
**RED ACADÉMICA INTERNACIONAL DE
PROTECCIÓN DE DATOS PERSONALES**

Revista Internacional de Protección de Datos Personales

RIPDP

**ASECHO DEL DERECHO A LA PRIVACIDAD
EN AMÉRICA LATINA**

ANTONIO ANSELMO MARTINO

Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia)
No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705

Asecho del derecho a la privacidad en América Latina

Antonio Anselmo Martino*

“La igualdad es una necesidad vital del alma humana. La misma cantidad de respeto y de atención se debe a todo ser humano, porque el respeto no tiene grados.”

SIMON WEIL

RESUMEN

La tensión entre dos valores: “seguridad vs. privacidad”, parece inclinarse a favor de la primera por un defectuoso sentido de la noción de soberanía que se refuerza en la vigencia de Internet. Vivimos tiempos de grandes y veloces cambios en la era de la digitalización e Internet. La mayor parte está concentrada en el hemisferio norte y la brecha tecnológica afecta a América Latina. La tradición de gobiernos fuertes alimenta la teoría de la soberanía que termina justificando violaciones y atropellos a los derechos de privacidad. Contamos una historia basada en un libro de ciencia ficción pero que podría ser realidad con consecuencias inesperadas para el dilema seguridad-privacidad. Enunciamos buenas prácticas para defendernos de los asechos.

ABSTRACT

The tension between two values: “security vs. privacy” seems to lean in favor of the first by a defective sense of the notion of sovereignty that is reinforced in the life of the Internet. These are times of great and rapid changes in the age of digitization and the Internet. Most are concentrated in the northern hemisphere and the technology gap affecting Latin America. The tradition of strong government feeds the theory of sovereignty that ends justifying violations and abuses of the rights of privacy. We have a story based on a book of science fiction but it could be reality with unexpected consequences for the security dilemma privacy. Enunciate best practices to defend the stalking.

* Abogado por la Universidad de Buenos Aires. Doctor en Derecho y Ciencias Sociales por la Universidad de Buenos Aires. Profesor emérito de la Universidad del Salvador. Profesor Emérito de la Universidad de Pisa. Miembro de la Academia Nacional de Derecho y Ciencias Sociales de Córdoba (Argentina). Miembro asociado del Center for Artificial Intelligence and Cognate learning of the University of Greenwich. Miembro de la European Association of Legislation. Miembro del Instituto de Derecho Constitucional de la Academia de Derecho y Ciencias Sociales de Buenos Aires. Director del Manual del Digesto Argentino. Miembro del Consejo Científico de las revistas: *Computer/Law Series*, Amsterdam; *Artificial Intelligence and Law*, Boston; *Law and Information Technology*, Oxford; *Derecho de la alta tecnología*, Buenos Aires; *Legisprudencia*, *International Journal of the study of legislation*, London; *Derecho del ciberespacio*, revista de derecho informático y de la sociedad de la información, Madrid. Correo: aamartino@gmail.com

PALABRAS CLAVE: Gobierno electrónico, brecha tecnológica, soberanía, transparencia, privacidad.

KEYWORDS: E-government, technology divide, sovereignty, transparency, privacy.

SUMARIO

Introducción - I. EL RESURGIMIENTO DE LA NOCIÓN DE SOBERANÍA - A. *Una historia* - II. CONCLUSIONES - Bibliografía.

Introducción

Vivimos un momento de transición profunda entre una sociedad de corte industrial y otra marcada por el procesamiento de la informática y las telecomunicaciones; el uso de la información afecta de manera directa e indirecta todos los ámbitos de la sociedad y les imprime su sello de indiferencia entre los ricos y los pobres. El aprovechamiento de la información propicia la mejoría de los niveles de bienestar y permite aumentar la productividad y la competitividad de las naciones. El mundo de hoy está inmerso en una nueva revolución tecnológica basada en la informática, que encuentra su principal impulso en el acceso y en la capacidad de procesamiento de información sobre todos los temas y sectores de la actividad humana. Ha contribuido a que culturas y sociedades se transformen de forma acelerada tanto económica como social y políticamente. Pero esto no ha sido uniforme y sin costos. Hay una brecha tecnológica que aqueja a zonas como América Latina, y precios que se están pagando por la crisis económica mundial y la crisis política, aun en países muy desarrollados. Hay también una brecha económica que se amplía: “Se estima que los activos de los ricos van a seguir aumentando anualmente entre un 4% y un 5% en los próximos cinco años para llegar hasta los 150 000 millones de dólares para finales del 2016. En relación al número de habitantes, Singapur, Catar y Austria albergan el mayor número de fortunas superiores a los 100 millones de dólares del planeta.”¹

Además, por tradiciones políticas, cuando se quiere imponer alguna medida impopular o que afecta directamente la libertad “*lato sensu*” de los ciudadanos se invoca la noción de soberanía.

Es decir, a la diatriba “transparencia vs. privacidad” se agrega esta condición particular de las nuevas tecnologías que, siendo un medio, pueden ser usadas para inclinar la balanza hacia una u otra parte, y en Latinoamérica el uso indebido de la noción de soberanía la inclina hacia la primera parte del dilema.

Ya, la existencia de Internet afecta a la soberanía, pues es difícil establecer barreras. Pero, hilando más fino, la noción de soberanía se usa muchas veces para soslayar sustanciales derechos de libertad y, en particular, la privacidad. Es de estos días una sentencia de un tribunal de apelaciones norteamericano declarando que es importante que se mantengan en secreto los acuerdos entre la NSA y Google² en materia de

² A EPIC le interesan los detalles del ataque masivo contra las cuentas de Gmail de varios activistas y disidentes chinos que tuvo lugar en enero de 2010. El grupo apeló a la Ley de Libertad de Información, insistiendo en que el público tiene el derecho a conocer si en este caso los ciudadanos podrían ser espiados. No obstante, no ha habido ‘milagro’ de la democracia y el Tribunal de Apelaciones norteamericano ha dictado que para prevenir posibles ciberataques, la NSA no debe revelar ningún acuerdo que tenga con el gigante informático.

Esta decisión reafirma la sentencia de una corte menor que afirmaba que la Agencia no necesitaba negar o confirmar ninguna relación con Google. El presidente del Partido Pirata de Madrid, Daniel Riaño, cree que el veredicto judicial sería un golpe a la privacidad de los usuarios del buscador.

“Toda la noticia está envuelta en tal misterio que no se puede saber nada. Lo que sí que sabemos es que tradicionalmente ese tipo de agencias han abusado del secreto simplemente para no dar ninguna información en cosas que les eran no convenientes para ellos, pero que en ningún momento ponían en peligro la seguridad de sus países ni la seguridad de otras personas. Los términos en los que se ha pronunciado este tribunal hoy podrían permitir que la relación entre la NSA y Google pusiera en riesgo la privacidad de todos los usuarios de Google. En la actualidad no sabemos qué tipo de colaboración tiene Google y la NSA. Lo malo de esta sentencia es que permite que esta relación se vaya haciendo cada vez más intensa y más estrecha sin

¹ BOSTON CONSULTING GROUP, junio del 2012.

vigilancia sobre cuentas. En el mes de julio de este año tuvo lugar en Dubái la Reunión Internacional de las Telecomunicaciones, que es el ámbito dentro del cual Internet está incluida en toda la telecomunicación. Existe un grupo de países y de intereses que quisieran sacar a Internet de la ICANN y hacerla regular por una comisión de Naciones Unidas. ICANN es un ámbito tecnológico donde están representados no solo los países sino también los productores de hardware, de software y los consumidores. El peligro de llevar a Internet a una sección de Naciones Unidas daría más espacio a los representantes nacionales y mucho menos a los específicamente técnicos, con la consiguiente pérdida de la independencia obtenida hasta el momento. Afortunadamente no se ha conseguido consenso al respecto pero el peligro existe.³

En los países latinoamericanos esta noción de soberanía se está empleando, sea para defensa de materias consideradas estratégicas, sea para la información.

I. EL RESURGIMIENTO DE LA NOCIÓN DE SOBERANÍA

La dependencia cada vez mayor del gobierno electrónico y de Internet es un hecho. Pero no tiene un avance parejo en razón de los distintos grados de desarrollo e implementación de sistemas de redes. Por ejemplo, la penetración

que ni el Gobierno de EE. UU., ni los ciudadanos de EE. UU., ni el resto de los usuarios de Google tenga jamás noticia ni siquiera de si está habiendo una colaboración entre Google y las agencias de espionaje norteamericanas.”

3 Ver la carta preocupada de Vincet Cerf en <http://www.itu.int/en/wcit-12/Pages/default.aspx>

de Internet en los diferentes países es motivo de reflexión. Y esta reflexión pasa también por el modo como se pueden usar estos medios tecnológicos para avasallar derechos humanos aun en los sistemas democráticos.



Mucho tienen que ver los derechos humanos con la democracia. Y en particular con la condición primera de la democracia que es el Estado de derecho. Sin Estado de derecho nadie puede garantizar la existencia plena de los derechos humanos y esta lucha está lejos de haber sido dirimida.

Finalmente, cuando todos esos derechos están asegurados o por lo menos reconocidos, aparecen otros más refinados que tienen que ver con la condición humana y la posibilidad de expresarse y realizarse: el derecho a la privacidad. Hablamos groseramente de privacidad porque

4 Las imágenes que reproducimos en este *post* muestran que los usuarios “activos” de la Web —más exactamente la cantidad de conexiones o direcciones IP— se concentran en la parte superior del mapa: en Norteamérica, donde se encuentra el 56% de los usuarios; y luego en Europa, donde reside otro 22%. En tercer lugar se encuentra Asia, con el 14% de los usuarios; y luego América del Sur, que representa 3,5% de números IP activos. Oceanía ocupa el cuarto lugar con un 2,8%. El estudio también pone en relación el nivel de conectividad con la densidad de población de cada región, lo que muestra que en zonas muy pobladas de África, India y China, la adopción de Internet todavía es muy baja comparada con la de Estados Unidos. Estos mapas están disponibles en el sitio de IPIgence, una empresa que se dedica a la geolocalización: la conversión de IPs a datos geográficos (regiones, países, ciudades, coordenadas) para poder usarlas en diversas aplicaciones y servicios <http://histointernet.wordpress.com/2010/09/28/mapa-de-la-distribucion-de-los-usuarios-de-internet-en-el-mundo/>

para nosotros contiene la noción de intimidad que es más reducida.⁵

Hay culturas en las cuales todo parece público y poco privado, como las mediterráneas y otras en las cuales se da el fenómeno opuesto, como en las del norte europeo y el mundo anglosajón⁶.

La privacidad ya no es considerada como un principio según el cual nadie invade “nuestro mundo”, demasiado estrecho, sino que también debe entenderse como el derecho de todos a expresar libremente las aspiraciones más profundas y a que se realicen, libre y plenamente, en todo su potencial.

En este sentido se habla de la intimidad como “la libre determinación y soberanía sobre sí mismo” (Stefano Rodotà)⁷ y “derecho a ser yo” (José Fortunato)⁸; de este modo se transforma en un derecho activo que permite afirmar un ámbito personal frente a los acosos permanentes de las entidades poderosas públicas o privadas que se apoderan de datos e historias. Deja de ser un derecho pasivo de resistencia para tornarse un instrumento activo de la propia libertad

que da capacidad de investigar, pedir explicaciones, revisiones, eliminaciones y olvido de datos que afecten el derecho de ser uno mismo.

El derecho a la intimidad es una creación de derecho, que lo ubicó entre los derechos inalienables.

Olvidemos por el momento el adjetivo “informática” y vayamos al sustantivo “soberanía”. El Diccionario de la Real Academia Española⁹ define *soberano* como aquel que manda sobre todos y es independiente. No hace falta ser un gran experto para reconocer la teoría de Austin sobre la soberanía¹⁰. Es difícil mejorar esta presentación de la teoría: “En esta versión simple... dondequiera haya un sistema jurídico es menester que exista alguna persona o cuerpo de personas que emitan órdenes generalmente respaldadas por amenazas y que esas órdenes sean generalmente obedecidas, y tiene que existir la creencia general de que estas amenazas serán probablemente hechas efectivas en el supuesto de desobediencia. Esta persona o cuerpo debe ser internamente supremo y externamente independiente. Si, de acuerdo con Austin, llamamos *soberano* a tal persona o cuerpo de personas supremo e independiente, las normas jurídicas de cualquier país serán ordenes generales respaldadas por amenazas dictadas por el so-

5 Para un mayor desarrollo ver el artículo citado en la nota 20 de mi autoría.

6 Pero además se presta a equívocos formidables: en América Latina y en Francia, un autor que ha cautivado el mundo de la izquierda ha sido Gramsci. En el mayo francés los estudiantes gritaban “nada es privado, todo es público” y creían estar en el tope de la revolución socialista. En realidad, Gramsci tomó la frase de Giovanni Gentile, filósofo de la derecha, inspirador y ministro de Educación del gobierno fascista italiano.

7 Privacy, Freedom, and Dignity Closing Remarks at the 26th International Conference on Privacy and Personal Data Protection Wroclaw, 16 September 2004.

8 Discurso de incorporación de Fortunato González Cruz a la Academia de Ciencias Políticas y Sociales de Venezuela.

9 Soberanía. f. Cualidad de soberano. || 2. Autoridad suprema del poder público. || 3. Alteza o excelencia no superada en cualquier orden inmaterial. || 4. ant. Orgullo, soberbia o altivez. || ~ nacional. f. La que reside en el pueblo y se ejerce por medio de sus órganos constitucionales representativos. soberano, na. (Del b. lat. *superānus). adj. Que ejerce o posee la autoridad suprema e independiente.

10 Austin, J.L., *The Province of Jurisprudence Determined*, 1832, Conferencia VI (ed. 1954, p. 259).

berano o por los subordinados que obedecen a aquel.”¹¹

Hobbes: “el legislador no es aquél bajo cuya autoridad la ley fue hecha por primera vez sino aquél por cuya autoridad continúa hoy siendo ley.”¹²

La independencia de una autoridad extranjera no significa poder ilimitado internamente. Las constituciones federales distinguen entre los poderes del gobierno federal y de los estados miembros y, en general, se reparten las facultades entre poderes como el legislativo, el ejecutivo y el judicial. Es más, la mayor parte de las constituciones contienen cláusulas generales de garantía para los ciudadanos, que no pueden modificarse sino con ritos especiales, como la famosa Quinta enmienda a la Constitución de Estados Unidos que establece (entre otras cosas) que ninguna persona será privada de “su vida, libertad o propiedad sin el debido proceso legal”. Con base en estas cláusulas muchas leyes del Congreso han sido declaradas contrarias a la Constitución y por ello inválidas.

La contraposición entre la concepción jurídica y política de la soberanía es relativa pues si se revisan con cuidado las teorías enunciadas se verá que en casi todas aparecen ambos aspectos, más o menos subrayados. En el caso de Kelsen, la soberanía es un producto normativo unitario del Estado, pero tiene un límite muy claro en el uso, esto es, en el *iuris consensum*.

11 Hart, H.L.A., *The concept of Law*, Oxford University Press, 1961, traducción española de Genaro R. Carrió, Abeledo Perrot, Buenos Aires, 1963, p. 32.

12 *Leviathan*, cap. XXVI.

Tres elementos aparecen claramente hoy en día: la existencia de derechos supraestatales como la Unión Europea o la Corte Internacional de Justicia; la fuerza económica transnacional de un mundo de la producción y el consumo siempre más *globalizado*¹³; el avance tecnológico de los medios de comunicación de masas que constituyen una opinión pública global y que hacen saltar las referencias espaciales y temporales del pasado.

Cada vez que los gobiernos quieren imponer el avasallamiento de los derechos a la intimidad de los ciudadanos, sobre todo en América Latina, se recurre a la idea de soberanía.

En algunos países, como Italia, se ha creado una autoridad independiente (*authority*) para vigilar expresamente el derecho a la privacidad.

Declina el Estado, nacen nuevos poderes; van previstos, descritos y reglamentados. Aparecen nuevos fenómenos de soberanía como el de la Autoridad Palestina, sobre un territorio fragmentado. Los derechos humanos son un claro límite a la soberanía interna.

La privacidad ya no es considerada como el principio por el cual nadie invade “nuestro mundo” condenada de antemano, sino también entenderse como un derecho que todos puedan expresar libremente sus aspiraciones más profundas y que se realicen, libre y plenamente, en todo su potencial.

El derecho a la intimidad es una creación de

13 Uso la expresión con dificultad, pero rindiéndome a un empleo generalizado.

derecho, que lo ubicó entre los derechos inalienables mencionados en el artículo 2 de la Constitución italiana. Tiene la función de definir el concepto de interés público en las noticias, con exclusión de la existencia de un derecho de la sociedad para penetrar en la intimidad de un individuo con el único propósito de satisfacer una curiosidad morbosa.

Existe un marcado interés en exaltar la importancia de proteger a los individuos de las injerencias de los Estados sobre el uso de Internet al igual que sucediera al reconocerse, primigeniamente, la supremacía del derecho a la intimidad frente a las intromisiones de la prensa escrita. La apertura mundial de la Red, que en sus orígenes fuera un lugar de privilegio para pocas personas, permitió poner al alcance de la mano de millones de usuarios asombrosas cantidades de información, en grado tal que esta ha adquirido estatus de bien jurídico susceptible de tutela legal. Pero, por otra parte, permitió que la masiva disposición de este valioso bien (v. g. la información) pudiera ser fácilmente recopilada, vendida o utilizada como medio de control de los propios usuarios. Es allí donde se advierte el problema que nos convoca: el innegable derecho de preservar la privacidad de quienes utilizan estos medios comunicacionales, el no menos importante derecho de aquellos que requieren obtener y utilizar información fiel sin que ello implique la afectación de las esferas íntimas y, finalmente, el controvertido principio que parece convertirse en rector de los vínculos entre los individuos y la red global: el anonimato.

Si en algún momento se advirtió que la actividad indebida de la prensa escrita podría cons-

tituir una amenaza a la privacidad o bien el accionar de la autoridad administrativa, legislativa o judicial podría ser constitutivo de actos lesivos a la intimidad, es claro que las actuaciones de los particulares también, en determinadas circunstancias, pueden considerarse como potencialmente peligrosas. Y es por eso que crece el derecho a la transparencia.¹⁴

El incremento de las posibilidades de obtener medios de comunicación económicos, masivos, con amplio poder de difusión y escasa protección a la confidencialidad ya en el aspecto técnico, ya en el legal, permite la proliferación de conductas que pueden resultar lesivas por intromisión en las esferas íntimas de los individuos. Tal desarrollo comenzó con la telefonía y las consecuencias del uso indebido de la información transmitida por dicho medio motivaron la necesidad de regulación específica.

Nos hallamos ante otro aspecto del problema pues no estamos ante una intromisión que afecta el principio de determinación autónoma de la conciencia del agraviado, sino que veda la posibilidad de la persona de manifestarse y actuar libremente, sin injerencias del poder público o de los particulares a quienes la comunicación no les está dirigida (art. 5, capítulo 1ro., de la Declaración Americana de Derechos y Deberes del Hombre; art. 12, de la Declaración Universal de Derechos Humanos¹⁵; art. 17, del Pacto Inter-

14 En estos días, durante su participación en la Cumbre Conectar las Américas, que se desarrolla en Panamá, el presidente Ricardo Martirelli anunció que propondrá ante las Naciones Unidas (ONU) la regulación mundial de los números IP en publicaciones a favor o en contra de alguna persona u organización a través de Internet.

15 "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su correspondencia, ni de ataques a su honra o su reputación.

nacional de Derechos Civiles y Políticos¹⁶ y art. 11, apartado 2, de la Convención Americana sobre Derechos Humanos¹⁷). Directiva Europea 95/46 CE de 24 de octubre del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En noviembre del 2005, la Unión Internacional de las Telecomunicaciones, una agencia de Naciones Unidas, presentó su informe sobre el *Internet de las cosas*. “El próximo paso es integrar cosas en una red de comunicación. Esta es la visión de una verdadera red ubicua: en cualquier lugar, a cualquier hora, por cualquier persona y con cualquier cosa”. Y las cuatro tecnologías que enumeraba para hacerlo posible eran las etiquetas de identificación por radiofrecuencia (RFID), los sensores inalámbricos, la inteligencia embebida y la nanotecnología. En un capítulo donde imaginan el futuro describen la vida de “Rosa, una estudiante española, en el 2020”. Quiere irse un fin de semana a los Alpes y los sensores de los neumáticos le avisan de una avería, compra una chaqueta multimedia con ajustes de temperatura, tiene una videoconferencia con su novio a través de las gafas...

Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

16 “1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

17 “Protección de la honra y dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

El Parlamento Europeo (PE) ha llamado a garantizar la privacidad y la protección de los datos personales de cara a la futura conexión de objetos cotidianos a la Red, el llamado *Internet de las cosas*. Teniendo en cuenta que “todos los objetos de nuestra vida cotidiana (tarjetas de transporte, ropa, teléfonos móviles, coches, etc.) podrían acabar equipados con un chip”, la Eurocámara considera que además de aprovechar las ventajas es necesario hacer frente a algunos riesgos. Por ello, en un informe elaborado por la socialista María Badía y aprobado por el pleno, hace hincapié en la necesidad de establecer un marco jurídico europeo que garantice la privacidad de los ciudadanos y la protección de los datos personales.

Internet, como red mundial de información, es una fuente generadora de eventos que atentan contra la intimidad, pues las reglas con que se rige solo tienen en mira permitir la agilidad y fluidez del tráfico de información, la ilimitada oferta y la ausencia de identificación de sus integrantes. En este entorno es imposible suponer que quienes pretendan ejercer plenamente su derecho a mantener su privacidad alejada de la intromisión ajena puedan resultar airosos. La ausencia de normas imperante dificulta la aplicación de las garantías constitucionales que estamos analizando. ¿Es posible tratar análogamente el domicilio a un terminal de computación o al contenido de un disco rígido?, ¿El contenido de una página o un sitio es comparable con una publicación o con los papeles privados?, ¿El correo electrónico guarda relación estrecha con la correspondencia postal? En todos los casos no se debe perder de vista que la garantía de la

inviolabilidad es una forma de libertad personal que protege la esfera de intimidad o reserva del individuo, manteniendo el secreto de toda expresión privada, y que, por tanto, no puede considerarse como tal a cualquiera de los elementos enunciados, sino que dicho concepto, en lo que a la tutela constitucional se refiere, incluye solo la información que comprenda, concretamente, la comunicación de ideas, sentimientos, propósitos o noticias de una persona hacia otra u otras personas determinadas por un medio apto para fijar, transmitir o recibir la expresión del pensamiento.

El tema es siempre respetar la transparencia pública permitiendo el derecho personal a la privacidad, que es libertad, independientemente del medio que se use.

La privacidad se refiere a la habilidad de guardar información oculta a los ojos de los usuarios. Lo ideal sería evitar que cualquiera obtuviera información sobre nosotros, nuestro sistema de computadora, sitios web favoritos y otros datos personales.

La privacidad ha sido definida como la demanda de personas, grupos o instituciones para determinar para ellos mismos cuándo, cómo y qué información personal es de comunicar a otros. Algunas personas creen que la enorme capacidad de las computadoras de almacenar y recuperar información hace más fácil para el gobierno o las empresas infringir nuestro derecho a la privacidad.

La recolección de datos favorece la fluidez del funcionamiento del gobierno, de los negocios

y de la investigación. Pueden utilizarse los datos para chantaje, en especial de tipo político a gran escala por parte de gobiernos o políticas con demasiado poder. Los errores en la recolección de datos pueden llevar a muchas prácticas injustas, tales como negar empleo o crédito. Datos obsoletos o incompletos que pueden provocar problemas. Los sistemas de transferencia electrónica de fondos (ETF) (TEF) también parecen implicar un atentado a la privacidad. Este sistema es muy popular entre los proveedores ya que la mala escritura de un cheque será cosa del pasado. El beneficio para los bancos es que el sistema reduce los trámites (o papeleo) requeridos para procesar los cheques. Las organizaciones pueden ayudar a salvaguardar la privacidad de los datos y reducir sus oportunidades de convertirse en víctimas de delitos informáticos de computadora instituyendo un sistema de seguridad. Un sistema de seguridad debe incluir un programa de control interno, procedimientos, organizaciones, equipo, software y base de datos. La meta de la seguridad de las computadoras y del control interno es desproteger esos recursos. La sociedad necesitará adaptarse a una legislación que limite la recolección, almacenamiento y acceso a la información personal. Entre las limitaciones que han sugerido están anotadas en este trabajo: personas a las que se les debe informar acerca del tipo de información que se está conservando. Las personas deben tener derecho a realizar el acceso a cualquier información almacenada sobre ellas mismas. Toda información debe ir firmada por la persona que la almacenó.

Correo electrónico. Esto ha llevado a numerosos reclamos legítimos por parte de empleados y a

algunos juicios por la violación de la privacidad. Cuando esté utilizando un sistema de correo electrónico, tenga en mente que los mensajes pueden ser monitoreados. Los controles pueden ser divididos en tres categorías básicas: controles generales, controles de programas y documentación.

Existe un marcado interés en exaltar la importancia de proteger a los individuos de las injerencias de los Estados sobre el uso de Internet al igual que sucediera al reconocerse, primigeniamente, la supremacía del derecho a la intimidad frente a las intromisiones de la prensa escrita.

Otra gran trampa para avasallar los derechos de la privacidad, de la intimidad y hasta de “ser yo” es oponerle otro derecho humano como la transparencia, que en casos como la persecución de delitos de la dictadura puede llegar a obnubilar la idea de que si hay dos derechos en conflicto no necesariamente el de índole pública es más importante que el de índole privada. En Argentina el caso de casos más famoso es el de Marcela y Felipe Noble Herrera¹⁸. En 2002 se realizó una denuncia penal a instancias de las Abuelas de Plaza de Mayo y de las familias Lanuscou-Miranda y García-Gualdero, que suponen que Marcela Noble Herrera y Felipe Noble Herrera podrían ser hijos de desaparecidos. El 17 de diciembre de 2002, el juez Marquevich dispuso que la policía condujera detenida a Herrera de Noble para tomarle declaración indagatoria por el delito de “uso de documento público falso” e inmediatamente le negó la excarcelación; este

proceder era arbitrario porque el delito que le imputaba —haber incurrido en una falsedad en las partidas de nacimiento de sus hijos— había prescrito y no podía ser investigado, y el juez, para poder seguir adelante con el proceso vinculó la adopción “sin prueba alguna” con la sustracción de menores durante el último gobierno de facto. Herrera de Noble es dueña del diario *Clarín* opositor al gobierno. Con la excusa de la mayor importancia de la investigación de desaparecidos (soberanía) se sometió a los Herrera a toda suerte de atropellos, incluyendo la obtención de prendas íntimas que fueron obligados a dar a la policía luego de una feroz caza y atrape en sus domicilios. Se pidió la revisión de los DNA de los Herrera con todos los que tienen las Abuelas de Plaza de Mayo como pertenecientes a desaparecidos, no obstante que los hermanos declararan que no tenían ningún interés en conocer sus orígenes. Fueron muchas instancias y años de discusiones sobre el derecho a la intimidad de los Herrera, a los cuales se hizo caso omiso. El caso se resolvió simplemente porque en la reconstrucción de los DNA los hermanos resultaron totalmente ajenos a cualquier DNA de desaparecidos. El problema es que se hizo valer la noción de valor público mayor del derecho a saber (soberanía) transparencia contra el derecho a la intimidad (valor subjetivo).

A. Una historia

Una historia, no importa si real o no, la cuenta uno de los más famosos autores de los últimos tiempos: Neal Stephenson.¹⁹

18 Ver MARTINO, A.A., Entre la transparencia y la privacidad, Actas del Congreso de Monterrey, 2010. Ahora en impresión en la *Revista de derecho de las telecomunicaciones, internet y medios audiovisuales*.

19 STEPHENSON, N., *Criptonomicon*, 1999, p. 395 y ss. Con traducción y adaptaciones mías.

El gran visir de Kinakuta lo conduce a las oficinas de su jefe, el sultán, y lo deja solo por algunos minutos... Se encuentran en el palacio nuevo, cuyas tres alas enmarcan los jardines exóticos del antiguo y majestuoso palacio viejo. La sala de conferencias tiene techo cóncavo de diez metros de altura. La parte que mira al jardín está construida totalmente de vidrio, en forma tal de crear la impresión de estar en una terraza que contiene un modelo en escala reducida del palacio del sultán... La puerta vuelve a abrirse y el gran visir introduce un grupo de japoneses... o chinos... tal vez de Taiwán. Otras delegaciones entran en la sala guiadas por el gran visir, australianos, asiáticos... la mesa es una de conferencias para alta tecnología con cables eléctricos y telefónicos incorporados que permiten a quien interviene conectar la laptop sin necesidad de desenrollar cables y tomas de corriente... Comienzan a llegar pequeños kinakutanos que se acomodan en un extremo de la mesa suficientemente grande como para hospedar la Última Cena. En el lugar correspondiente a Jesús hay una poltrona enorme y costosa... finalmente entra un hombre pequeño, que mira el suelo aparentemente desinteresado de la presencia de otra gente. Tiene los pelos que parecen pegados al cráneo con barniz y la solemnidad de su aspecto está atenuada por un *capolarovo* de Armani. Se acomoda en la poltrona, es el sultán.

El dueño de casa comienza a hablar de Kinakuta como lugar de encuentro de culturas. Nada más natural, por ende, que el deseo de los kinakutanos modernos de tender en todas las direcciones grandes cables de fibra óptica co-

nectados a las más importantes compañías de telecomunicaciones de los países circunstantes y de transformar a la isla en una suerte de bazar digital. Después de todo, continúa el sultán, la ubicación física no tiene alguna importancia en un mundo digitalizado y conectado en redes. El ciberespacio no conoce límites. Pero, un momento, ¡¡esta es una enorme estupidez!! La ubicación física cuenta y cómo... A este punto la sala se sumerge en penumbra, mientras la luz que la invadía de afuera se atenúa gracias a un invisible mecanismo incorporado a los vidrios: una especie de persianas a cristales líquidos. Desde fisuras hábilmente escondidas en el techo bajan pantallas. El sultán hace aparecer gráficos partiendo de un planisferio en el cual Estados Unidos y Europa parecen aprisionados por hilos articulados. Sobre el planisferio, en sobre impresión, aparece el trazado de líneas rectas cada una de las cuales une grandes ciudades, las líneas crecen tanto hasta oscurecer totalmente el planisferio. Esta, dice el sultán, es la visión corriente de Internet: una red sin un centro que une todos con todos.

¡Pero esto también es una estupidez! Compáren esta otra visión del planisferio. Ahora se notan las redes internas en cada país y en algunos casos continentes enteros. Pero entre país y país y sobre todo entre continente y continente hay muy pocas líneas de conexión. ¡No tiene el aspecto de una red! En realidad la casi totalidad del tráfico intercontinental vía Internet pasa por un número limitado de cuellos de botella administrados por gobiernos locales. Como consecuencia, la posibilidad misma de usar Internet al socaire de las injerencias de los gobiernos

está perjudicada de entrada por un problema estructural y de fondo.

“Los cuellos de botella no son sino uno de los obstáculos estructurales que se interponen a la creación de un espacio libre, soberano, realmente descentrado.” “Un ulterior obstáculo está representado por el heterogéneo mosaico de las legislaciones y de los modelos jurídicos vigentes en materia de garantías de la privacidad, libertad de expresión, política de telecomunicaciones...”

Aparece otro planisferio, cada Estado ha sido coloreado, surcado de rayas o de puntos sobre la base de un esquema de formidable complejidad.

“La actitud de un cierto modelo jurídico sobre temas de la privacidad es, en general, el fruto de progresivos ajustes introducidos en el curso de los siglos por cortes de justicia y cuerpos legislativos”. Dice el sultán: “con el debido respeto todo esto tiene poco que ver con las cuestiones de la privacidad en el mundo actual”.

Vuelve la luz, el sol irrumpe en las ventanas, las pantallas desaparecen en el techo y todos están sorprendidos de ver al sultán en pie. Se está dirigiendo a una gran tabla de go lujosa y decorada con piedras preciosas. “Tal vez podamos establecer una analogía con el juego del go o del ajedrez. Al comienzo de cada partida, las piezas se disponen según un esquema simple y fácil de visualizar. Cada partida, empero, tiene muchos desarrollos, los jugadores hacen una movida por vez, lo que permite seguir las; más difícil es comprender la complejidad de todo el juego a

medida que avanzan las movidas que solo las mentes más refinadas pueden comprender. La analogía es clara, nuestras políticas en materia de libertad de expresión, telecomunicaciones y criptografía, una decisión luego de otra ha adquirido un grado tal de complejidad que nadie está en condiciones de desmadejarlas en un solo país. Figuremos cuál es la situación si se toman todos los países contemporáneamente...” El sultán da grandes pasos en torno a la mesa de go. Permanece en silencio, silencio que se torna embarazoso. Finalmente, extiende su brazo sobre la mesa y con un gesto rápido y violento tira todas las fichas al suelo con un solo golpe. Sigue un silencio de quince segundos.

“Es hora de comenzar de nuevo —dice el sultán— cosa difícil en los grandes países donde las leyes son emanadas por cuerpos legislativos, interpretadas por jueces, influenciadas por antiguos precedentes. Aquí estamos en Kinakuta, el sultán —o sea yo— declaro que la ley debe ser extremadamente simple: libre circulación de las informaciones. Yo renuncio, por lo tanto, a cualquier derecho gubernamental sobre flujo de informaciones dentro de mis confines. Nadie, por ninguna razón, miembros o agentes del gobierno intentarán poner bajo control o limitar tales flujos. Esta es la nueva ley de Kinakuta. Los invito a aprovecharla. Gracias”.

La narración puede aparecer improbable, pero es posible y lo más importante: es físicamente posible.²⁰ “La naturaleza copia al arte” diría

20 Que una norma sea físicamente posible, esto es, que los presupuestos físicos que describe y que van a servir para el antecedente de la normación, es sumamente importante. Muchas leyes fracasan porque simplemente los presupuestos fácticos desde los cuales se parte son falsos. En una lógica clásica, si el antecedente es falso la proposición

algún provocador. Pero hay un elemento destacable en la historia: podría ser verdadera, así como son verdaderos los paraísos fiscales. Todo depende de la soberanía informática. Y las consecuencias no serían tan simples como pensamos la “libertad de información”. Aquí lo que se decide es libertad para los contenidos y para los transportadores de contenidos. Ya estamos en una era en la cual pensamos que los transportadores están avanzando demasiado sobre los contenidos. Por ejemplo, las propuestas Sopa en EEUU y Acta en Europa son una limitación para todo derecho pues los dueños de los medios deciden quién “respetar” y quién no el derecho a la propiedad intelectual y con esa excusa pueden oscurecer cualquier transmisión que les resulte incómoda. Por otro lado, la falta total de control sobre los contenidos lleva a que cualquiera pueda decir cualquier cosa sobre otros y de nuevo gana la transparencia (ahora es un negocio) y pierde la privacidad que no encuentra formas de hacer valer sus derechos.

II. CONCLUSIONES

En un mundo globalizado e intercomunicado crecen las posibilidades de violar la privacidad de los individuos y las empresas.

El desarrollo y la penetración de Internet no son parejos y América Latina está retrasada en la segunda; ello no es obstáculo para que siga aferrada a una noción de soberanía en franco

decaimiento pero que puede servir cuando se quieren obtener objetivos de “bien común” que contradigan las libertades, sobre todo las relativas a la intimidad.

Las reformas jurídico-políticas y tecnológicas que habilitarían una gestión democrática de estos derechos ciudadanos son de alta complejidad. Por ejemplo, ¿cómo podrían los ciudadanos ejercer un derecho a ser olvidados cuando sus datos e informaciones ya son gestionados por corporaciones comerciales que se niegan a cumplir las leyes, engañan a los usuarios y pueden copiar y transferir en segundos estos datos a cualquier parte del mundo? ¿Se habrá iniciado una era pos-privacidad?

Una buena práctica para cubrirse de asechos consiste en crear autoridades independientes de los demás poderes, que se ocupen sustancialmente de defender y proteger a los ciudadanos de los abusos del Estado o de cualquier entidad pública o privada, como pueden ser las grandes empresas internacionales. No solo Italia tiene una entidad de este tipo; toda Europa cuenta con un **Supervisor Europeo de Protección de Datos (SEPD)**, que es la autoridad independiente que se encarga de promover buenas prácticas sobre la privacidad.

En todo el mundo se tratan de imponer algunas normas sobre protección de la propiedad intelectual que son conflictivas con el derecho a la privacidad de los ciudadanos, pues implican un monitoreo y la posibilidad de ser eliminados de Internet por la interpretación que las empresas editoriales dan a la expresión “propiedad intelectual”. Esto está aconteciendo en EEUU con

es verdadera por definición; en lógica deóntica, si el antecedente es falso, no hay manera de verificar la posibilidad de aplicación del mandato contenido en el consecuente, por ende toda la normación carece de sentido, dado que la norma tiene su justificación y fin en el cumplimiento generalizado.

proyectos como Sopa y todos sus derivados, y en Europa con el proyecto Acta que tiene más o menos los mismos contenidos. El SEPD ha advertido que las medidas del Acta, que persiguen defender los derechos de la propiedad intelectual, pueden derivar en amenazas para la privacidad y la protección de datos si no se llevan a cabo de un modo correcto.

En concreto, estas amenazas tienen lugar en el contexto de la *monitorización de los usuarios* y de sus comunicaciones por vía electrónica, lo que choca de frente con la Carta de Derechos Fundamentales y con la Directiva Comunitaria de Protección de Datos. Además, para poder llevar a cabo este control, se prevé que las isp participen en el proceso, lo que es contrario al precepto de Neutralidad de la Red que en principio Europa defiende.

Por último, el SEPD denuncia que el Acta no contiene **suficientes garantías** para que su puesta en funcionamiento conlleve el debido rigor de un juicio justo, presunción de inocencia o derecho a la privacidad y a la protección de los datos de las personas que puedan ser objeto de investigación.

La del SEPD es una voz más que surge, contraria a las imprecisiones que supone el Acta, y se da a conocer un día antes de que se abra el debate en torno al borrador que dará paso a la votación del Acta en sede parlamentaria.

Una guía simple y sencilla de seguir sería que todos los países adoptaran un criterio de diez reglas relativas a los asechos que tiene la defensa de la privacidad. No se trata de entorpecer ninguna acción pública o privada, solo de recaudos

para un bien tan difícil de custodiar y antes de que se produzca el daño:

1. Determinación de los objetivos de la investigación y justificación de los datos necesarios para cumplir con estos objetivos.
2. Limitar la recogida de datos personales.
3. Determinar si el consentimiento de los individuos se requiere.
4. Gestionar y documentar el consentimiento.
5. Informar a los posibles participantes de la investigación sobre la investigación.
6. Reclutar a los posibles participantes de investigación.
7. Protección de datos personales.
8. Controlar el acceso y la divulgación de datos personales.
9. Establecer límites razonables a la retención de los datos personales.
10. Garantizar la rendición de cuentas y la transparencia en la gestión de los datos personales.

Casi todos los países latinoamericanos tienen autoridades de protección de datos y privacidad pero carecen de los recursos y de la envergadura para atender antes de que se produzcan los eventos, durante y después. Se hacen reuniones americanas o mundiales²¹ pero no son suficientes cuando la puesta en juego es grande.

21 Como la última de México el año pasado.

Otra buena práctica es la existencia de redes de instituciones públicas o privadas dedicadas a la protección de datos y privacidad, sea para advertir al ciudadano, sea para estar presente cuando se discutan leyes u ordenanzas administrativas que puedan ser peligrosas.

Los Estados deben prohibir a las empresas de Internet y telefonía móvil (proveedores del servicio, buscadores y redes sociales) que almacenen datos sensibles de los usuarios, clientes y ciudadanos. Por el otro, se deben aumentar las capacidades que tienen los usuarios para ejercer sus derechos de reserva y su derecho a ser olvidados.

El otro asecho que se debe tener presente es el conflicto de prioridades que puede presentarse cada vez que se invocan valores de derechos humanos del derecho público. Nada hace suponer que deba prevalecer necesariamente el de derecho público a menos que se invoque o suponga la teoría de la soberanía. Es uno de los casos más peligrosos de resolver justamente por la confrontación entre valores.

Si por casualidad alguien intentara la solución para los temas de Internet como hemos relatado en la historia de ciencia ficción, esto funcionaría como un paraíso fiscal (pero no solo a los efectos fiscales sino también de dominio absoluto sobre transportadores de datos y contenidos) y tentaría por igual a empresas multinacionales ávidas de manejar todos los datos y a gobiernos autoritarios abroquelados detrás de la noción de soberanía (sería la versión negativa de la historia contada). En todo caso, la amenaza sobre la privacidad sería muy fuerte y es

conveniente tratarla antes de que a alguien se le ocurra materializarla para tener prontas las armas de organismos internacionales —como este— en defensa del derecho a ser yo, la intimidad y la privacidad.

Bibliografía

AMBOS, K. *La nueva justicia penal supranacional. Desarrollos post-Roma*. Valencia: Tirant lo Blanch, 2002, 549.

AA.VV. Lineamientos europeos para el proceso penal alemán. Análisis con base en la jurisprudencia del Tribunal Europeo de Derechos Humanos en el periodo 2000-2003. *Anuario de derecho constitucional latinoamericano*. Décimo año. Edición 2004. Tomo II. Montevideo: Konrad-Adenauer-Stiftung, 2004, págs. 761-800.

PECORELLA, C. *Il diritto penale dell'informatica*. 2000. Padova: CEDAM, págs. 404; "Dieci anni di giurisprudenza sui reati informatici: i principali problemi interpretativi sollevati dalle nuove disposizioni". En: AA.VV., *Interpretazione e precedente giudiziale in diritto penale*, 2005, Padova: CEDAM, págs. 241-269.

ETXEBERRIA GURIDI, J.F., ORDEÑANA GEZURAGA, I. *Video-vigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*. Valencia: Tirant lo Blanch, 2010.

STEPHENSON, N. *Criptonomicon*, 1999, págs. 395 y ss.

- AUSTIN, J.L. *The Province of Jurisprudence Determined*. 1832. Conferencia VI (ed. 1954, pág. 259).
- MARTINO, A.A. *Entre la transparencia y la privacidad*, Actas del Congreso de Monterrey, 2010. Ahora en impresión en la *Revista de derecho de las telecomunicaciones, internet y medios audiovisuales*.
- REMOLINA ANGARITA, N., et al., “Actualidad de protección de datos personales en América Latina. Caso Colombia”. En: *Colombia revista española de protección de datos*, ISSN: 1887-7907 ed.: v. 7, fasc. págs. 227-271, 2009.
- REMOLINA ANGARITA, N. “¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?”. En: *Colombia International Law*, revista colombiana de derecho internacional, ISSN: 1692-8156, Bogotá, Pontificia Universidad Javeriana, v.16, fasc. N/A págs. 489-523, 2010.
- EUROLAT. *La protección de datos en Europa y América Latina*, n.º 83, año 17, agosto 2011.
- VILLANUEVA, R. *Protección constitucional de los derechos sexuales y reproductivos*. IIDH, UNFPA, 2008.
- PUCINELLI, O.R. *Tipos y subtipos de hábeas data en América Latina*, Astrea, 2004.
- BRIAN NOUGRÈRES, A. “El sistema legal uruguayo de protección de datos personales”. En: *Revista de derecho comunicaciones y nuevas tecnologías*, Bogotá, Universidad de los Andes, 2007.
- AA.VV. *Privacy, Freedom, and Dignity Closing Remarks at the 26th International Conference on Privacy and Personal Data Protection Wrocław*, 16 September 2004.