EXAMEN PERIÓDICO UNIVERSAL – 4º CICLO

APORTE AL EXAMEN DE ARGENTINA

FALTAS DE CONTROL EN EL USO DE TECNOLOGÍAS PARA LA PREVENCIÓN DEL DELITO Y LA INVESTIGACIÓN CRIMINAL

1. El empleo de tecnologías digitales para la prevención del delito y la investigación criminal puede poner en entredicho derechos humanos como la libertad de expresión y la privacidad, entre otros, si no se cumplen con las debidas salvaguardas. En los últimos años, a pesar de los compromisos asumidos por el Estado argentino[1], se han observado problemas de distinto orden en la utilización de herramientas tecnológicas, como un uso extendido más allá de lo establecido en las normativas, la falta de publicidad y transparencia en los sistemas de contrataciones de empresas privadas y de acuerdos entre agencias estatales y la creación de regulaciones difusas, laxas y sin el marco de discusión necesarias

I. Los sistemas de reconocimiento facial en la Ciudad de Buenos Aires y la protección de datos personales

2. En el ámbito de la Ciudad de Buenos Aires, en el mes de abril de 2019, se puso en funcionamiento el Sistema de Reconocimiento Facial de Prófugos. Se dispuso que el mecanismo sería empleado *"únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires, como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC)*" (art. 2º del anexo de la resolución Nro. 398/MJYSGC/19). Se estableció que la información necesaria para dicha actividad sería entregada por autoridades del gobierno nacional, a través de los registros de la mencionada CONARC y los datos personales de las personas que integran ese registro que posee el Registro Nacional de las Personas (RENAPER). Se aclaró de manera expresa que estos últimos datos deben corresponder exclusivamente a quienes registren orden judicial de restricción de la libertad debidamente registrada (art. 3)

3. El 19 de noviembre de 2020, a su vez, en la Ciudad de Buenos Aires se sancionó la Ley nro. 6339, que modificó la Ley nro. 5688 (del Sistema Integral de Seguridad Pública de la Ciudad de Buenos Aires), y definió el sistema de reconocimiento facial de la siguiente manera: "el Sistema de Reconocimiento Facial de Prófugos tiene como objetivo la identificación y el reconocimiento de personas prófugas de la justicia basado en el análisis en tiempo real de imágenes de video". La norma limitó

[1] Ver A/HRC/37/5 Promesas y compromisos voluntarios “d) La Argentina se compromete a continuar promoviendo las reformas necesarias para lograr mejores niveles de transparencia, acceso a la información, confección de datos y estadísticas públicas a fin de tener un mejor conocimiento de la situación de los derechos humanos en el país”

el empleo del sistema a tareas requeridas por el Poder Judicial Nacional, Provincial o de la Ciudad de Buenos Aires, y a la detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (art. 480 bis de la Ley 5688).

4. En el marco de los debates legislativos en la Ciudad de Buenos Aires las organizaciones de la sociedad civil señalamos distintos reparos sobre el mecanismo de reconocimiento facial. Entre otros señalamos que el mecanismo puede generar detenciones arbitrarias con la consiguiente afectación de la presunción de inocencia, y que afecta el principio de igualdad y no discriminación, en tanto los softwares de reconocimiento facial han sido reiteradamente criticados por presentar sesgos en los márgenes de error en función del color, la etnia y el género de las personas. En el caso del CELS (integrante de ICCSI), ha dicho que el reconocimiento facial en las actividades de videovigilancia tiene potenciales riesgos sobre derechos tales como la privacidad, a la libertad de expresión y a la protesta. Además, agregó que se ha demostrado que esta tecnología tiene dificultades para distinguir personas de tez oscura, lo cual deriva en un sinnúmero de falsos positivos y afecta de forma desproporcionada a los grupos que ya se encuentran en situación de vulnerabilidad[2]. Por su parte, la Defensoría del Pueblo de la Ciudad de Buenos Aires, destacó la existencia de deficiencias en las bases del CONARC, y sostuvo que estos “errores” podrían haberse evitado si se hubiera hecho un estudio de impacto previo a la implementación del sistema que probara también la consistencia de la base utilizada. La Defensoría solicitó a la Corte Suprema que se subsanen los errores. Ese estudio de impacto aún no fue realizado y la CONARC sigue desactualizada.[3]

5. El Relator Especial de Naciones Unidas sobre el Derecho a la Privacidad, Joseph Cannataci, se refirió a estos inconvenientes -en el marco de una visita a la Argentina y con relación al sistema de la Ciudad de Buenos Aires-, y dijo "soy consciente de la necesidad de detener a las personas sospechosas de haber cometido delitos y llevarlas ante la justicia, pero no veo la proporcionalidad de instalar una tecnología con graves implicaciones para la privacidad para buscar en una lista de 46.000 personas que actualmente incluye a menores y delitos no graves y que no se actualice y compruebe cuidadosamente su exactitud... El hecho de que el reconocimiento facial se esté implementando sin el PIA (Evaluación de Impacto en la Privacidad) necesario, así como la consulta deseable y las fuertes salvaguardias, también es motivo de preocupación"[4].

6. En función de estos antecedentes y de las críticas al sistema de reconocimiento facial, organizaciones sociales impugnaron el sistema de reconocimiento judicial en la justicia. El Observatorio de Derecho Informático (ODIA) presentó un amparo colectivo, y otras organizaciones, adherimos a esa presentación. El proceso tramita en la justicia contencioso administrativo de la Ciudad de Buenos Aires.

---

[2]https://www.cels.org.ar/web/2020/10/la-legislatura-portena-debe-rechazar-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico/

[3] https://srfp.odia.legal/cels.pdf

[4] Ibídem, puntos 20 y 21.

7. En el marco de este proceso, se conoció que el Gobierno de la Ciudad de Buenos Aires accedió a los datos personales de carácter biométricos, que registra el Estado Nacional, a través del Registro Nacional de las Personas (RENAPER) de más de 7,5 millones de personas, cuestión que excede las habilitaciones normativas previstas para acceder a esa información. El Gobierno de la Ciudad tenía habilitación para acceder a los datos personales biométricos de aquellas personas que estuvieran en la base de datos de la CONARC (es decir, el registro de personas buscadas o prófugas de la justicia, que depende también del Gobierno Federal), que cuenta con alrededor de 40.000 personas.

8. La operatoria de acceso a tal volumen de información personal biométrica por parte del Gobierno de la Ciudad se realizó a partir de un convenio celebrado entre el Gobierno de la Ciudad (Ministerio de Justicia y Seguridad) y el Registro Nacional de las Personas (RENAPER). El convenio autoriza al Gobierno de la Ciudad de Buenos Aires a cruzar la base de datos personales biométricos de ese organismo con el listado de personas con orden de captura judicial para localizarlas a través de cámaras de seguridad equipadas con software de reconocimiento facial. Pero -como dijimos- el universo de personas buscadas contiene un número mucho menor, apenas por encima de los 40.000 hombres y mujeres, lo que implica una extralimitación en esas tareas de identificación que abarcaron a millones de individuos.

9. Esta situación que aún no ha sido aclarada ni explicada por las autoridades del Gobierno de la Ciudad de Buenos Aires ni tampoco por las autoridades del gobierno federal, pone en evidencia la falta de control sobre transferencias entre agencias federales y provinciales de la información biométrica que registra el Estado nacional, a partir de la identificación de personas para el otorgamiento del documento nacional de identidad. La normativa vigente de datos personales establece criterios laxos de transferencia de información entre agencias del estado (nacional y provincial).[5] Al mismo tiempo, las autoridades sobre la base de esta laxitud amplían las posibilidades de circulación de la información entre las agencias del Estado. Sobre estos ámbitos el Estado no ha desarrollado mecanismos de control y seguimiento sobre el uso y utilización de la información más allá de los fines por los que se recolectó, lo que pone en duda la capacidad de las personas sobre el control de la información personal y/o sensible que el Estado registra sobre ellas.

---

[5] Art. 11 de la ley 25.326, sobre datos personales. Dice lo siguiente: "1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo (…) 3. El consentimiento no es exigido cuando:... b) En los supuestos previstos en el artículo 5° inciso 2; **c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias**; 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

10. Además, en Argentina no sólo la Ciudad de Buenos Aires ha implementado un sistema de reconocimiento facial, también lo han hecho varias provincias y municipalidades (Gobiernos locales), sin control sobre los usos que hacen de ellas, el destino de la información acopiada, y el resguardo del derecho a la privacidad.

II. El uso de softwares para la investigación criminal sobre los que no hay información disponible por parte del Ministerio de Seguridad de la Nación

11. En noviembre de 2020, junto con una serie de organizaciones de la sociedad civil nucleadas en la Iniciativa Ciudadana para el Control de los Sistemas de Inteligencia (ICCSI) [6] realizamos un pedido de información relativo a los convenios celebrados por el Ministerio de Seguridad en el marco del Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos y de la Estrategia Nacional de Ciberseguridad. Además, requerimos la nómina completa de empresas y sus representantes con quienes el Ministerio de Seguridad de la Nación negocia convenios de cooperación para el intercambio de información, formación y cooperación en materia de tecnología para prevención de delitos y, en particular consultamos por el convenio para la utilización del software desarrollado por la empresa Cellebrite que, entre otros quince, fuera anunciado por dicho Ministerio a partir de un comunicado de prensa[7]. Con fecha 18 de diciembre de 2020, el Ministerio respondió que no se había concretado suscripción alguna de los convenios consultados.

12. El 10 de marzo de 2022 tuvo lugar una protesta social frente al Congreso de la Nación en oposición al acuerdo con el FMI que se estaba debatiendo en el recinto legislativo. En el contexto de dicha protesta un grupo de personas arrojaron piedras que causaron destrozos en el despacho de la vicepresidenta Cristina Fernández de Kirchner y en otras oficinas del Congreso Nacional. En el marco de las investigaciones judiciales para dar con las personas responsables de los disturbios, se hicieron públicas distintas noticias[8] que informaban sobre la utilización de un software de reconocimiento facial por parte de la Policía Federal Argentina dependiente del Ministerio de Seguridad de la Nación. De los portales web del Ministerio de Seguridad de la Nación y de la Policía Federal Argentina no surge información sobre el uso de herramientas de este tipo, pero a partir de una nota en

---

[6] La Iniciativa Ciudadana para el Control de los Sistemas de Inteligencia (ICCSI) es un espacio es un espacio destinado al seguimiento, impulso y promoción del funcionamiento efectivo de los mecanismos de control sobre el sistema de inteligencia de nuestro país, integrado por el Centro de Estudios Legales y Sociales (CELS), la Fundación Vía Libre, el Instituto Latinoamericano de Seguridad y Democracia (ILSED) y el Núcleo de Estudios de Gobierno y Seguridad de la Universidad Metropolitana para le Educación y el Trabajo (UMET).

[7] Acciones para mayor eficiencia en la investigación criminal en el ámbito digital. Disponible en: https://www.argentina.gob.ar/noticias/acciones-para-mayor-eficiencia-en-la-investigacion-criminal-en-el-ambito-digital

[8] "Identificaron a ocho sospechosos por el ataque al despacho de Cristina Kirchner" Disponible en: https://www.pagina12.com.ar/407956-identificaron-a-ocho-sospechosos-por-el-ataque-al-despacho-d "Piedras en el Senado: detuvieron a un sospechoso por el ataque a la oficina de Cristina Kirchner" Disponible en: https://www.ambito.com/politica/cristina-fernandez-kirchner/piedras-el-senado-detuvieron-un-sospechoso-el-ataque-la-oficina-cristina-kirchner-n5393547

la prensa escrita[9] se conoció específicamente el funcionamiento del software "Luna Plataform" para estos fines. Con fecha 28 de abril del corriente desde el mismo colectivo de organizaciones de la sociedad civil mencionado, enviamos un pedido de información al Ministerio de Seguridad de la Nación con el fin de solicitar información pública relativa a la adquisición y el uso por parte de esta cartera de un software de reconocimiento facial para la investigación criminal. La información brindada por el Ministerio no responde información básica como dar a conocer los términos del convenio con la empresa proveedora del software, los protocolos para su utilización, los sistemas de controles y los convenios de confidencialidad. Por otra parte, el ministerio tampoco responde con claridad sobre la existencia de otros software en uso por parte de las fuerzas de seguridad a su cargo.

III. Vigilancia en las redes sociales sin una clara regulación

13. En abril de 2020 el Ministerio de Seguridad de la Nación informó que, en el marco de las tareas de control de cumplimiento de las restricciones a la circulación impuestas para prevenir la difusión del virus Covid-19, se encontraba realizando tareas de ciberpatrullaje. Esta intervención se encontraba amparada en una resolución ministerial dictada en el año 2018 por la anterior gestión de gobierno[10]. Allí se instruía a las áreas de Ciberdelito de las fuerzas federales a "tomar intervención" en un conjunto definido de delitos a través de "actos investigativos" que debían realizarse en sitios digitales de acceso público. Así, esta norma habilitaba a realizar tareas de vigilancia y/o inteligencia en fuentes abiertas y redes sociales sin fijar un marco regulatorio preciso de estas acciones. No definía con claridad las características de los "actos investigativos" ni los escenarios en los que podrían iniciarse. Además, de la norma se infería que podría tratarse de actuaciones sin orden ni control judicial ya que según lo establecido en el artículo 2, una vez "reunidos los medios probatorios necesarios" se establecería el contacto con los funcionarios judiciales. La definición acotada de los delitos enumerados en la normativa parecía tener como objetivo impedir las tareas de vigilancia indiscriminada. Sin embargo, el carácter general y difuso de este instrumento generaba zonas grises al no aclarar qué tipo de decisión (y tomada por qué actor) es la que podría iniciar las intervenciones de las áreas dedicadas a los ciberdelitos.

14. Ante las críticas realizadas por distintas organizaciones, entre ellas el CELS[11], que señalaban que la medida podría habilitar una vigilancia masiva ilegal y que era preciso regular estas actividades, el Ministerio de Seguridad puso en circulación un proyecto de protocolo y convocó a una mesa de discusión. Allí se presentaron distintas propuestas para mejorar el proyecto inicial y finalmente en junio de 2020 fue aprobada y publicada en el Boletín Oficial[12] una nueva resolución. En esta

---

[9] "Exclusivo: los sospechosos y las pruebas de la investigación del ataque al Congreso por el acuerdo con el FMI" Disponible en: https://www.infobae.com/politica/2022/03/26/exclusivo-los-sospechosos-y-las-pruebas-de-la-investigacion-del-ataque-al-congreso-nacional-por-el-acuerdo-con-el-fmi/

[10] N° RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018

[11] Vigilancia en las redes sociales: pedimos información al ministerio de seguridad. https://www.cels.org.ar/web/2020/04/vigilancia-en-las-redes-sociales-pedimos-informacion-al-ministerio-de-seguridad-de-la-nacion/

[12] Resolución 144/2020 MINISTERIO DE SEGURIDAD. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=338229

oportunidad se buscó limitar la habilitación a tareas de vigilancia indiscriminada introduciendo la idea de “indicadores delictivos” y dejando a la Secretaría de Seguridad (y no de los propios policías) la tarea de definirlos, aunque nuevamente sin especificar cómo se realizará esa definición. Por otra parte, se dispuso que la vigencia de esta medida se extendería mientras dure la “emergencia pública” por la pandemia, hecho que genera una incertidumbre sobre la regulación de estas actividades una vez superada la crisis sanitaria, quedando en la actualidad pendiente la discusión de un marco normativo específico y permanente.

15. La nueva regulación estableció la creación de una Mesa Consultiva que, entre otras, tiene la función de evaluar el funcionamiento del protocolo y proponer modificaciones o disposiciones complementarias. En dicho espacio la Unidad de Gabinete de Asesores del Ministerio de Seguridad podrá solicitar opiniones y dictámenes, entre otros, a actores de la sociedad civil; y podrá, asimismo, invitarlos a participar de las reuniones de la Mesa Consultiva. Desde la creación de esta norma, el Ministerio de Seguridad ha desarrollado dos reuniones en julio y en septiembre del 2020 con presencia de organizaciones de la sociedad civil. En noviembre del 2020 las organizaciones que participamos de la Mesa Consultiva enviamos al Ministerio de Seguridad una propuesta de trabajo conjunto sobre la que no hubo respuesta. El 31 de mayo de 2021, desde este mismo colectivo de organizaciones enviamos un pedido de información para tener conocimiento de la aplicación de esta medida sobre la que tampoco el Ministerio emitió una devolución.

Recomendaciones al Estado:

1. La elaboración de directivas y reglas expresas por parte de la Dirección Nacional de Datos Personales y de la Agencia Federal de Acceso a la Información con relación al uso de datos personales de carácter biométrico para sistemas de reconocimiento facial en Argentina.

2. Promover normativa en los niveles federales y provinciales que establezcan como requisito para la puesta en funcionamiento y supervisión de mecanismos de reconocimiento facial de una “evaluación de impacto en privacidad”.

3. Establecer en la normativa que habilita el uso de sistemas de reconocimiento facial en Argentina mecanismos locales y federales de control periódicos sobre su implementación con un esquema de rendición de cuentas interpoderes y que incluya el monitoreo de la sociedad civil los.

4. Iniciar un proceso de discusión sobre la necesidad de una nueva ley de protección de datos personales y datos sensibles, que incluya los datos biométricos como parte de los datos personales que deben ser protegidos por el Estado cuando forman parte de registros o bancos públicos.

5. Establecer en una normativa con rango de ley el marco en el que los organismos de seguridad pueden realizar actividades de inteligencia criminal a través de la vigilancia e inteligencia de fuentes abiertas (OSINT) y particularmente de medios sociales (SOCMINT)

6. Reforzar el compromiso con las obligaciones de transparencia activa en virtud de la ley 27275 de acceso a la información y de las leyes de cada provincia y de la Ciudad de Buenos Aires.

7. Establecer normativamente la obligación de publicitar los procesos y términos de contratación, uso y capacitación de las tecnologías utilizadas para la prevención del delito y la investigación criminal