario, ya que éste no accederá a la información que le concierne si le resulta complicado y/o costoso (tanto en tiempo como en dinero). Estas herramientas pueden hacer uso de la técnica del «seguimiento de datos» para permitir a los usuarios la inspección de los flujos de datos que les afectan, a saber, cuándo se divulgan datos personales, a quién se divulgan y con qué fines. Los diseñadores de sistemas deben contar con la necesaria educación y formación para el desarrollo de herramientas acordes con las directrices de conceptualización utilizable y la aplicación de sistemas de TIC seguros y ajustados a la normativa sobre protección de la intimidad. Para garantizar una correcta transposición de la normativa y el lenguaje jurídicos a las interfaces de usuario, será necesario contar con la participación de las autoridades de protección de datos.

Inclusión de información jurídica en los protocolos técnicos

Normas técnicas tales como los protocolos de comunicación de RFID pueden incluir asimismo referencias adicionales a la legislación aplicable, a la identidad del responsable de la recogida de datos o a los plazos de uso y conservación previstos.

Desafíos en materia jurídica

Unos pictogramas normalizados facilitan la comprensión de cuestiones jurídicas

Para facilitar la accesibilidad y la comprensibilidad de las políticas de protección de la intimidad se han propuesto una serie de pictogramas que expresan contenidos en este ámbito al tiempo que ahorran a la población la necesidad de estudiar la jerga jurídica, que puede inducir a confusión. La normalización de tales iconos puede contribuir a facilitar la percepción y la elección. Sin embargo, las propuestas existentes no se centran aún en la legislación europea de protección de datos.

Desafíos en materia de comunicación

Un apoyo activo a la educación del usuario por parte de los Estados y de las APD

Los Estados pueden y deben apoyar el desarrollo de herramientas de asistencia. En ámbitos concretos de la administración electrónica (*e-government*) y la participación electrónica (*e-participation*) en los que los Estados implican de manera directa a sus ciudadanos en el tratamiento de sus datos, deben ofrecer modelos de herramientas de asistencia en materia de seguridad y intimidad y enseñar a sus ciudadanos a utilizar éstas. Se puede asignar a las autoridades de protección de datos la tarea de apoyar a los usuarios educándoles, facilitándoles archivos de configuración o asistentes para la protección de la intimidad descargables en lo posible, dándoles instrucciones sobre cómo protegerse en entornos típicos y ofreciéndoles un servicio de atención general. Los avatares pueden representar una opción interesante para ofrecer a los usuarios unas metáforas más sencillas para comprender y gestionar la identidad en línea y las «identidades parciales». Ello está estrechamente ligado a las lagunas y los desafíos identificados en los ámbitos de la inclusión digital en relación con la

protección de la intimidad, el acceso en línea a los datos personales y la información sobre incidentes de seguridad.

Enlaces

Rundle[8] y Mehldau[9] han propuesto una serie de ejemplos de iconos sobre protección de la intimidad.

El proyecto PRIME ha investigado los requisitos de diseño de interfaces de usuario en las herramientas de protección de la intimidad.[10]

4.3 Derecho de acceso a los datos personales: medidas para una aplicación eficaz

Toda persona goza de derecho de acceso y rectificación

El artículo 12 de la Directiva 1995/46/CE relativa al tratamiento de datos personales establece el derecho de acceso de toda persona, es decir, el derecho de ésta a obtener del responsable del tratamiento la confirmación de la existencia o inexistencia del tratamiento de los datos que le conciernen, así como información de los fines de dicho tratamiento, las categorías de datos a que se refiera y los destinatarios o las categorías de destinatarios a quienes se comuniquen los datos. Además, el mismo artículo establece el derecho a obtener del responsable del tratamiento la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa de su carácter incompleto o inexacto.

En la actualidad ha aumentado la importancia y la urgencia de las razones que justificaron el establecimiento de tal derecho. Éste no constituye un mero apoyo para facilitar la reparación en casos concretos, sino que debe funcionar como mecanismo básico de transparencia sociopolítica para advertir a los responsables de la formulación de políticas en caso de que la protección de la intimidad se esté viendo amenazada sistemáticamente en algún sector. Dos encuestas del Eurobarómetro realizadas a lo largo de los cinco últimos años han confirmado una disminución de la sensibilización y del ejercicio de los derechos de acceso, por razones obvias: la obtención de toda la información a la que se tiene derecho, cuando se necesita y en una forma que sea útil, resulta frustrante, onerosa e incómoda.

[8] Véase http://identityproject.lse.ac.uk/mary.pdf
[9] Véase http://asset.netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf
[10] Véase https://www.prime-project.eu/prime_products/reports/

Lagunas concretas

El acceso en línea a los datos personales facilita un ejercicio más cómodo del derecho a la intimidad de las personas

El derecho del interesado de acceder a sus datos personales se ha tornado en un derecho humano «Cenicienta». La retórica del fomento de la sociedad de la información resuena de llamamientos a la eficiencia de las empresas, a la innovación y a la comodidad para los ciudadanos. Sin embargo, si alguien desea seguir el rastro de los datos que se conservan sobre él y comprender las inferencias hechas a partir de ellos y que influyen en el modo de tratarlos, tendrá que superar una legalista carrera de obstáculos que bien podrían haber concebido Dickens y Kafka. Existe una laguna en la oferta a las personas de unos métodos más sencillos de ejercicio de su derecho a la intimidad, en particular a través de un acceso en línea a los datos personales que pueda reducir de manera significativa tal umbral. Incluso en el caso de los servicios en línea, lo normal es que los usuarios no gocen de acceso en línea a todos sus datos personales, incluidos los almacenados en archivos de registro o los tratados por sistemas de elaboración de perfiles, calificación o extracción de datos.

Lo primero que debe considerarse para la mejora del ejercicio de este derecho es garantizar una autenticación satisfactoria de la persona a la que se refiere la información y que formula la petición. Si el proceso de autenticación es deficiente, dará lugar a la mayor laguna en la protección de la intimidad: las solicitudes de acceso «pretextadas». Y sin embargo se dispone de la herramienta ideal para la autenticación del acceso a los datos personales: los sistemas de gestión de la identidad centrados en el usuario, que permiten a éste gestionar las relaciones en línea con una pluralidad responsables del tratamiento de datos no relacionados entre sí y establecen un sólido marco de autenticación mutua de cada parte.

El acceso en línea a los datos personales debe ser posible de un modo que minimice el intercambio de datos

Además, faltan procedimientos de acceso a los datos relacionados con seudónimos, lo que reviste particular importancia en el mundo en línea, habida cuenta de la diversidad de identificadores que puede tener un usuario.

Soluciones propuestas

Los interesados deben gozar de un mejor apoyo en el ejercicio de su derecho a la intimidad, sobre todo en el mundo en línea. Los responsables del tratamiento de datos deben ofrecerles acceso en línea siempre que sea posible.

Desafíos en materia de I+D

El responsable del tratamiento debe ofrecer un diseño del acceso a los datos de uso sencillo

Para ofrecer un modo conveniente de ejercer el derecho a la intimidad es necesario contar con interfaces de usuario comprensibles. Los responsables del tratamiento de datos no deben limitar el acceso a los datos principales de sus clientes. Por lo general, el acceso a la lectura de datos en línea no plantea problemas cuando el usuario se ha autenticado y los datos personales solicitados pueden mostrarse por separado de otra información protegida; en cambio, la rectificación o la supresión de datos puede no resultar tan fácil de llevar a la práctica en caso de conflicto con otros objetivos. Por ejemplo, los usuarios no

deben tener la posibilidad de alterar historiales de auditoría o pruebas digitales. En concreto, será necesario realizar investigaciones que permitan

- estructurar los sistemas de los responsables del tratamiento de datos de manera que se minimice el efecto de las exenciones (por ejemplo, datos que se relacionen exclusivamente con el interesado y no entrañen otras exenciones),
- adoptar opciones estratégicas de imposición gradual de obligaciones a los responsables del tratamiento de datos que mantienen relaciones de identidad en línea con los interesados, con objeto de garantizar que éstos puedan cumplimentar solicitudes en línea de manera segura y del modo práctico más completo que resulte posible.

Herramientas para usuarios que apoyen el ejercicio del derecho a la intimidad

Además, se puede dotar a los usuarios de herramientas que les asistan para enviar peticiones al responsable del tratamiento de datos o —en caso de necesidad— para presentar reclamaciones ante una autoridad de supervisión. Tales herramientas pueden aprovechar la funcionalidad de la gestión de la identidad controlada por el usuario y de las políticas de protección de la intimidad legibles por máquina. Revisten importancia

- la supresión de las trabas el ejercicio del derecho de acceso a los datos personales que no se adecuen a la situación del acceso en línea,
- las medidas de «metaintimidad» necesarias para proteger a las personas de la interferencia, la vigilancia o la discriminación derivadas del ejercicio de sus derechos de acceso y
- los procedimientos para el ejercicio de los derechos de acceso frente a los responsables del tratamiento de datos «indirectos» (a saber, los responsables del tratamiento que conservan datos referibles a las personas únicamente a través de un identificador seudónimo).

Métodos de minimización de datos para el acceso a los datos personales

El derecho de acceso a los datos personales exige una cierta prueba de la identidad, para que no se revelen éstos a una persona no autorizada. Si un usuario ha revelado datos con un seudónimo determinado, se ha de probar que el usuario que los solicita es realmente su titular. Ello exige unos mecanismos adecuados de autenticación —minimización de datos— entre los que cabe incluir los siguientes:

- un sólido marco de autenticación mutua del interesado y el responsable del tratamiento de datos mediante sistemas de gestión de la identidad centrados en el usuario adecuados para la presentación y la cumplimentación de solicitudes en línea y
- un nivel más elevado de autenticación inequívoca del interesado, con el fin de autorizar la activación de mecanismos de acceso a datos personales en línea ante un responsable del tratamiento específico.

Desafíos en materia jurídica

Exigencia legislativa de acceso en línea

En cuanto a los servicios de tratamiento de datos personales en Internet y otros marcos en línea, debe exigirse por la vía legislativa, en la medida de lo posible, la oferta de un acceso y otros cauces en línea para el ejercicio del derecho a la intimidad.

Exigencia de unos seudónimos adecuados para un acceso conforme al principio de minimización de datos

Además, ha de debatirse si en el tratamiento de datos son aceptables los seudónimos que no permiten demostrar la titularidad personal de un modo ajustado al principio de la minimización de datos (al menos sin la necesidad de revelar la identidad civil de la persona), toda vez que, en tal caso, las personas no pueden ejercer su derecho a la intimidad. Ello podría requerir, asimismo,

- opciones de garantías jurídicas extraordinarias frente a riesgos de acceso a los datos mediante coacción y
- un marco de órganos de supervisión que evalúen la idoneidad de las medidas de seguridad que protegen los mecanismos y procedimientos de acceso en línea.

Desafíos en materia de comunicación

Informar a las personas de sus derechos en materia de intimidad

Se debe sensibilizar a las personas y a los responsables del tratamiento de datos respecto a los derechos relativos a la intimidad y de las posibilidades de ejercerlos.

Enlaces

El proyecto del PM6 PRIME (*Privacy and Identity Management for Europe*[11]) propuso métodos de integración del acceso en línea a los datos personales en el marco de un sistema de gestión de la identidad controlado por el usuario.

En ciertos países, los ciudadanos gozan de acceso en línea a sus datos personales en el registro nacional, incluido el archivo de registro que contiene los accesos a sus datos, por ejemplo, en Bélgica («mijndossier/mondossier») y Noruega («minside»).

Encuestas del Eurobarómetro sobre protección de datos:

- *Data Protection, Opinion Poll, Special Eurobarometer No. 196, Wave 60.0 – European Opinion Research Group EEIG*, encuesta realizada por encargo de la Dirección General de Mercado Interior, Unidad E4 – Medios de Comunicación y Protección de Datos, diciembre de 2003, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_data_protection.pdf.

- *Data Protection in the European Union – Citizens' perceptions, Analytical Report, Flash Eurobarometer No. 225*, encuesta realizada por Gallup Organization Hungary por encargo de la Dirección General de

[11] https://www.prime-project.eu/

Justicia, Libertad y Seguridad, febrero de 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

4.4 Gestión de la identidad para la separación de contextos

La vinculación a unos fines constituye un importante principio jurídico en Europa

Es sabido que la acumulación de datos personales puede ocasionar graves problemas de vulneración de la intimidad. El principio de la vinculación a unos fines que se establece en la Directiva sobre la protección en el tratamiento de los datos personales aspira a limitar la recogida y posterior utilización de datos a unos fines predeterminados: «Los Estados miembros dispondrán que los datos personales sean: […] b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; […] c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente» (artículo 6, apartado 1, de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales).

La acumulación intercontextual de datos personales pone en peligro la intimidad de las personas

Sin embargo, se observa en Europa una tendencia que está menoscabando este principio, al utilizarse a menudo los datos personales disponibles para fines distintos de los previstos, aunque tal utilización se haya excluido en los procesos legislativos. Por ejemplo, se debate actualmente sobre el posible uso de datos aduaneros con fines policiales o la retención de datos de las telecomunicaciones con fines comerciales. Esta tendencia se ve amplificada por la existencia de cada vez más identificadores únicos, que pueden servir de «Personenkennzeichen» (números de identificación personal). Estos identificadores suelen aparecen en diversos contextos de aplicación (por ejemplo, en diversos ámbitos de la Administración pública o del uso de Internet a través de distintas actividades) y pueden identificar de manera unívoca a la persona que se halla tras ellos. La aparición de datos personales en diversos contextos permite el establecimiento de vínculos intercontextuales, lo que, a su vez, faculta para una elaboración de perfiles cada vez más detallados. Este extremo ha sido reconocido por expertos en materia de intimidad no europeos, como Nissenbaum, quien analiza la cuestión de la intimidad en el marco de la «integridad contextual».

Lagunas concretas

El problema: aumento de la disponibilidad digital de datos personales vinculables

El aumento de la disponibilidad digital de datos personales combinado con el incremento de su «vinculabilidad» representa un importante problema. Aunque los datos sean anónimos en un principio, pueden vincularse a un perfil que, posteriormente, podrá ofrecer información suficiente para identificar a la persona a la que se refieren. El aumento de la vinculabilidad de los datos se debe fundamentalmente a la utilización reiterada de identificadores únicos, introducidos a menudo por los sistemas TIC, a saber, direcciones IP, *cookies* o números índice en bases de datos, aunque la revelación de información tal como

la referida al nombre puede también ser suficiente, en ocasiones, para que los motores de búsqueda acumulen la información relacionada.

Es difícil aplicar el principio de vinculación a unos fines determinados

El principio de vinculación a unos fines determinados resulta difícil de aplicar a menos que los datos ya estén preparados para una utilización ligada a un contexto específico[12]. El uso del principio de minimización de datos sustenta de un modo bastante eficaz el principio de vinculación a unos fines. Existen diversas posibilidades de restricción de los datos a un uso vinculado a un contexto específico, tales como el uso de identificadores sectoriales en la administración electrónica (véase la tarjeta del ciudadano [*Bürgerkarte*] en Austria), el uso de seudónimos distintos en los diferentes sitios web de Internet, la «seudonimización» de los datos personales en las bases de datos o el uso de «credenciales privadas» o «certificados de revelación mínima»: Tales credenciales constituyen métodos favorables a la protección de la intimidad y garantizan la responsabilidad al tiempo que aseguran el anonimato del usuario: sólo se podrá identificar a éste en caso de abuso. Así pues, aplican métodos de responsabilidad en el mundo en línea sin necesidad de que el usuario facilite su nombre real y otra información personal a todas las partes con las que interactúa.

Escasa distribución de soluciones tecnológicas

Aunque todas estas soluciones se analizan como componentes de los sistemas de gestión de la identidad centrados en el usuario y han adquirido madurez a lo largo de los últimos años, los conceptos en que se inspiran, sobre todo los planteamientos más avanzados en materia de credenciales privadas, no se conocen bien, con lo que los diseñadores de aplicaciones rara vez los emplean en sus sistemas TIC. También está poco desarrollado el debate social sobre las condiciones de «vinculabilidad» y «no vinculabilidad» deseadas, ya que numerosos interesados todavía no lo han percibido como una dificultad importante, o bien no conocen las posibles soluciones.

Soluciones propuestas

Desafíos en materia de I+D

Necesidad de mejorar la aplicación

Aunque la madurez de los conceptos de separación de contextos y gestión de la identidad centrada en el usuario ha aumentado en el último año, sigue siendo necesaria una mejor integración, interoperabilidad y usabilidad.

Necesidad de crear las infraestructuras para las credenciales privadas

Asimismo, recomendamos que la Administración pública y la industria contribuyan a la creación de la necesaria infraestructura de expedición e interoperabilidad de credenciales y que hagan uso de éstas en sus sistemas TIC cuando proceda.

[12] Dejamos abierta la cuestión del grado de precisión con el que debe definirse el concepto de uso vinculado a un contexto específico. En determinados contextos, cada transacción puede representar un contexto propio, mientras que en otros casos puede ser apropiado aplicar una perspectiva menos definida. El concepto de los fines puede representar un hito para el debate sobre los contextos, aunque también en este caso faltan las correspondientes disposiciones normativas.

Necesidad de medir la «vinculabilidad»

Además, debe investigarse sobre la medición de la vinculabilidad y la no vinculabilidad. Esta cuestión es importante tanto para el diseño de los sistemas TIC como para el control que el propio usuario ejerce sobre su esfera privada. En el caso concreto del mantenimiento de la intimidad a largo plazo, no se ha respondido a la pregunta de cómo garantizar la protección de datos.

Desafíos en materia jurídica

Evaluación de la legislación actual a la luz de las credenciales privadas

La disponibilidad de tecnologías de separación de contextos influye en la interpretación del principio de minimización de los datos, a saber, que el tratamiento de datos personales no debe ser excesivo, sino que ha de limitarse al mínimo necesario. Recomendamos que los legisladores y los responsables de la formulación de políticas a escala nacional y europea evalúen las leyes actuales a la luz de las credenciales privadas.

Desafíos en materia de comunicación

Entablar un debate social sobre «vinculabilidad» y «no vinculabilidad»

Proponemos que las condiciones de vinculabilidad y no vinculabilidad y las posibles aplicaciones jurídicas, organizativas y tecnológicas se sometan a la atención de los responsables de la formulación de políticas, los desarrolladores, los responsables de la protección de la intimidad y los usuarios. Se trata de un tema de especial importancia en el caso de conceptos que no favorecen una comprensión intuitiva como es el caso de las credenciales privadas.

Enlaces

Brands, Stefan A.: *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000

Camenisch, Jan, Anna Lysyanskaya: *Efficient Nontransferable Anonymous Multishow Credential System with Optional Anonymity Revocation, Research Report* RZ 3295, no. 93341, IBM Research, noviembre de 2000

Chaum, David: Security Without Identification: *Transaction Systems to Make Big Brother Obsolete, Comm*. ACM, vol. 28, no. 10, Oct. 1985, pp. 1030-1044.

Clauß, Sebastian, Marit Köhntopp: *Identity management and its support of multilateral security, Computer Networks* 37(2): 205-219 (2001)

Jøsang, Audun, Simon Pope*: User Centric Identity Management, Proceedings of AusCERT*, Gold Coast, mayo de 2005

Nissenbaum, Helen: *Privacy as Contextual Integrity, Washington Law Review*, Vol. 79, No. 1, 2004

PRIME White Paper – Privacy and Identity Management for Europe V3, https://www.prime-project.eu/prime_products/whitepaper/.

4.5 Información sobre los incidentes de seguridad

Las personas sólo podrán proteger eficazmente su intimidad si disponen de suficiente información sobre el tratamiento que está previsto dar a los datos, los riesgos que afectan a la seguridad y la intimidad conexos y los incidentes relativos a la seguridad y la intimidad que afectan a los datos personales.

Lagunas concretas

No existe la obligación de informar a las personas sobre las vulneraciones de la seguridad y la intimidad.

Con arreglo al marco jurídico europeo vigente en materia de protección de datos, los responsables del tratamiento de datos no están obligados a informar a las personas afectadas del acaecimiento de incidentes relativos a la seguridad y la intimidad. Según el artículo 4 de la Directiva 2002/58/CE[13], la obligación del responsable del tratamiento de datos de mitigar posibles riesgos mediante la adopción de medidas de seguridad y de información al usuario de tales riesgos sólo se activa antes de que se produzca un incidente de seguridad, pero no existe la obligación de comunicación después de que se produzca éste.

Los legisladores podrían pensar que el entorno competitivo, junto al proceso autorregulador, han completado el marco jurídico con la aplicación de las garantías técnicas y organizativas exigidas para la gestión adecuada de un incidente de seguridad. Sin embargo, a la luz de ciertos incidentes críticos y esclarecedores acaecidos, parece que estos primeros incentivos no bastan para promover la necesidad de notificar al usuario final las vulneraciones de la seguridad y para mitigar, de manera anticipatoria, sus efectos negativos.

La carencia o, incluso, la absoluta ausencia de notificación de incidentes socavan asimismo la ejecución de las medidas preventivas exigidas con arreglo al marco jurídico vigente.

Otra consecuencia directa de la ausencia de notificación e información sobre incidentes de seguridad consiste en la elaboración de cifras y estadísticas que no son fiables y que no contribuyen a crear un entorno más fiable y transparente.

Incluso si de dispone de información sobre el hecho de que se ha producido una vulneración de la seguridad, lo normal es que las personas no sepan cómo podría afectarles tal incidente ni cómo reaccionar de un modo adecuado.

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

Soluciones propuestas

Desafíos en materia de I+D

Fuentes de seguridad como formato normalizado de notificación

Sobre la base de las fuentes (*feeds*) de noticias para la notificación de vulnerabilidades relevantes para la seguridad por parte, por ejemplo, de equipos de respuesta a emergencias informáticas, se ha demostrado cómo un prototipo de «fuente de seguridad» podría transferir información sobre amenazas e incidentes en materia de seguridad y intimidad mediante un formato XML estructurado y a través de una fuente RSS, que posteriormente sería interpretada por el sistema de gestión de la identidad del proyecto PRIME (*Privacy and Identity Management for Europe*). Este concepto comprende todos los mecanismos y procedimientos en uso, tales como protocolos, aplicaciones y algoritmos criptográficos, así como el propio software del sistema de gestión de la identidad. En concreto, se informa a los usuarios del riesgo que amenaza a su esfera privada, es decir, quién goza ya o podría gozar de acceso no autorizado a los datos personales, y de las consecuencias, esto es, de las opciones de actuación existente.

Desafíos en materia jurídica

Hemos de obligar jurídicamente a los responsables del tratamiento de datos a comunicar las vulneraciones de la seguridad

Los propios responsables del tratamiento de datos deben estar obligados a informar a las personas a título individual o a través de una comunicación sobre incidentes, análogamente a lo establecido en las *Security Breach Notification Acts* que se emplean en numerosos Estados de los EE.UU.

En noviembre de 2007, la Comisión Europea publicó una propuesta[14] de modificación de la Directiva 2002/58/CE e introdujo la obligación de notificar las vulneraciones de la seguridad.

Los incidentes en materia de vulneración de la intimidad también son relevantes

Nótese que el debate suele centrarse exclusivamente en los incidentes referidos a la seguridad, es decir, en ataques de piratas informáticos (*hackers*) o en datos extraviados. Podrían producirse otros acontecimientos relevantes para la intimidad, tales como las fusiones de empresas que unen sus bases de datos o el cambio del país en el que se tratan los datos personales. Esta clase de información también podría ser relevante para la intimidad personal.

Desafíos en materia de comunicación

La comunicación de incidentes permite al ciudadano gestionar su intimidad

Se debe informar a las personas, de un modo comprensible, de los incidentes relativos a la seguridad y la intimidad que hagan referencia a ellas o a sus datos. También se les debe prestar asesoramiento en cada caso concreto sobre las acciones pertinentes para minimizar los efectos no deseados en su intimidad. Este tipo de información refuerza la transparencia del tratamiento real de los

[14] Propuesta, de 13 de noviembre de 2007, de Directiva del Parlamento Europeo y del Consejo por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

datos referidos a la intimidad y sirve de base para la gestión de la esfera privada de las personas.

Una información más precisa y exhaustiva de las vulneraciones de la seguridad permitiría fomentar unas sólidas garantías posteriores al acaecimiento de incidentes y unas medidas de compensación bien definidas para la gestión de los riesgos residuales.

Múltiples canales de distribución para la información sobre los incidentes

No sólo los propios responsables del tratamiento de datos, sino asimismo otras partes, como la prensa escrita, las autoridades de protección de datos, las organizaciones de protección de los consumidores o las organizaciones que trabajen en el mismo campo, podrían divulgar la información disponible en materia de amenazas e incidentes relativos a la seguridad y la intimidad. Este tipo de información podría transmitirse en un formato digital normalizado que facilite su interpretación por el ordenador del usuario. En concreto, una combinación de sistemas de gestión de la identidad controlados por el usuario podría crear sinergias.

Enlaces

Security Breach Notification Laws: *Views from Chief Security Officers - A Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law*, diciembre de 2007, http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf

Hansen, Marit, Jan Schallaböck: *Extending Policy Negotiation in User-Controlled Identity Management by Privacy & Security Information Services, Position Paper Submission to the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, http://www.w3.org/2006/07/privacy-ws/papers/18-hansen-user-controlled-idm/.

Hansen, Marit: *Marrying Transparency Tools With User-Controlled Identity Management*. En: Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci (editores): *The Future of Identity in the Information Society, Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society*, agosto de 2007; IFIP - International Federation for Information Processing, volumen 262; Springer; 2008, pp. 199-220

Hogan & Hartson Analysys: *Preparing the Next Steps in Regulation of Electronic Communications – A Contribution to the Review of the Electronic Communications Regulatory Framework*. http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/next_steps/regul_of_ecomm_july2006_final.pdf.

Nageler, Antje: *Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem*. Tesis doctoral, Christian-Albrechts-Universität zu Kiel, mayo de 2006.

4.6 Orientación sobre los regímenes de certificación

Los regímenes de certificación pueden contribuir a la verificación del cumplimiento de la normativa

Uno de los principales problemas a los que se enfrenta hoy la sociedad de la información es la falta de transparencia de los productos y servicios TIC en lo que respecta al cumplimiento por su parte de las normas de seguridad y protección de la intimidad. Para los usuarios, los responsables del tratamiento de datos y las APD, el cumplimiento de la normativa de protección de la intimidad representa uno de los principales desafíos que plantean los sistemas TIC. Los regímenes de certificación deben garantizar que un producto o servicio se ha diseñado y puede utilizarse de conformidad con la legislación europea de protección de datos.

Lagunas concretas

En la actualidad no existen tales regímenes de certificación en materia de intimidad

La disponibilidad a día de hoy de soluciones TIC fiables en general y de aplicaciones tecnológicas que protejan la intimidad y la seguridad de los datos en particular reviste una importancia equivalente para todos las partes interesadas en la UE. Así pues, debe hacerse hincapié en el desarrollo de los medios y los criterios necesarios para ofrecer regímenes de certificación fiables y ajustados a las disposiciones en materia de intimidad de un modo armonizado en todos los Estados miembros.

Los regímenes de certificación potencian la eficacia de la protección de la intimidad

En la presente sección, la exposición que sigue ilustra la existencia de la laguna en cuestión, así como los requisitos que han de cumplirse y los efectos o ventajas que podrían obtenerse. Entre éstas cabe incluir ventajas competitivas, el refuerzo de la confianza en los productos certificados, la confianza de la opinión pública y la sensibilización de ésta, el fomento de la protección de la intimidad conforme a un designio y no como un efecto secundario y la aplicación de los principios de la protección de datos de un modo homogéneo y, por ende, más eficaz, a todas las partes interesadas de la sociedad de la información (personas a las que se refieren los datos, responsables del tratamiento de los mismos, autoridades de protección de datos, desarrolladores de TIC, proveedores, fabricantes, Estados miembros, etc.).

Debe fijarse un nivel mínimo de protección de los datos personales

Destacamos aquí que: a) los regímenes de certificación citados deben garantizar en último extremo que un producto concreto cumpla un nivel (mínimo) determinado de protección de los datos personales, b) es necesario desarrollar una metodología orientada a tal fin y al de fomentar la adopción de tales sistemas de certificación y c) los organismos de normalización deben normalizar las referencias, los criterios y las condiciones de certificación empleados para evaluar el cumplimiento de las disposiciones sobre protección de la intimidad.

Soluciones propuestas

Debe incentivarse la certificación

Los Estados miembros deben fomentar y regular los regímenes de certificación, contando siempre con la participación de las asociaciones de consumidores: deben ofrecerse incentivos fiscales a las empresas que cumplan la normativa y los Estados miembros han de considerar la conveniencia de liberar a las empresas de determinadas obligaciones en materia de información siempre que dispongan de un certificado de protección de la intimidad.

Tras evaluar si un sistema de certificación debe ser obligatorio o no, quién debe aprobar su adopción y cómo se ha de lograr la transparencia para alcanzar un consenso general sobre los requisitos en materia de intimidad que deben cumplirse para solucionar dicha laguna, habría que proceder al examen de nuevas soluciones que fomenten el cumplimiento. Por ejemplo, los Estados miembros deben desarrollar herramientas de carácter voluntario para la certificación o la autocertificación del cumplimiento de la legislación sobre protección de datos en cualquier licitación abierta para un contrato público.

Ya hay experiencias con regímenes de certificación

Proponemos que se extraigan enseñanzas de la ejecución de proyectos de investigación similares (por ejemplo, EuroPriSe[15]), incluso procedentes de otros países (Suiza[16]) que han desarrollado tales regímenes de certificación, así como de la experiencia conseguida con las firmas electrónicas acreditadas, las tecnologías de cifrado y sus respectivos marcos jurídicos.

Características fundamentales de un régimen de certificación de la intimidad

Recomendamos que un régimen de certificación conste de las siguientes características fundamentales: Ante todo, las partes que deseen darse a conocer a la opinión pública como certificadores acreditados en materia de intimidad y seguridad deben obtener previamente una certificación a tal efecto otorgada por un (tercero) independiente establecido con anterioridad como organismo de acreditación específico (en cooperación con las APD). Dicha certificación ha de otorgarse una vez comprobado el cumplimiento de los correspondientes requisitos tecnológicos y jurídicos (intimidad con arreglo a un designio, buenas técnicas disponibles, principios relativos al mínimo de intimidad) establecidos en la reglamentación correspondiente adoptada por las APD en cooperación con el Grupo de trabajo del artículo 29 y con la Comisión Europea. Este certificado ha de tener una duración determinada de no más de dos o tres años, por ejemplo, período durante el cual debe preverse la evaluación anual del cumplimiento. En caso de vulneración, abuso, falsedad o apropiación indebida del mismo, deben imponerse sanciones y multas, aparte de su anulación. Es preciso, pues, emprender nuevas medidas legislativas en este sentido, dentro de la Comisión, para facilitar una ejecución y una aplicación armonizadas en toda la Unión

[15] Véase http://www.european-privacy-seal.eu/

[16] Consúltese la *Ordonnance sur les certifications en matiere de protection des donees* (OCPD), 28 de septiembre de 2007, Le Conseil federal suisse, y la *Loi federale sur la protection des donnees* (LPD) de 19 de junio de 1992 (versión de 1 de enero de 2008), L'Assemblee federale de la Confederation Suisse. Véase http://www.admin.ch/ch/e/rs/235_13/index.html.

Europea. En concreto, han de definirse los controles pertinentes y la responsabilidad de los evaluadores y los certificadores.

Es necesaria una normalización internacional

Por último, los regímenes de referencias de certificación deben normalizarse a nivel internacional con el fin de garantizar la armonización y la transparencia de las metodologías empleadas y de los criterios evaluados. Dichas referencias han de contener los criterios que habrían de verificarse al evaluar los productos o servicios en cuestión. Deben también servir de orientación a los evaluadores en cuanto al modo de valorar productos y servicios TIC.

4.7 Herramientas de supervisión

Son necesarias herramientas para una auditoría interna de la intimidad

Las empresas que tratan datos personales deben especificar su política en materia de intimidad y garantizar que se aplica adecuadamente en su entorno. Tal política puede ser, de hecho, muy compleja debido a la gran cantidad de parámetros que se deben tener en cuenta. Al aplicarla, habrían de tenerse en cuenta soluciones de verificación del cumplimiento «escalables» y automatizadas. Sin embargo, la industria no dispone de herramientas de supervisión y gestión adecuadas que sean eficaces para la auditoría interna de la protección de la intimidad.

Tales herramientas también serían útiles para las autoridades de supervisión

Además, las autoridades de protección de datos (APD) se enfrentan continuamente a desafíos en lo que respecta a la aplicación de controles y a la realización de auditorías sobre los datos personales registrados, tratados y utilizados. Por último, aunque el marco jurídico europeo defina de manera detallada las obligaciones y garantías que los responsables de tratamiento de datos han de aplicar y seguir[17], no ofrece herramientas de supervisión prácticas ni pide que se desarrollen en beneficio de las autoridades de control.

Lagunas concretas

La auditoría individual de la intimidad exige un uso intensivo de recursos

Los sistemas TIC que tratan datos personales no suelen estar diseñados para facilitar las actividades de auditoría ni aun de autoauditoría. Tales herramientas de supervisión deben, pues, desarrollarse de manera individualizada, lo que supone una cantidad de recursos adicional. Además, es necesario verificar que la política de intimidad concreta cumple lo previsto en la política de alto nivel al respecto. La intimidad, en suma, precisa un sistema métrico específico, que incluya la relación de las especificaciones de alto nivel con las configuraciones físicas dentro del sistema de información.

Además, habida cuenta del ingente volumen de la actividad de recogida de datos que debe auditarse, es crucial desarrollar técnicas de registro normalizadas y no repudiables que permitan una auditoría automatizada fiable.

[17] Véase, a modo de ejemplo ilustrativo, el artículo 17 de la Directiva 1995/46/CE.

A continuación cabría considerar la conveniencia de poner tales herramientas a disposición de las APD para ayudarles en el desempeño de sus competencias de inspección de un modo continuo y, de ser posible, remoto. El usuario final debe hallarse asimismo en situación de obtener automáticamente información sobre el modo en que se tratan sus datos personales.

Las herramientas de supervisión serían útiles tanto para la industria como para las APD y los usuarios

Soluciones propuestas

Desafíos en materia de I+D

Podrían aplicarse políticas en materia de intimidad (encapsuladas según expresa el término inglés «sticky policies») que obliguen a los responsables del tratamiento. Por motivos de transparencia, ello requeriría documentar no sólo —tal como exigen las leyes en la actualidad— las categorías de destinatarios sino, de un modo preciso, los destinatarios reales.

Paradigma de las «sticky policies»

Unas herramientas eficaces de auditoría automatizada para el desempeño de las actividades de protección de datos facilitarían el cumplimiento de las políticas. Podrían incluirse en los sistemas historiales de auditoría con carácter proactivo para disponer de una ingeniería inversa sobre cualquier política técnica de protección de la intimidad y verificar que cumple los requisitos de una política de intimidad de alto nivel aceptable.

Sincronizar políticas técnicas y jurídicas de protección de la intimidad a través de historiales de auditoría

Deben fomentarse las actividades de I+D referentes a la disponibilidad de herramientas de control más automatizadas, a la trazabilidad y a las operaciones de auditoría. Otra posibilidad es externalizar esta actividad y encomendársela a organismos (privados) acreditados, capaces de llevarla a cabo y de expedir certificados a las organizaciones que cumplan los requisitos en materia de intimidad (véase, por ejemplo, el régimen de certificación aplicado en el cantón de Ginebra, Suiza).

Tanto los auditores internos (el departamento de auditoría) como los externos (la APD competente) podrían beneficiarse del establecimiento de puntos de comprobación (de ser posible, normalizados) en los sistemas TIC y en los flujos de trabajo relativos al tratamiento de datos. Además, los procedimientos de prueba empleados en las auditorías deben comprender todos los casos relevantes. En una supervisión a largo plazo podrían introducirse incluso datos ficticios (*dummy*) para observar si éstos se filtran y acaban apareciendo fuera del sistema TIC. Ello quiere decir que ha de prestarse especial atención para garantizar que estos datos ficticios de prueba no se conviertan en una identidad digital incontrolada de la que se pueda abusar.

Unos puntos de comprobación definidos simplifican la verificación

Desafíos en materia jurídica

Sería posible exigir por ley que el tratamiento de los datos personales sólo esté permitido si los datos proceden de una fuente digna de confianza en la que se hayan documentado todas las transferencias de datos.

Exigencia de historiales de auditoría lo largo de todo el historial de los datos

Acceso remoto para las APD

Podría considerarse la conveniencia de conceder a las APD un acceso remoto y permanente a determinadas funciones de las herramientas de supervisión de la intimidad empleadas por los responsables del tratamiento, con objeto de verificar que los sistemas cumplen los requisitos en materia de notificación y de facilitar las inspecciones.

Desafíos en materia de comunicación

Pruebas internas mediante autoauditoría

Los informes de autoauditoría podrían contribuir asimismo al desempeño eficaz de las tareas de las autoridades de supervisión encaminadas a identificar los puntos más débiles y a centrarse en ellos durante su propio procedimiento de auditoría.

4.8 Orientación sobre buenas técnicas disponibles

Las BTD son una combinación concreta de tecnologías, protocolos y normas

La intimidad y la seguridad son cuestiones complejas que no se podrán resolver de manera definitiva con ningún tipo de solución técnica universal. En lugar de ello, los distintos ámbitos de aplicación exigen un apoyo técnico diferenciado para ofrecer intimidad a los ciudadanos. Dicho apoyo técnico ha de complementarse cuidadosamente con marcos jurídicos y directrices prácticas orientados de manera específica a un ámbito de aplicación concreto o a un conjunto determinado de principios operativos. Denominamos a esta combinación específica de tecnologías, protocolos normas, prácticas, etc., que pueden facilitar un nivel razonable de protección de la intimidad en un ámbito concreto, «buenas técnicas disponibles».

Lagunas concretas

Deben definirse y armonizarse BTD en materia de intimidad y seguridad

Existe una laguna en la definición y posterior armonización —a nivel europeo— de las buenas técnicas disponibles (BTD) en distintos ámbitos y en la determinación del grado en que estas técnicas deben ser empleadas por los responsables y los encargados del tratamiento de datos.

Ejemplo: intimidad relativa a la localización

El debate en curso acerca de las técnicas de protección de la intimidad en lo que respecta a los sistemas de localización podría ilustrar esta laguna. Muchas de las propuestas actuales en esta materia intentan ocultar las solicitudes de localización en una zona lo bastante grande para albergar, al menos, una cifra de otros usuarios equivalente a *k-1*. Es lo que se denomina «k-anonimato». Sin embargo, por muy potente que sea la técnica que se aplique, es importante tratar de un modo más específico su uso práctico. ¿Cómo puede emplear un usuario, por ejemplo, una técnica de *k-anonimato*? ¿Cómo juzgar el valor de la variable *k* que es apropiado o cuándo activar o desactivar el sistema? ¿Cómo conseguir un equilibrio entre la precisión de la localización y la intimidad de ésta? ¿Se debe adoptar simplemente el modelo de un tercero de confianza, en virtud del cual, por ejemplo, el proveedor de los servicios de telefonía móvil administre todos los datos de manera centralizada, y hacer uso de sistemas de bases de datos

estadísticas y de otras herramientas para proteger los perfiles de los usuarios? Distintos ámbitos de aplicación podrían requerir diferentes respuestas.

Soluciones propuestas

La creación de unas BTD en el ámbito de la protección de datos exige tanto identificar técnicas idóneas como establecer un proceso de armonización de las mismas en todos los Estados miembros de la UE.

Desafíos en materia de I+D

Identificar y agrupar tecnologías y prácticas

En una primera fase, habría que identificar los conjuntos de aplicaciones relevantes, sobre todo las agrupadas en torno a los nuevos desarrollos tecnológicos (RFID, servicios basados en la localización, biometría). Luego, habría que agruparlas con arreglo a sus respectivos modelos de flujo de información, es decir, a sus prácticas de tratamiento de datos y sus necesidades de información concretas.

Identificar conjuntos de técnicas adecuados según los ámbitos de aplicación concretos

Una vez identificados los tipos de aplicación genéricos, se podrían estudiar las tecnologías y prácticas actuales y establecer un conjunto bien definido de buenas técnicas disponibles para las aplicaciones de cada uno de esos tipos. Como se ha indicado anteriormente, la viabilidad económica y técnica es un factor importante en tal evaluación.

Desafíos en materia jurídica

Analizar la participación y los modelos de aplicación de las APD

Las autoridades de protección de datos (APD) deben participar en este proceso de identificación y enumeración de BTD en materia de intimidad y seguridad. Debe determinarse el modo en que las APD pueden y deben imponer el uso de las BTD, sobre todo si se dispone de tecnologías pero éstas no forman parte de sistemas convencionales (por ejemplo, el borrado seguro mediante herramientas de borrado que no forman parte de los sistemas operativos convencionales) o si su uso precisa la cooperación de varias partes o una infraestructura adicional (por ejemplo, los sistemas de «anonimización» que protegen los datos personales antes de que éstos sean perceptibles para un responsable del tratamiento concreto no los podrá gestionar el propio responsable del tratamiento sino que precisarán la participación de proveedores independientes adicionales).

Anticiparse a las futuras combinaciones tecnológicas

Nótese que las soluciones habrán de tener en cuenta los riesgos que genere la combinación de varias tecnologías existentes, es decir, habrá que anticiparse a tales riesgos, analizarlos y cuantificarlos. Por ejemplo, la combinación de las técnicas biométricas de reconocimiento facial con herramientas de videovigilancia o con servicios basados en la localización dotados de información cartográfica genera importantes riesgos. Al definir una política sobre un tecnología específica, habría que prever, pues, en la medida de lo posible, sus futuros usos, de manera que se puedan incluir garantías de limitación de la finalidad adecuadas en la fase de diseño.

Desafíos en materia de comunicación

Un proceso público

La lista de BTD identificadas en relación con ámbitos de aplicación importantes y sus características debe hacerse pública, de manera que puedan conocerla todos los responsables y encargados del tratamiento de datos. También las buenas prácticas podrían ilustrar el uso de las BTD.

Enlaces

Las BTD se definieron de manera satisfactoria, en el marco medioambiental, en la Directiva 96/61/CE «IPPC»[18].

La BSI (*Bundesamt für Sicherheit in der Informationstechnik*: Oficina Federal de Seguridad de la Información de Alemania) inició recientemente un proyecto que podría constituir un ejemplo ilustrativo de BTD para aplicaciones RFID[19].

4.9 Incentivos y sanciones eficaces

Es frecuente que se incumpla la legislación sobre protección de la intimidad

La legislación de protección de datos tiene raíces profundas. Sin embargo, en el mundo actual del tratamiento de datos se observa un frecuente incumplimiento de esa legislación por parte de los componentes TIC y de las estructuras organizativas. Se ha podido comprobar, a lo largo de las últimas décadas, que, cuando se basan únicamente en las fuerzas del libre mercado, las tecnologías de fomento de la protección de la intimidad apenas evolucionan.

Lagunas concretas

Falta motivación y no se ofrecen incentivos suficientes

La falta de motivación adecuada de los responsables del tratamiento de datos para cumplir la legislación sobre protección de datos constituye una laguna de carácter general. Muy relacionada con esta laguna está también la falta de motivación para emplear tecnologías de fomento de la protección de la intimidad que puedan estimular la evolución tecnológica.

La falta de herramientas dificulta el control del cumplimiento por parte de las APD

En general, sólo pueden imponerse sanciones por incumplimiento si llega a conocimiento de la autoridad de supervisión responsable o de un tribunal la infracción correspondiente. Actualmente las autoridades de protección de datos sólo verifican la actuación de una pequeña fracción de los responsables del tratamiento de datos, por lo que los incumplimientos de la normativa pasan, con frecuencia, desapercibidos.

La escala actual de las sanciones no ofrece incentivos suficientes para cumplir la ley

Habida cuenta de la escasa entidad de buena parte de las sanciones, los incentivos económicos para cumplir la normativa de protección de la intimidad son, a menudo, mínimos. Por ejemplo, los responsables del tratamiento de datos,

[18] Véase http://ec.europa.eu/environment/air/legis.htm#stationary.
[19] Véase http://www.bsi.de/presse/pressinf/071207_RFID.htm.

en determinadas jurisdicciones, sólo pueden ser multados una vez, por lo que no se repite la multa aunque no modifiquen sus procesos de tratamiento de datos. En diversos casos, los tribunales han invalidado la obligación de pago de la multa para no tener que examinar las denuncias por discriminación presentadas contra todos los competidores del responsable del tratamiento de datos condenado.

Soluciones propuestas

Fomentar el cumplimiento mediante recompensas o castigos

Para fomentar la protección de la intimidad de las personas por parte de los responsables del tratamiento de datos caben dos soluciones generales:

1. Ofrecer *incentivos* que recompensen al responsable del tratamiento de datos
2. Imponer *sanciones* que castiguen al responsable del tratamiento de datos

Unas sanciones eficaces serán distintas según se trate de entidades privadas o públicas

Qué puede representar un incentivo o una sanción dependerá del tipo de responsable del tratamiento de datos. Por ejemplo, lo que más importa a las empresas son los factores económicos. Esto significa que una multa impuesta por incumplimiento de la legislación de protección de datos debe de hacer mella en una empresa: no deben resultar rentables las conductas infractoras. En el caso de los órganos de la Administración pública, el tratamiento *debe* cumplir la legislación de protección de datos; de otro modo los órganos supervisores reglamentarios deben intervenir de inmediato.

Desafíos en materia de I+D

Se necesitan herramientas de auditoría normalizadas para comprobar eficazmente el cumplimiento de la ley

La falta de herramientas de auditoría automatizadas reduce al mínimo el cumplimiento de la legislación. Tales herramientas requerirían cierto proceso de normalización y certificación que identificara, en colaboración con las autoridades de protección de datos, el conjunto de informaciones necesario para trazar el historial de auditoría.

Desafíos en materia jurídica

Certificación obligatoria o uso de tecnologías de protección de la intimidad

Las condiciones de contratación de los servicios públicos podrían exigir el cumplimiento de la legislación de protección de la intimidad desde la fase de diseño, o bien la presentación de una certificación o una autocertificación. Ciertas medidas tecnológicas podrían considerarse obligatorias, puesto que ya lo son en determinadas jurisdicciones; ha de determinarse aún, no obstante, cuáles serían beneficiosas.

Unas sanciones económicas eficaces y perceptibles

Unas sanciones eficaces contribuirían a convencer a los responsables del tratamiento de datos de la conveniencia de aplicar sistemas que respeten las normas de protección de la intimidad. Las sanciones no deben ser únicamente administrativas (en algunos países, pueden ser también penales), sino que han de incluir, además, un sistema de responsabilidad eficaz. En este caso, las organizaciones de consumidores podrían desempeñar una función importante.

Sin embargo, en numerosos Estados miembros el régimen sancionador no funciona de manera eficaz. Este régimen debe basarse en un sistema de auditoría eficiente. Por otra parte, también deben ofrecerse incentivos. Éstos pueden ser, por ejemplo, de carácter fiscal, lo que requiere un régimen de certificación y está estrechamente vinculado a éste.

Recomendamos que la Comisión Europea y los Estados miembros fomenten un sistema de incentivos vinculado a un régimen de certificación y a un sistema eficaz de sanciones económicas.

Desafíos en materia de comunicación

Campañas para fomentar la exigencia del consumidor en cuanto al cumplimiento de la normativa

El cumplimiento de la normativa de protección de la intimidad o el diseño (contrastado) basado en criterios de fomento de esa protección pueden constituir una propuesta comercial única para un responsable del tratamiento de datos. Además favorecerían la adquisición de una buena reputación capaz de atraer y vincular a los clientes. Las campañas de sensibilización respecto a la protección de la intimidad podrían crear una demanda de mercado de sistemas que cumplan la normativa en la materia, máxime si existen métodos accesibles para que los clientes expresen sus exigencias al respecto. Cuantos menos datos personales, menos riesgos de abuso, lo que también es positivo para la reputación del responsable del tratamiento de datos.

Explicar las ventajas de los datos anónimos

Se podría convencer a los responsables del tratamiento de datos de que una organización que fomente la protección de la intimidad en el tratamiento de datos, sobre todo si se adecua a los principios de la minimización de datos, resulta a menudo más barata que la dotación no sólo de medios de almacenamiento sino, asimismo, de unas garantías adecuadas, de la correspondiente documentación y del acceso al interesado (o a las autoridades policiales).

Enlaces

Ross Anderson mantiene una página sobre economía y recursos de seguridad (*Economics and Security Resource*) en su sitio web.[20] Alessandro Acquisti ofrece un sitio similar dedicado a las cuestiones económicas de la intimidad[21].

4.10 «Ser o no ser» datos personales

El concepto de datos personales comprende toda la información que se pueda relacionar con una persona

Con arreglo a la Directiva 1995/46/CE, se entiende por datos personales toda información sobre una persona física (el «interesado») identificada o identificable. Este concepto es muy amplio, hasta el punto de que comprende toda la información que se pueda relacionar con una persona. De hecho, es posible combinar múltiples datos distintos que pueden contribuir a la

[20] Véase http://www.cl.cam.ac.uk/~rja14/econsec.html.
[21] Véase http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.

identificación de una persona concreta (por ejemplo, observando las redes sociales, controlando las etiquetas RFID, combinando las consultas efectuadas en los motores de búsqueda, etc.). Ahora bien, aunque los legisladores europeos han adoptado un concepto de datos personales amplio, éste no carece de límites. El ámbito de aplicación de las normas de protección no debe ampliarse en exceso, si bien ha de evitarse también la restricción indebida del concepto de datos personales. Dado el carácter difuso que tiene en ocasiones la frontera entre los datos personales y no personales, se han emprendido iniciativas al respecto, en las que se enmarca el dictamen del Grupo del artículo 29 sobre el concepto de datos personales.

Lagunas concretas

No siempre está claro si ciertos datos son personales o no

Pese a la reciente iniciativa del Grupo de trabajo del artículo 29 para aclarar el concepto de datos personales, con frecuencia se sigue discutiendo éste. Surge aquí un problema: cuando no está previsto que un dato se convierta en personal, no tienen por qué ofrecerse las suficientes garantías para asegurar que no lo haga.

Ejemplo: Las etiquetas RFID de los comercios minoristas no se desactivan aunque no tengan finalidad alguna fuera del punto de venta

Por otra parte, lo que constituye una intrusión aceptable en la intimidad personal y la percepción de los datos personales por parte del usuario son conceptos dinámicos. Por ejemplo, actualmente se usa la tecnología RFID en múltiples aplicaciones (como el comercio minorista, la identidad digital en pasaportes, las llaves de coche, el pago mediante teléfono móvil, etc.). Esta tecnología presenta numerosas amenazas, ya que puede permitir al usuario controlar y recoger datos posiblemente cualquier lugar sin que el interesado se percatase de ello. Puede, por ejemplo, identificar a una persona física en caso de que la etiqueta en cuestión contenga datos como su nombre o sus datos biométricos. Permite seguir y rastrear a una persona y elaborar un perfil de ella a través de los artículos etiquetados que posea, los cuales contienen números únicos. En el comercio minorista, puesto que los datos contenidos en una etiqueta no se consideran personales cuando ésta se emplea con fines logísticos, no es habitual desactivarla en el punto de venta, con lo que a partir de ese momento el usuario pasa a llevar consigo artículos cuyas etiquetas activas permitirían localizarlo.

Además, lo que constituye una intrusión aceptable en la intimidad personal y la percepción e los datos personales por parte del usuario son conceptos dinámicos que evolucionan conforme a factores sociales, a las expectativas en materia de seguridad y a los adelantos tecnológicos. Los factores sociales dependen de las reacciones personales ante las tecnologías invasoras de la intimidad, ya que la definición de la esfera privada de cada cual es subjetiva y depende de la edad, la cultura y el entorno de la persona. Las expectativas en materia de seguridad también difieren, ya que, mientras que los usuarios expertos quizá traten de configurar sus sistemas con precisión, es probable que la mayoría prefiera unos ajustes por defecto sencillos, comprensibles y respetuosos de la normativa de protección de la intimidad. Por último, los datos que hoy no se considerarían personales (dados los recursos excesivos que se necesitarían para

personalizarlos) pueden convertirse en personales si la evolución tecnológica reduce tales recursos a unos niveles razonables.

Soluciones propuestas

Desafíos en materia de I+D

Desarrollar unas garantías tecnologías adecuadas, incluso en relación con los datos que no está previsto que se conviertan en personales

Para evaluar los riesgos para la intimidad relacionados con el tratamiento de datos deben desarrollarse y aplicarse metodologías de evaluación del impacto en la intimidad. La complejidad del análisis que se lleve a cabo debe depender de la sensibilidad del tratamiento y de los datos en cuestión.

Deben desarrollarse las oportunas garantías para proteger adecuadamente los datos de las personas, sean éstos de carácter personal o no. Con ello se mejorarán significativamente la capacitación y el control del usuario.

Debe preverse adecuadamente la evolución de los medios tecnológicos al diseñar sistemas y definir normativas, de manera que los datos que no se consideren personales no se conviertan en tales al evolucionar la tecnología.

El impacto social de las nuevas tecnologías debe evaluarse sistemática y científicamente; asimismo, ha de demostrarse su utilidad.

Desafíos en materia jurídica

La reglamentación debe garantizar que los datos no personales no se conviertan en tales

La reglamentación debe garantizar una protección adecuada de los datos, máxime si existe (o existirá) incertidumbre sobre la posibilidad de que se conviertan en personales.

Sin embargo, a modo de ejercicio del derecho a la intimidad y el derecho a la protección de los datos, debe hallarse un equilibrio continuo entre el derecho al anonimato y los demás derechos fundamentales. Puesto que no suele ser posible un anonimato absoluto, debe dejarse un margen para formas de anonimato «razonable».

Sobre todo en relación con datos sensibles deben emplearse, siempre que sea posible, sistemas de «anonimización» adecuados.

Una vez que la ley haya establecido un derecho, equilibrándolo con otros, la tecnología debe desarrollar las correspondientes normas. La eficacia del derecho al anonimato debe garantizarse mediante la tecnología y ésta ha de establecer la protección de diversos grados de anonimato.

Podría incorporarse a la legislación la obligación de realizar evaluaciones de impacto sobre la intimidad.

En los casos que tales evaluaciones revelen la existencia un riesgo importante para la intimidad asociado al tratamiento de los datos, el legislador podría imponer las garantías pertinentes para mitigarlo.

Desafíos en materia de comunicación

Al mejorar la comprensión de las tecnologías de capacitación del usuario y de la necesidad de proteger los datos personales, las campañas de sensibilización mejorarán las prácticas del usuario y contribuirán así a mitigar los riesgos a los que se enfrentan los ciudadanos de la UE en el mundo en línea.

La sensibilización mitigará los riesgos a los que se enfrentan los ciudadanos de la UE en el mundo en línea

Mediante uso sistemático de metodologías y procesos de evaluación del impacto sobre la intimidad armonizados, la industria mejorará la transparencia y mitigará los riesgos de seguridad vinculados a los datos que trate, beneficiándose así de un aumento de la confianza en la tecnología por parte de los usuarios.

Estas campañas crearán asimismo la necesidad de la opinión pública de contar con unas tecnologías de fomento de la intimidad comprensibles y eficaces.

Enlaces

La Directiva 1995/46/CE[22] define los datos personales y el marco legislativo aplicable.

El concepto de datos personales se aclaró y analizó detalladamente en 2007 en el dictamen del Grupo de trabajo del artículo 29[23].

4.11 Protección de la intimidad y clasificación social

En muchos casos, los responsables del tratamiento de datos no pretenden identificar de manera unívoca a las personas —es decir, obtener datos personales—, sino que el tratamiento se concentra en grupos poblacionales y persigue alguna categorización, es decir, alguna ordenación, estratificación, segmentación o clasificación social. Esta categorización puede realizarse mediante técnicas de elaboración de perfiles o de calificación para fines tan variados como el marketing, la determinación de la solvencia crediticia, la discriminación de precios o la toma de decisiones en procesos de contratación electrónica (*e-recruitment*), así como en el sector sanitario o en las investigaciones penales. En estos casos, es frecuente que los propios datos no se consideren personales, ya que no se refiere a personas concretas: los responsables de su tratamiento no conocen el nombre de las personas cuyos datos se están tratando. Sin embargo, las consecuencias de esta recogida y análisis de datos afectan con frecuencia a las personas y, por ende, a su intimidad. Las disposiciones del artículo 15 de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales sobre las decisiones individuales automatizadas no están concebidas para comprender esta concatenación de circunstancias.

La clasificación social puede vulnerar la intimidad de las personas aunque los datos tratados no sean personales

[22] http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.
[23] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

Lagunas concretas

No existe transparencia en la clasificación social de las personas

La principal laguna consiste en que, a menudo, las personas no saben cuándo se les está sometiendo a un proceso de clasificación social ni cómo se adoptan las decisiones concretas que les afectan. Eso significa que no saben si los datos en los que se basa la clasificación social son correctos ni si los algoritmos y aplicaciones de calificación, o las demás herramientas de análisis, funcionan adecuadamente. En particular, la entidad que genera las decisiones que se adoptan en relación con las personas puede no ser la misma que recoge y compendia la información, lo que dificulta que los afectados puedan interponer reclamaciones y lograr una reparación. Además, al tratarse de hipótesis predictivas, la persona no suele poder demostrar que determinado pronóstico es erróneo.

El ejercicio del derecho a la intimidad individual no funciona al tratarse de datos que no son personales

El hecho de que los datos tratados no se consideren personales menoscabará la posibilidad de ejercicio del derecho a la intimidad (acceso, rectificación, supresión de datos si se almacenan ilegalmente, revocación de autorización). Para ello habría que demostrar que los datos en cuestión pertenecen de manera única a uno mismo como persona. Hay casos, por ejemplo, en los que se ha denegado el derecho de acceso al tratarse de datos en relación con *cookies*, ya que éstas no están necesariamente ligadas, de manera única, a una persona. Queda así de manifiesto que son muchos los identificadores que tienen una capacidad de vinculación suficiente para ofrecer a la entidad que trate los datos la información deseada, mientras que no permiten a las personas afectadas ejercer su derecho a la intimidad.

La accesibilidad puede facilitar la manipulación directa

Además, en determinados entornos es posible dirigirse y acceder a las personas, por ejemplo, mediante una llamada telefónica, un correo electrónico o un anuncio personalizado por televisión o a través de un sitio web. En concreto, todos los tipos de marketing que pretenden seducir a clientes potenciales pueden ser manipuladores y vulnerar la intimidad de la persona. También pueden provocar una reacción que permita a la entidad responsable del tratamiento depurar los datos recogidos o establecer una vinculación personal.

Soluciones propuestas

El derecho a la autodeterminación en materia de información sólo podrá ejercerse de manera íntegra si las personas pueden conocer todo lo que concierne al tratamiento de los datos referidos a ellas.

Desafíos en materia de I+D

Historial del auditoría completo de todo el tratamiento de datos

Una posible solución consistiría en elaborar un marco organizativo y técnico que garantizase que las personas afectadas puedan protegerse y ejercer sus derechos. Para ello podría requerirse la preparación de un historial de auditoría completo siempre que vayan a tratarse datos —sean personales o no— con posible perjuicio para las personas. Cada fase del tratamiento de datos, con todos los flujos de información entrante y saliente, incluida la relativa a las partes

responsables de los datos, los algoritmos y las aplicaciones, debería ofrecerse de manera transparente a las personas afectadas o a las personas en que éstas confíen. De este modo, los datos incorrectos o los errores en su tratamiento podrían identificarse y corregirse más fácilmente.

El marco organizativo y técnico resulta tanto más necesario si se considera cómo será el mundo futuro, caracterizado por la presencia de toda suerte de sensores que se comunicarán entre sí y recogerán información sobre su entorno, incluidas las personas. En este caso, las tecnologías que potencien la transparencia podrían brindar a apoyo a las personas afectadas [Hildebrandt/Koops 2007].

Desafíos en materia jurídica

Un marco jurídico coherente para todos los tratamientos de datos que afecten a las personas

La legislación en vigor relativa a esta laguna parece hallarse dispersa: se reparte entre la normativa sobre protección de datos y la normativa sobre lucha contra la discriminación, e incluso aspectos que parecen no tratarse plenamente. Por ello, el principal desafío jurídico consiste en la elaboración de un marco jurídico coherente y completo para todos los tipos de tratamientos de datos, personales y no personales, que puedan afectar a las personas. Este marco debe contener, especialmente, la obligación de mejorar la transparencia y la comprensibilidad del tratamiento de los datos para las personas afectadas.

Desafíos en materia de comunicación

Informar a las personas sobre la recogida y el análisis de datos

Las personas deben saber cuándo están dejando, sin ser conscientes de ello, rastros de datos, qué información sobre ellas están recogiendo y relacionando diversas partes o cuándo se les está considerando —acaso de manera errónea— responsables de acciones concretas. Además, se les debe informar sobre cómo reaccionar mejor si se sienten tratadas de un modo injusto en lo que concierne a su intimidad.

Enlaces

Hildebrandt, Mireille, Serge Gutwirth (editores): D7.4: *Implications of profiling practices on democracy and rule of law*, *FIDIS Deliverable*, Fráncfort del Meno, Alemania, septiembre de 2005, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.4.implication_profiling_practices.pdf

Hildebrandt, Mireille, Bert-Jaap Koops (directores de edición): D7.9: *A Vision of Ambient Law*, *FIDIS Deliverable*, Fráncfort del Meno, Alemania, octubre de 2007, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf

Lessig, Lawrence: *Code and other laws of cyberspace*, Basic Books, Nueva York, 1999

Lyon, David: *Surveillance as Social Sorting*: *Privacy, Risk and Automated Discrimination*, Routledge, 2002

Phillips, David J.: *Privacy policy and PETs – The influence of policy regimes on the development and social implications of privacy enhancing technologies*, en: New Media & Society, Vol. 6, No. 6, SAGE Publications, Londres, Thousand Oaks, CA y Nueva Delhi, 2004, pp. 691-706

Grupo de trabajo del artículo 29: Dictamen 4/2007 sobre el concepto de datos personales, 20 de junio de 2007, 01248/07/ES, WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf

4.12 Intimidad, protección de datos y espacio

La falta de fronteras del ámbito digital

La intimidad territorial desempeña desde hace tiempo una función importante en la protección de la intimidad («mi hogar es mi castillo»). Un territorio suele ser un continuo en el espacio; los elementos reales y digitales de una persona, sin embargo, pueden coexistir en localizaciones diversas (en último extremo, todo elemento digital se graba en un disco duro u otro medio que tiene una sustancia y una localización concretas, aunque la última puede cambiar con el tiempo, por ejemplo, si el dispositivo es móvil). Esta ausencia de fronteras territoriales claras en el mundo digital genera problemas jurídicos concretos y problemas generales de percepción al gestionar la intimidad personal.

Lagunas concretas

La necesidad de mantener los datos personales de los ciudadanos dentro de la jurisdicción de Europa

Con arreglo al artículo 25 de la Directiva 1995/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, éstos sólo se podrán transferir a un tercer país cuando éste garantice un nivel de protección adecuado. Existen excepciones a esta norma tales como la transferencia a empresas de los Estados Unidos, que se atienen a los principios de puerto seguro.

Sin embargo, en todos los casos situados fuera de la jurisdicción de Europa, el nivel de protección de la intimidad adecuado definido no tiene en cuenta la posibilidad de acceso por las agencias de seguridad nacionales. Esto significa que todos los datos en tales países pueden ser objeto de acceso y análisis por tales agencias, lo que puede tener consecuencias no deseadas para las personas y las organizaciones, a saber, para las empresas cuyos secretos comerciales pueden verse expuestos.

Físico frente a digital

Existe en la sociedad de la información cierta falta de territorialidad y, por tanto, de fronteras de protección. Al mismo tiempo, existe una multiplicidad de puentes invisibles e incontrolados entre los entornos real y digital. Aunque seguimos disponiendo de las herramientas en el mundo físico para gestionar nuestra intimidad (a distancia), no sucede así en el caso del mundo digital, pese a que este nuevo entorno se está convirtiendo, a través de la existencia de un número creciente de puentes, en una parte inherente al espacio vital de nuestra vida cotidiana.

Las normas jurídicas, las normas socioculturales tácitas e incluso las tradiciones constituyen las directrices para la comprensión por las personas de lo que constituye un espacio privado o público o de lo que se acepta socialmente como espacio privado o público. Aunque la distinción entre ambos espacios no está siempre muy clara, las personas saben que existen fronteras y obran en consecuencia (por ejemplo, una finca privada vallada, el cartel de «no pasar» en el césped de un vecino, la mirada inquisitiva o enojada que se dirige a los forasteros en un bar de barrio).

Percepción del espacio en el ciberespacio

Aunque las personas tienen un sentido intuitivo de lo que constituye una vulneración de su intimidad en el espacio físico, no tienen tal sentido en el caso del ciberespacio. Por ejemplo, incluso en espacios públicos, si alguien escucha a escondidas, está claro que está vulnerando la intimidad. En el ciberespacio no está claro si alguien está escuchando a escondidas, ni si ello constituye una vulneración de la intimidad. ¿Cómo se pueden hacer más explícitas tales fronteras en el ciberespacio?

El almacenamiento remoto complica la noción de frontera espacial en el ciberespacio

En este contexto, y sin subestimar la naturaleza ya compleja de la intimidad en el espacio físico y la dificultad de protegerla adecuadamente, parece que, en el espacio digital, la intimidad es mucho más fácil de vulnerar y mucho más difícil de proteger, ya que para ello no basta con hacer caso omiso de un contacto no deseado. Además, la situación de partida en el ciberespacio invade, con mayor probabilidad, la intimidad del usuario y requiere, pues, la acción adecuada de éste. Considérese, por ejemplo, la situación en virtud de la cual, al instalar un programa o registrarse en un servicio de Internet en línea, uno queda automáticamente suscrito a boletines periódicos o servicios y recibe información, a continuación, de que para cancelar la suscripción debe dirigirse al sitio web correspondiente. Considérese asimismo un álbum de fotos que conservamos en un armario del salón y que, supuestamente, sólo podrán ver los familiares y amigos a quienes les permitamos hacerlo; en cambio, ese mismo colocado en Internet en el que, incluso, se pueden hacer búsquedas no estará por lo general protegido del mismo modo[24].

La posibilidad de autoexclusión de estos tipos de aplicaciones es, pues, en la mayoría de los casos, más complicada y requiere más esfuerzo por parte del usuario, aparte de conocimientos técnicos. Para empeorar la situación, el usuario desconoce con frecuencia la cantidad y el tipo de información (a saber, dirección IP, *cookies*, seguimiento de web, caché, términos de búsqueda, etc.) que se capta mientras navega por la red o lleva a cabo otras actividades en línea, lo que dificulta aún más la autoexclusión o la protección de la intimidad.

[24] Las aplicaciones de «redes sociales» tales como mySpace.com, Flickr, YouTube o Facebook permiten almacenar, clasificar, compartir y, sobre todo, buscar fotografías y vídeos.

Mundos virtuales

Los denominados mundos virtuales constituyen otra manifestación de esta falta de claridad. Según ciertos pronósticos, las empresas convencionales comenzarán a utilizarlos en breve. Están apareciendo aplicaciones como Kaneva, en las que convergen las redes sociales y los mundos virtuales. Son muchas las cuestiones referidas a la intimidad que no se han explorado aún en este ámbito. Por ejemplo, ¿cuál es el estatuto jurídico de los datos financieros virtuales (por ejemplo, de las cuentas denominadas en dólares Linden)? Otra cuestión interesante es la relativa a la procedencia de la expedición de un documento de identidad para un avatar, con la justificación de que incluso las personas puramente digitales pueden beneficiarse de una autenticación rigurosa combinada con un control de la vinculabilidad. El avatar como metáfora de una identidad digital parcial puede ser también una herramienta de interfaz de usuario de utilidad en lo que respecta a la intimidad.

Soluciones propuestas

Desafíos en materia de I+D

Almacenamiento e infraestructura dentro de la jurisdicción de la UE

Para proteger los datos personales de los ciudadanos europeos deben aplicarse mecanismos que los mantengan dentro de la jurisdicción europea siempre que sea posible. En cuanto a los motores de búsqueda, eso podría lograrse mediante la oferta de *proxies* para los servicios extraeuropeos o bien a través de la oferta de motores de búsqueda separados.

Del mismo modo, las infraestructuras críticas deben ejecutar sus actividades exclusivamente dentro de la jurisdicción europea, para evitar dependencias de otros países.

Desafíos en materia jurídica

La gestión de datos en estos servicios europeos debe ceñirse a la legislación europea sobre protección de datos, lo que evitaría un almacenamiento y un uso innecesarios.

Concepto de territorio digital

Al digitalizar el ámbito personal y, asimismo, sus fronteras, el concepto de territorio digital brinda la oportunidad de introducir la noción de territorio, propiedad y espacio en un entorno digital. El objetivo consiste en proporcionar una herramienta que permita a los usuarios gestionar la proximidad y la distancia con respecto al prójimo en este futuro espacio de inteligencia ambiental, tanto en el sentido jurídico como en el social, tal como hacemos actualmente en el mundo físico.

El concepto físico y tradicional de residencia constituye un santuario jurídico y protege al ciudadano frente a interferencias del exterior o a medidas invasivas[25]. Este santuario jurídico debe extenderse ahora a la parte digital de nuestro espacio privado.

[25] Véanse los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Desafíos en materia de comunicación

Tendrán que desarrollarse herramientas de comunicación para expresar qué elementos corresponden a estos territorios personales.

Enlaces

Beslay, Laurent, Hannu Hakala: *Digital Territory*: *Bubbles*. En: Paul T. Kidd (editor): *European Visions for the Knowledge Age*: *A Quest for New Horizons in the Information Society*, Cheshire Henbury, 2007, pp. 69-78.

Benoliel, Daniel: *Law, Geography, and Cyberspace*: *The Case of online Territorial Privacy*, CFP 2004[26]

Daskala, Barbara, Ioannis Maghiros: *Digital Territories, Towards the protection of public and private space in a digital and Ambient Intelligence environment*[27]

[26] Véase http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf.
[27] Véase http://ftp.jrc.es/eur22765en.pdf.