

¿Está muerta la privacidad? Algunas reflexiones a modo de respuesta

Carlos Gregorio de Gràcia¹

La primera pregunta a abordar es si los derechos mueren. La respuesta no es fácil, al menos desde una perspectiva jurídica. Hoy todos creemos que la esclavitud (en tanto derecho de propiedad sobre una persona) está muerta. Sin embargo en Brasil, por ejemplo, el Tribunal Superior de Trabalho sigue recibiendo causas por trabajo esclavo. Por otra parte, cuando se abolió la esclavitud en Brasil no bastó una decisión legislativa: el entonces ministro de Justicia Rui Barbosa mandó a quemar los libros que contenían los registros de propiedad de los esclavos, en la llamada *Queima dos Arquivos da Escravidão*.² Esto muestra que los derechos no solo se apoyan en las formalidades legales, las costumbres, o la administración de justicia; otros elementos como las bases de datos y la información tienen un papel muy relevante en su existencia.

Por eso, para poder hablar de una eventual muerte de la “privacidad”, es pertinente preguntarse cómo nació el derecho a la

¹ Investigador y consultor del Instituto de Investigación para la Justicia, Uruguay.

² Este hecho (la quema de los archivos de la esclavitud), ocurrido en 1891, independientemente de la controversia sobre su fundamentación señala que existe una estrecha relación entre los “registros” y los derechos, entre su existencia y su vigencia, y que no es posible garantizar ciertos derechos si se mantiene una base de datos activa, y viceversa. Por esta razón, no basta mirar las leyes sobre privacidad y su vigencia, sino que también es necesario analizar qué datos personales se registran y con qué finalidad.

privacidad. Podemos identificar dos nacimientos: uno en los EE.UU., con los trabajos de Warren y Brandeis en la década de 1890, para proteger fundamentalmente la intimidad sexual. La llamada *privacy* no está contemplada en la Constitución de los EE.UU., por lo que ha sido modelada por la Suprema Corte a través de una serie de sentencias, la mayoría de ellas relacionadas con casos donde los hechos refieren a la sexualidad. Para dar un ejemplo reciente, una decisión en *Vernonia School District v. Wayne Acton et ux.* 515 U.S. 646 (1995) entiende que los atletas tienen una menor expectativa de privacidad precisamente por el grado de desnudez con que intervienen en los deportes.

A su turno, la privacidad también nace en Europa, esta vez bajo la forma de la protección de los datos personales. El motivo subyacente es un hecho histórico: el exterminio de judíos, gitanos y otros grupos determinados de personas que emprendieron los nazis en Alemania, utilizando los datos del censo para identificarlos. De allí aprendieron los alemanes que la única protección de los ciudadanos en el futuro, ante nuevas concentraciones de poder, era evitar de raíz la acumulación de datos personales. Esta percepción de la protección de los datos personales como un derecho fundamental se extiende por toda Europa.

No es extraño entonces que la primera ley latinoamericana de protección de datos se sancionara en Argentina en 1994, como consecuencia de la inclusión del *habeas data* en una reforma constitucional. El movimiento de protección de datos personales en Argentina podría relacionarse con las prácticas de exterminio de la dictadura militar (1976—1983). El gobierno dictatorial, aparte de disponer de todos los datos que se acumulaban bajo el nombre de “inteligencia del Estado”, cuando capturaba una persona utilizaba sus agendas telefónicas para investigar y capturar a otros contactos que allí figuraban.

Desde el punto de vista de la sociedad de la información, el paradigma de la *privacy* de los EE.UU. ha quedado descolocado, pues hoy la sexualidad no es mas un tabú como en 1890 y el tema sexual se hace público sin un reproche generalizado.

También es cierto que la protección de datos personales concebida como derecho fundamental en la tradición del modelo europeo es más adecuada para resolver los problemas de la sociedad de la información. Ante un flujo de datos sensibles sin ningún tipo de control y protección, el riesgo fundamental que quiere evitarse es la discriminación con fines injustos.

Esto puede verse si se analiza con cuidado la legislación más reciente sobre protección de datos de salud de EE.UU.³ que, podría decirse, ha tomado el paradigma europeo de protección de datos y ha dejado muy lejos el concepto del derecho a ser dejado solo de la tradicional *privacy*.

En la visión europea la protección de datos es uno de los derechos comprendidos por la libertad de expresión. Esta libertad incluye en primer lugar el derecho a expresarse, pero también el derecho a no expresarse (también llamado autodeterminación informativa, que es equivalente al derecho de protección de datos), así como el derecho de audiencia. Las implicaciones de la libertad de expresión pueden “enfocarse en quien habla” versus “enfocarse en la audiencia”; el derecho de audiencia atiende al interés de proveer a los ciudadanos de un amplio acceso a puntos de vista conflictivos y a asuntos poco corrientes, no solo porque quienes tienen ideas disruptivas tengan derecho a ser oídos, sino porque la sociedad tiene un especial interés en oírles.⁴ Esta visión más actual de la libertad de expresión no refuerza el derecho de expresar ideas excéntricas, sino que prioriza el derecho de todos los ciudadanos a acceder a todas las ideas, en especial las que no coinciden con su forma de pensar.

Cuando se analizan los riesgos actuales resulta obvio que la privacidad y la protección de datos están siendo atacadas, pero

3 Privacy Act 5 U.S.C. § 552a, 45 CFR 160.103, Subpart E—Privacy of Individually Identifiable Health Information § 164.501 y fundamentalmente HITECH Act TITLE XIII- Subtitle D—Privacy - SEC. 13400

4 Tushnet, Rebecca. 2008. “Power Without Responsibility: intermediaries and the First Amendment”. 76 *Geo. Wash. L. Rev.* 101 (2008) www.ssrn.com/abstract=1205674

no pueden morir, porque sin estos derechos seríamos mucho más vulnerables a ser discriminados (en el empleo, en el acceso al crédito, a los seguros o a la salud) sin ningún tipo de protección.

En el contexto del actual desarrollo de la sociedad de la información varios derechos están amenazados de muerte: en primer lugar el derecho al anonimato y a la expresión anónima, ya que la cantidad de datos que circulan ha dado lugar a la aparición de algoritmos matemáticos capaces de desanonimizar bases de datos. Estudios con bases de datos de prescripciones médicas han determinado que la probabilidad de desanonimizar datos de un paciente a partir del código postal y la fecha de nacimiento es de 69%, y si el paciente es mayor de 60 años esta probabilidad sube a 95%.⁵

La libertad de expresión también está en riesgo. Si bien es posible expresarse con más libertad, es muy difícil encontrar opiniones diversas, ya que la mayoría de las veces se sigue a una persona conocida mientras que los desconocidos continúan difícilmente accesibles. En este sentido la denominada “burbuja Google” atenta contra el derecho de audiencia, porque hace que los resultados de la búsqueda respondan a criterios de búsquedas anteriores, y elimina aquellos que podrían ser alternativos al pensamiento propio.

La protección de datos personales también está en riesgo, no necesariamente por los desarrollos tecnológicos, sino por las decisiones judiciales tanto en Europa como en las Américas, pues se ha instalado el criterio del “interés público predominante” para calificar un dato personal como “no protegido”. En 2001 el Comisionado de Privacidad de Canadá determinó que el nombre de un médico en una prescripción médica no es un dato personal protegido. En el mismo sentido, la Suprema Corte de EE.UU. consideró que existe un “interés corporativo pre-

5 Sweeney, L. 1997. “Weaving Technology and Policy Together to Maintain Confidentiality”. *Journal of Law, Medicine & Ethics*, 25, nos. 2&3: 98-110, www.data-privacy.org/dataprivacy/projects/law/jlme.pdf

dominante” para permitir el libre acceso a los nombres de los médicos.⁶ Estas decisiones ampliaron el ya instalado concepto de figuras públicas –y su consecuente pérdida de privacidad– a las figuras parcialmente públicas, que incluirían al menos a los profesionales, si se extrapola el paradigma de los médicos en el ejercicio de sus funciones.

En América Latina el derecho a la protección de los datos personales ha seguido el camino europeo en Argentina, Uruguay, México, Perú, Colombia y Costa Rica. En otros países las leyes todavía están en evolución. Las agencias de protección de datos de la región son aún muy débiles. Por ejemplo, en Argentina se han aplicado solo 25 multas en más de 12 años de vigencia de la ley, mientras que en España esa cantidad puede encontrarse en un solo día. Irónicamente, podría decirse, el impulso para crear leyes de protección de datos fue incentivado por acceder al mercado de trabajo de los *call centers*,⁷ más que por el desarrollo de un derecho fundamental (quizás con la excepción de México y Colombia).⁸

Si bien los ataques a los datos personales pueden venir tanto del Estado como de las empresas, los de las empresas son los más peligrosos. Esta afirmación suscita discusión –fundamentalmente porque los Estados manejan información sensible de los ciudadanos– sin embargo existe una diferencia cualitativa y es la existencia de leyes de acceso a la información gubernamental. En América Latina –con la excepción de Argentina– y

6 Sorrell v. IMS Health Inc., 23 de junio de 2011

7 Existen estudios que vinculan la expansión del mercado de *call centers* en Argentina a la certificación dada por la Comisión Europea como “nivel adecuado de protección” [Decisión 2003/490/CE]. En efecto las operaciones de un *call center off shore* (como por ejemplo las que derivan llamadas de un usuario en un país europeo a un centro de atención en Argentina) hacen un tratamiento de datos personales; una declaración de legislación equivalente daría a los usuarios las garantías de tratamiento.

8 Remolina, Nelson. 2013. “41 personas condenadas por el delito de violación de datos personales y 544 multas por infracción de la ley 1266 de 2008” 18-04-13 *Observatorio Ciro Angarita Barón* www.habeasdatacolombia.uniandes.edu.co/?p=980

en particular en México, las leyes de acceso precedieron a las de protección de datos, y han brindado a los ciudadanos la posibilidad de saber qué datos posee el gobierno. Téngase como ejemplo la destrucción en México de la base de datos RENAUT (Registro Nacional de Usuarios de Telefonía Móvil) ordenada por el Instituto Federal de Acceso a la Información y Protección de Datos para proteger la privacidad de los usuarios.⁹ Paradójicamente, desde 2003 en Argentina existe una ley que establece el libre acceso a la información ambiental, que incluye a las empresas privadas.¹⁰ En muchos casos los ciudadanos ignoran qué información sobre ellos poseen las empresas, y cómo y con qué finalidad está siendo utilizada. En este sentido, si no existe una autoridad garante de la protección de datos y si no se aplican sanciones económicas ejemplificadoras, ninguna empresa cambiará sus políticas.

En definitiva la protección de la vida privada y de los datos personales no está muerta, pero debe vivificarse. Eso depende de un discurso que sensibilice a los ciudadanos sobre lo necesario que son estos derechos para su vida cotidiana, y a las autoridades sobre el respeto de los derechos humanos y el estado de derecho.

9 “Destruye Segob bases de datos personales del Renault” 15-06-12 *Proceso* www.proceso.com.mx/?p=311021

10 República Argentina. Ley 25.831 *Régimen de libre acceso a la información pública ambiental*. www.infoleg.gob.ar/infolegInternet/anexos/90000-94999/91548/norma.htm

El espionaje en internet en América Latina

Katitza Rodríguez¹

Al desarrollo vertiginoso de la expresión en internet que hemos visto en la pasada década se suma ahora una explosión de la vigilancia de las comunicaciones. Las tecnologías pueden también abrir una caja de Pandora de intrusiones de los Estados con el fin de vigilar a la población que antes era inimaginable. Por ejemplo, internet y la telefonía celular ya no son plataformas en las que la comunicación privada esté a salvo de que los gobiernos sepan cuándo, dónde y entre quiénes ha ocurrido una comunicación. Las posibilidades que las nuevas tecnologías ofrecen para recopilar y analizar datos hacen que éstos se conviertan en señales de que uno está presente en la red. La Electronic Frontier Foundation (EFF)² considera que los metadatos (la información que registra las actividades individuales de comunicación) son tan confidenciales como el contenido de la comunicación y, por ende, merecen mayor protección en tanto derecho humano.

Por ello, a fines de 2012, EFF organizó un taller³ en el que una diversidad de expertos, periodistas, abogados y activistas de todo el mundo, y en particular de América Latina y el Caribe,

¹ Directora del Departamento de Derechos Internacionales de Electronic Frontier Foundation (EFF).

² Organización sin fines de lucro que lucha por los derechos de las personas en internet y trabaja para que ésta siga siendo abierta y libre. Fundada en 1990, tiene un único y simple objetivo: lograr que se respeten los derechos de todas las personas en el mundo de la red.

³ State Surveillance and Human Rights Camp wiki.surveillancehumanrights.org/Electronic_Surveillance_And_Human_Rights_Camp