EL DEBIDO PROCESO DIGITAL

Siete puntos para una agenda mínima de discusión sobre política criminal y tecnología en Argentina

APC
por los Derechos Civiles

Asociación por los Derechos Civiles

Diciembre 2019
adc.org.ar

Investigación y redacción: Eduardo Ferreyra
Diagramación: Matías Chamorro
Diseño de tapa: El Maizal

El debido proceso digital

Siete puntos para una agenda mínima de discusión sobre política criminal y tecnología en Argentina

La discusión sobre las garantías constitucionales en el proceso penal ha tenido un fuerte impulso luego de la aparición de las tecnologías digitales. Los hechos del mundo físico son diferentes de los fenómenos que suceden en el ámbito digital y, por eso, existe una tendencia creciente hacia la sanción de reglas específicas para abordar la problemática. El tema que despierta mayor interés es la regulación de la evidencia digital y de ciertas tecnologías de investigación que -si son mal utilizadas- pondrían en peligro, como mínimo, la privacidad de las personas.

En junio de 2018, la Argentina culminó el proceso de ingreso a la Convención de Budapest sobre Cibercrimen,[1] único documento legal internacional que aborda de manera específica, hasta el momento, el tema de la criminalidad informática.[2] Con este paso, el país cerraba el proceso de incorporación al convenio nacido en el Consejo de Europa. El tratado pretende abordar el fenómeno desde una óptica integral. Es por eso por lo que sus disposiciones abarcan cuestiones de derecho penal sustantivo, procesal y cooperación internacional. De este modo, se ocupa de establecer las conductas que deben considerarse como delitos, así como los poderes y facultades que las autoridades poseen para investigarlos.

El impacto del Convenio de Budapest sobre los derechos y garantías de las personas fue analizado en un documento anterior de la Asociación por los Derechos Civiles (ADC).[3] Allí se sugería que aquellos países que ya habían aprobado el instrumento enfoquen sus energías en la implementación de dicha normativa a través de la legislación interna. El objetivo de este esfuerzo debería dirigirse a establecer de manera más detallada las garantías que se encuentran insuficientemente previstas en el Convenio.

Antes, en abril de 2018, hubo un intento por parte del Senado de dar media sanción a un proyecto de reforma del Código Procesal Penal de la Nación, que incorporaba un capítulo sobre técnicas especiales de investigación. La iniciativa contemplaba un apartado para diversas medidas de vigilancia electrónica, acústica y de comunicaciones. Frente a este anuncio, organizaciones de defensa de derechos manifestaron su preocupación por la propuesta. En primer lugar, se hizo notar que el tratamiento exprés del proyecto impidió un debate amplio, robusto y con la participación de la sociedad civil.[4] En segundo lugar, hubo severos cuestionamientos

a aspectos sustantivos de la iniciativa. Así, desde la ADC sostuvimos que la reforma implicaba poner en manos del Estado la potestad de utilizar tecnología con capacidades altamente intrusivas de la intimidad de las personas sin haberse adoptado las garantías adecuadas.[5] En particular, nos despertó gran preocupación la autorización para recurrir a vigilancia remota sobre equipos informáticos. De este modo, se legitimaba el uso de software por parte de las autoridades para acceder de forma subrepticia a dispositivos electrónicos de los individuos.[6] Esta medida es particularmente peligrosa en tanto puede habilitar al Estado a acceder a los contenidos de una computadora, celular, tablet u otro aparato; o llevar adelante acciones de vigilancia en tiempo real (prender el micrófono o la cámara, hacer capturas de pantalla, activar el GPS, etcétera).

Finalmente, el proyecto fue sancionado sin la inclusión del capítulo sobre técnicas especiales de investigación. Sin embargo, el frustrado intento no significa que el debate haya quedado sepultado. En tanto las autoridades recurren con mayor asiduidad a herramientas tecnológicas para la investigación de crímenes, tarde o temprano surgirán otros intentos por dotar de una regulación específica. Es por eso por lo que desde la ADC presentamos los siguientes puntos para encarar una futura agenda de discusión con un enfoque que contemple una perspectiva de derechos.

1. Realizar un debate amplio y participativo como condición previa de legitimidad. La decisión de autorizar nuevos métodos de investigación y vigilancia supone por definición que el Estado tendrá más poder que antes. Por lo tanto, es necesario que haya una participación significativa de la sociedad en la discusión previa a la toma de una decisión de estas características. Esta exigencia se potencia en el caso de tecnologías digitales, ya que la complejidad de su funcionamiento implica por un lado que su capacidad de afectar derechos fundamentales es mayor y por el otro, que necesitamos el auxilio de especialistas para comprender qué riesgos presentan estas herramientas. De este modo, un requisito básico de legitimidad consiste en convocar a un debate lo más robusto posible antes de sancionar cualquier norma. La participación de la sociedad civil, especialistas en pericias informáticas y la comunidad técnica es central para sancionar una legislación que respete las garantías constitucionales.

2. Diseñar reglas cuyo objetivo sea equilibrar el desbalance entre Estado y ciudadanos producido por las herramientas digitales, El uso de este tipo de tecnologías por parte de las fuerzas de seguridad para actividades de vigilancia e investigación supone una significativa expansión del

poder estatal. Por lo tanto, es necesario aumentar las protecciones a los individuos con el fin de restaurar el balance de poder entre personas y gobierno que ya existía antes del surgimiento de estas técnicas. Bajo este enfoque, el establecimiento de salvaguardas legales específicas no es más que una forma de cumplir con el mandato constitucional de garantizar el debido proceso, la privacidad y demás derechos. En síntesis, se trata de recuperar el clásico equilibrio previsto por la Constitución para aplicarlo a la evidencia digital y la vigilancia electrónica.[7]

3. Repensar el concepto de privacidad: la noción de privacidad establecida en nuestra Constitución está fuertemente vinculada a la idea de propiedad sobre un espacio cerrado. El objetivo de la protección jurídica es resguardar al individuo de la mirada o la escucha de aquello que sucede dentro de su casa u otro ámbito reservado a su intimidad. En este sentido, la "autodeterminación informativa", base del derecho a la protección de datos personales, resulta un estándar más adecuado para afrontar la inmensa cantidad de datos recogidos por dispositivos de vigilancia en espacios públicos (cámaras, globos de vigilancia, drones o sistemas de reconocimientos facial). Asimismo, la "teoría del mosaico"[8] puede contribuir con esta visión al sostener que la recolección de grandes cantidades de información o el uso de dispositivos tecnológicos de investigación por largo tiempo (ej.: monitoreo a través de GPS) merecen un alto grado de escrutinio en tanto posibilitan la construcción de un "mosaico" de la personalidad del individuo. La razón es que estas tecnologías permiten acceder a detalles de las personas de maneras cualitativamente distintas de una observación tradicional. Herramientas conceptuales como las recién descriptas deben ser contempladas al momento de regular sobre el fenómeno digital.

4. Sancionar normativa específica para el tratamiento de datos personales por parte de las fuerzas de seguridad. Cualquier intento de regulación debería plantearse como objetivo el establecimiento de mayores límites para el manejo de las bases de datos que poseen las fuerzas de seguridad. Algunas de las medidas que se podrían incluir serían: la inclusión de plazos para la supresión de los datos personales o para su revisión periódica, a fin de evaluar la pertinencia de su almacenamiento; la distinción entre datos personales recabados en base a hechos, de aquellos que puedan derivarse de apreciaciones personales, opiniones, juicios de valor propios de los agentes que realizan las tareas de seguridad; la realización de evaluación de impacto en privacidad antes del uso de tecnologías invasivas, entre otras.

5. Prohibir o restringir al máximo la utilización de herramientas de hackeo estatal para investigación o vigilancia, Las técnicas de acceso remoto a equipos informáticos permiten que las fuerzas de seguridad pueden acceder de manera subrepticia –es decir, sin conocimiento de la persona investigada y de terceros ajenos a la pesquisa– a dispositivos electrónicos, como computadoras, smartphones, tablets, sistemas informáticos o bases de datos. Como tal, el hacking gubernamental es quizás la técnica de vigilancia más intrusiva debido a la gran cantidad de datos íntimos que almacenan nuestros equipos. Por lo tanto, la correspondencia de esta técnica con los derechos humanos se encuentra bastante cuestionada. Sin perjuicio de esto, en caso de que el Estado decida implementar esta técnica, debe hacerlo con las máximas garantías posibles. Esto incluye su autorización para una lista taxativa de delitos graves, dentro de un periodo de tiempo razonable y establecido con claridad, y siempre que los medios alternativos de investigación se revelen notoriamente ineficaces. Además, se deben establecer requisitos de transparencia para que su publiquen informes acerca de las operaciones y se permitan auditorías externas e independientes. Por último, la creación de autoridades de supervisión autónomas y transparentes sería un elemento crucial para garantizar los derechos de los individuos.

6. Proteger el cifrado de las comunicaciones. La adopción del cifrado punto a punto por parte de los servicios de mensajería constituye un elemento esencial para asegurar la privacidad de las comunicaciones. De esta manera, se contribuye a crear un ambiente en que los individuos tienen libertad para intercambiar información e ideas, sin que enfrenten la amenaza de vigilancia. A pesar de estos beneficios, distintos gobiernos del mundo están haciendo esfuerzos por lograr que las compañías permitan "accesos exclusivos" o "puertas traseras" a sus sistemas.[9] En este sentido, una agenda de reforma sería una excelente oportunidad para consagrar como ley la protección del cifrado, en particular, la prohibición de exigir a los servicios de mensajería la implementación de mecanismos que lo debiliten. De este modo, sería una gran señal de que no es intención de los poderes públicos la vigilancia de las comunicaciones cotidianas de los ciudadanos.

7. **Evitar usos de inteligencia artificial que puedan producir situaciones de discriminación y estigmatización.** La aplicación de inteligencia artificial (IA) para abordar cuestiones sociales puede impactar significativamente en grupos marginalizados. Los efectos perjudiciales de las decisiones algorítmicas se hacen sentir con mayor intensidad en las personas que

están en un especial estado de vulnerabilidad. Esta situación se vuelve preocupante en materia de política criminal. Una de las características de los sistemas penales -y el argentino no es la excepción- es su desproporcionada aplicación a sectores de bajos ingresos. En este sentido, el uso de algoritmos puede reforzar los estereotipos existentes. Un ejemplo de este fenómeno pudo verse en el uso del software PredPol por parte del Ministerio del Interior de Uruguay con el fin de identificar secciones de la ciudad donde hay más probabilidades que se cometan delitos. La tecnología fue cuestionada por organizaciones que sostuvieron que estas herramientas "tienden a replicar los sesgos de las bases de datos utilizadas para su entrenamiento, y que se utilizan para justificar la presencia policial en barrios marginados".[10] Otro caso se relaciona con la aplicación de reconocimiento facial en Brasil, que según investigadores ha resultado en que el 90 por ciento de las personas detenidas por esa tecnología son negras.[11] Para evitar que hechos de este tipo sucedan en Argentina, se debe restringir el uso de inteligencia artificial para el diseño de política criminal y de seguridad.

* * *

Notas

1 "Argentina joins the Budapest Convention" [Argentina se une a la Convención de Budapest], junio de 2018, disponible en https://www.coe.int/en/web/cybercrime/-/argentina-joins-the-budapest-convention (último acceso: 11/11/19).

2 Convención sobre cibercrimen, disponible (en inglés) en https://www.coe.int/en/web/conventions/full-list/- /conventions/rms/0900001680081561(último acceso: 11/11/19). Existe una traducción no oficial al español disponible en https://rm.coe.int/16802fa41c (último acceso: 11/11/19)

3 Asociación por los Derechos Civiles. *La Convención de Cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas,* marzo de 2018. Disponible en https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf (último acceso: 11/11/19).

4 Coalición por la Reforma Procesal Penal (ADC, ACIJ, APP, INECIP y CELS). "La reforma del código procesal amplía las facultades del estado para vigilar", 17 de abril de 2018, disponible en https://www.cels.org.ar/web/2018/04/la-reforma-del-codigo-penal-amplia-las-facultades-del-estado-para-vigilar/ (último acceso: 11/11/2019).

5 Asociación por los Derechos Civiles. *Reforma Espía. Comentarios a la regulación de nuevas técnicas de vigilancia en el proyecto de reforma*, abril de 2018, disponible en https://adc.org.ar/wp-content/uploads/2019/06/036-reforma-espia-04-2018.pdf (último acceso: 11/11/2019).

6 Ibid.

7 Cfr.Orin Kerr. "An Equilibrium-Adjustment Theory of the Fourth Amendment", 29 de octubre de 2011, disponible en https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1960984_code328150.pdf?abstractid=1748222&mirid=1&type=2 (último acceso: 13/11/2019)

8 Cfr. Paul Rosenzweig. "In defense of the Mosaic Theory", 29 de noviembre de 2017. Disponible en https://www.lawfareblog.com/defense-mosaic-theory (último acceso: 13/11/2019).

9 Asociación por los Derechos Civiles. "Limitar el cifrado no nos hará más seguros", 7 de octubre de 2019, disponible en https://adc.org.ar/2019/10/07/limitar-el-cifrado-no-nos-hara-mas-seguros/, (último acceso: 13/11/2019)

10 World Wide Web Foundation. *Algoritmos e Inteligencia Artificial en Latinoamérica,* septiembre de 2018, disponible en http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_AW.pdf (último acceso: 15/11/2019)

11 Folha de S. Paulo. "151 pessoas são presas por reconhecimento facial no país; 90% são negras", noviembre 2019, disponible en https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml (último acceso: 09/12/2019).


por los Derechos Civiles