Últimos avances en el reconocimiento de la privacidad digital como un derecho humano[1]

Valentina Maria Ariemme[2]

1. Nuevas fronteras del derecho a la privacidad en el Siglo XXI. El concepto de privacidad digital

El reconocimiento de la privacidad como derecho humano fundamental y su protección contra violaciones externas se remonta varias décadas atrás[3]. Sin embargo, el derecho a la intimidad goza de renovado interés desde 2013, pues actuaciones como la filtración de datos confidenciales, el espionaje internacional o la divulgación no autorizada de información han tenido un elevado impacto mediático, generando un importante debate político en numerosos países de todo el mundo.

Dichos acontecimientos han puesto de manifiesto los nuevos riesgos a los que se expone la privacidad personal en la era de internet, ocasionando un gran impacto, nacional e internacional, tanto en la opinión pública como a nivel político.

Uno de los debates más importantes tuvo lugar en el seno de la ONU, entre el Alto Comisionado de las Naciones Unidas para los Derechos Humanos (Navanethem Pillay) y los Estados miembros de las Naciones Unidas, las

[1] Cómo citar este artículo: Ariemme V.M., Últimos avances en el reconocimiento de la privacidad digital como un derecho humano, *Estudios Tributarios Europeos*, núm. 2/2014, (www.seast.it/revista), págs. 91-96.

[2] Valentina Maria Ariemme, Doctoranda en Derecho Tributario Europeo en la Universidad de Bolonia. Traducido por María del Carmen Cámara Barroso, contratada postdoctoral de la Universidad de Jaén.

[3] La Declaración Universal de los Derechos Humanos, proclamada por la Asamblea General de Naciones Unidas (ONU) el 10 de diciembre de 1948, establece, en su artículo 12, que "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*". Dos décadas después (en diciembre de 1966), también la ONU, en el Pacto Internacional de Derechos Civiles y Políticos, reprodujo, en su artículo 17.1 dicha afirmación en términos similares, añadiendo, en su epígrafe segundo, que "*toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*".

organizaciones internacionales y regionales y las organizaciones de derechos humanos[4].

Dichos debates culminarían en el Informe final de la oficina del Alto Comisionado, que, habiéndose publicado el 30 de junio de 2014, contiene una visión general sobre los principales aspectos objeto de debate.

El Informe parte del hecho de que el desarrollo y la difusión de las tecnologías de internet: "*[….] pueden mejorar el disfrute de los derechos humanos*". Sin embargo, al mismo tiempo, se afirma que "*[…] las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos*"[5].

Dentro del Informe subyace la convicción de que los derechos que se han reconocido tradicionalmente a los ciudadanos también deben ser protegidos online, especialmente teniendo en cuenta que las injerencias en el disfrute pacífico de dichos derechos, probablemente, son más fáciles, rápidas, sutiles y, además, difíciles de detectar y prevenir online.

2. Injerencias: límites, riesgos y protección

Tradicionalmente, la principal preocupación en torno a las injerencias a la privacidad proviene de aquellas actuaciones de los poderes públicos que afectan a la vida privada de los ciudadanos y limitan su pleno disfrute.

Aunque esto puede ocurrir con frecuencia en una sociedad democrática, las intervenciones del Estado no pueden ser ni arbitrarias ni ilegales[6].

[4] Toda la documentación relacionada con este asunto puede encontrarse en la página web de la ONU, www.un.org (véase, en particular, la Resolución adoptada por la Asamblea General el 18 de diciembre de 2013, n. 68/167. El derecho a la privacidad en la era digital) y en la página web del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. En la misma línea, véase también la página web del Observatorio de Derechos Humanos.

[5] *El Derecho a la privacidad en la era digital. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos* presentado en el 27º periodo de sesiones del Consejo de Derechos Humanos el 30 de junio de 2014.

[6] El artículo 8.2 del Convenio Europeo de Derechos Humanos establece que "*no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*".

Así, dichas injerencias solo pueden tener lugar en los casos previstos por la Ley, y, a su vez, la legislación nacional necesita cumplir una serie de requisitos para ser legítima desde una perspectiva internacional: ser consistente con los convenios internacionales; razonable y necesaria bajo determinadas circunstancias; y proporcional al objetivo perseguido.

El de proporcionalidad se ha convertido en un concepto fundamental, especialmente en los último años en relación con las medidas adoptadas para combatir el terrorismo y la adopción por parte de los gobiernos de medidas de vigilancia de masas por motivos de seguridad nacional.

En su informe, el Alto Comisionado reconoce que: "*[…] las tecnologías de comunicación digital pueden ser, y han sido, utilizadas por particulares con fines delictivos*" y que "*la vigilancia por motivos de seguridad nacional o para prevenir atentados terroristas u otros delitos puede ser un objetivo legítimo*".

Dicha afirmación no es suficiente: las medidas adoptadas por los Estados deben ser proporcionales ("el instrumento menos perturbador de los que permitan conseguir el resultado deseado"), de lo contrario, incluso aun teniendo un propósito legítimo y habiendo sido adoptadas de forma legal, pueden ser consideradas como ilegítimas.

En otras palabras, debe existir un cierto equilibrio entre las necesidades estatales y la salvaguarda de la privacidad.

También debemos hacer referencia al hecho de que habitualmente los gobiernos solicitan información a las empresas privadas para tener acceso directo a las comunicaciones e información personal de sus clientes, almacenando dicha información.

Tales medidas pueden dar lugar a un abuso de poder[7].

En consecuencia, es evidente que dichas violaciones son más frecuentes y menos fáciles de detectar y, por ello, más difíciles de proteger[8].

---

[7] En la rueda de prensa donde se presentaba el Informe (www.ohchr.org/SP/NewsEvents), se señaló por Navi Pillay (Alta Comisionada de las Naciones Unidas para los Derechos Humanos) que la retención obligatoria de datos de terceros era una constante en los regímenes de vigilancia de muchos estados, exigiendo los gobiernos que las compañías de teléfonos y los proveedores de servicios de internet almacenen datos de todas las comunicaciones y ubicaciones de sus clientes para el posterior acceso a los mismos de la policía y de las agencias de inteligencia, no siendo dicha práctica ni necesaria ni proporcionada.

Según el Alto Comisionado, las soluciones contra las violaciones de la privacidad a través de la vigilancia digital puede articularse a través de diferentes herramientas judiciales, legislativas o administrativas.

3. Las resoluciones del Tribunal de Justicia de la Unión Europea (TJUE) sobre la Directiva de Conservación de Datos

Las resoluciones del Tribunal de Justicia juegan un papel importante respecto a las posibles soluciones a las violaciones del derecho a la privacidad.

A este respecto, es importante tener en cuenta el reciente pronunciamiento del TJUE en los asuntos acumulados C-293/12 y C-594/12[9], que arroja luz sobre esta cuestión.

El Tribunal debía pronunciarse acerca de si la Directiva 2006/24, que fija la obligación de los proveedores de servicios de comunicaciones electrónicas a mantener durante un periodo determinado de tiempo los datos personales de sus clientes,[10] era compatible con el derecho a la privacidad regulado en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea[11] y en el artículo 8 del Convenio Europeo de Derechos Humanos; y

---

[8] Sobre este punto véanse dos artículos publicados en el *International Data Privacy Law: Oxford Journal* referidos al Informe del Alto Comisionado. El primero de ellos, que lleva por título "Systematic government access to private-sector data" (*International Data Privacy Law*, 2012, Vol. 2, N. 4), ofrece un análisis detallado de las diferentes cuestiones que nacen de la constante solicitud por parte de los gobiernos de acceso a los datos de los clientes, señalándose que incluso en los países donde las leyes de protección de datos son rígidas, la recopilación de datos por motivos de seguridad nacional van más allá de su ámbito de aplicación, constituyendo una excepción a lo dispuesto en las mismas. En abril de 2014, después del escándalo de la fuga de datos, se publicó una actualización de dicho artículo (*International Data Privacy Law*, 2014, Vol. 4, N. 1). Sobre el particular, véanse también las contribuciones realizadas por la asociación internacional sin ánimo de lucro *European Digital Rights*.

[9] TJUE, Sentencia C-293/12 y C-594/12, de 4 de abril de 2014.

[10] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

El artículo 5 enumera la categoría de datos que deben conservarse, incluyéndose los datos necesarios para rastrear e identificar el origen de la comunicación (p.e., número de teléfono, e-mail o número de usuario (ID) en internet).

El artículo 6 regula el periodo de conservación, que oscilará entre 6 meses y 2 años a partir de la fecha de la comunicación.

[11] El artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea (2010/C 364/01) (respeto de la vida privada y familiar) establece que "*toda persona tiene derecho al respeto*

si era compatible con el artículo 8 de la Carta, relativo a la protección de los datos personales.

En primer lugar, se trataba de dilucidar si la conservación de datos para su eventual acceso por parte de las autoridades nacionales competentes era una cuestión de interés general, confirmándose por el Tribunal[12].

Sin embargo, el objetivo de "seguridad nacional" no es suficiente: toda injerencia de las autoridades públicas deben respetar unos límites y, en particular, los derechos fundamentales de los ciudadanos. Por ello, la normativa de la Unión debe establecer en la Directiva "*[…] reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión*"[13]; habiendo encontrado el Tribunal algunas lagunas en este punto.

En primer lugar, el Tribunal señala que la Directiva no especifica una relación clara entre los datos que deben conservarse y la amenaza que constituyen para la seguridad nacional; en segundo lugar, no fija ningún límite al acceso a los datos personales por parte de las autoridades públicas; además, las garantías que presenta son insuficientes[14]. La conclusión del Tribunal es que, en su opinión, la normativa de la Unión Europea no cumple con el principio de proporcionalidad entre sus objetivos y sus medidas de aplicación, siendo, en consecuencia, inválida.

---

de su vida privada y familiar, de su domicilio y de sus comunicaciones". El artículo 8 (protección de datos de carácter personal) señala que: "*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente*".

[12] Sobre este particular, los fundamentos 33 y 34 de la Sentencia del Tribunal establecen que: "*a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, […] los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención de delitos y la lucha contra la delincuencia, en especial la delincuencia organizada […]. Por consiguiente, debe reconocerse que la conservación de datos para su eventual acceso por parte de las autoridades nacionales competentes […] responde efectivamente a un objetivo de interés general*".

[13] Véase el fundamento 54 de la Sentencia.

[14] Una vez señaladas las carencias de la Directiva en este punto, el Tribunal llega a la conclusión de que "*[…] no establece reglas específicas y adaptadas a la gran cantidad de datos cuya conservación exige esta Directiva, al carácter sensible de estos datos y al riesgo de acceso ilícito a ellos*". En uno de los últimos fundamentos de la Sentencia el Tribunal también hace referencia al problema de la territorialidad, señalando que "*[…] dicha Directiva no obliga a que los datos en cuestión se conserven en el territorio de la Unión*", lo que implica importantes problemas de control de su protección.

4. Conclusiones

En su Informe, el Alto Comisionado de la ONU, en numerosas ocasiones hace referencia a distintos pronunciamientos de los Tribunales europeos, señalando su eficacia en la identificación de problemas y la búsqueda de soluciones en este ámbito.

Sin embargo, entendemos que los Tribunales no pueden ser los únicos actores a la hora de buscar soluciones al problema colectivo de la violación de la privacidad digital.

Una mayor apertura de los Estados y la cooperación con los intermediarios privados son unos de los primeros pasos que deben darse; por el momento, esto es solo una declaración de intenciones y no una solución real.