Abril 2023

Contribución a la Solicitud de aportes del mandato del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación

Lineamientos para el desarrollo de herramientas prácticas que ayuden a los órganos encargados de hacer cumplir la ley a promover y proteger los derechos humanos en el contexto de las protestas pacíficas

El Consejo de Derechos Humanos, en su 50º período de sesiones de junio del 2021 adoptó la resolución 50/21[1] por la que se encomendó al Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación a desarrollar "herramientas técnicas y prácticas específicas para ayudar a las fuerzas del orden a promover y proteger los derechos humanos en el contexto de las protestas pacíficas".

En este marco el Relator Especial publicó un llamado a aportes[2] con la finalidad de informar sobre el desarrollo de herramientas técnicas y prácticas específicas para ayudar a los órganos encargados de hacer cumplir la ley a promover y proteger los derechos humanos al tiempo que se facilitan las protestas pacíficas.

En virtud de la convocatoria efectuada a las múltiples partes interesadas, y tomando en consideración las preguntas guía, la Asociación por los Derechos Civiles extiende la presente contribución a la Relatoría Especial.

La Asociación por los Derechos Civiles (ADC) es una organización de sociedad civil con sede en Buenos Aires, Argentina que trabaja en la promoción y defensa de los derechos fundamentales. Desde el año 1995, la ADC focaliza sus actividades en el ámbito nacional con alcance regional e internacional en materia de libertad de expresión, acceso a la justicia, inclusión y diversidad, privacidad y protección de datos personales, entre otros.

En los últimos años, la ADC ha incorporado en su abordaje a las intersecciones entre los derechos humanos, las tecnologías y los entornos digitales. A través de su trabajo ha identificado que el incremento en el uso de tecnologías digitales en el Estado Argentino, ha resultado en prácticas lesivas para los derechos humanos por parte de operadores y operadoras del ámbito jurídico y de las fuerzas de seguridad.

A partir de la experiencia argentina, la presente contribución ilustra el estado de situación, a partir de tres cuestiones particulares: tecnologías de vigilancia, monitoreo de redes sociales y extracción de información de dispositivos móviles. Para luego, brindar recomendaciones a considerar en la creación de herramientas y la aplicación de las mismas de acuerdo a los estándares de derechos humanos.

Tecnologías de vigilancia

La utilización de tecnologías de vigilancia en Argentina ha crecido significativamente en los últimos años, como parte del diseño y ejecución de políticas estatales orientadas a la prevención del delito y la protección de la seguridad pública. En ese contexto, las injerencias en el derecho a la libertad de asociación y reunión se mantuvieron en un segundo plano, concebidas de algún modo como “el mal menor”, sin que ese criterio fuera consensuado con la ciudadanía.[3]

Dentro de las tecnologías de vigilancia, uno de los modelos más utilizados prevé la instalación de cámaras de seguridad, tanto en espacios públicos como privados, a los fines de monitorear la actividad que en ellos se desarrolla.[4] Esta práctica tiene como finalidad facilitar la intervención de las fuerzas de seguridad y el aparato judicial ante la detección de situaciones riesgosas para dichos lugares o para las personas que los frecuentan.[5] En un mismo sentido, el empleo de herramientas de recolección de datos biométricos tales como los sistemas de reconocimiento facial también han incrementado sustancialmente como parte de diversas políticas públicas.

En 2011, el Estado argentino creó el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), a cargo de la Policía Federal y bajo la supervisión del Ministerio de Seguridad de la Nación, con el fin de digitalizar las bases de datos de la Policía Federal y el Registro Nacional de las Personas (RENAPER). Es relevante señalar que este último organismo ya venía utilizando sistemas digitales de identificación desde 2009, recopilando a través de ellos datos biométricos, que incluyen huellas dactilares, huellas palmares y fotos de rostros, entre otros.[6]

Luego de la implementación de SIBIOS, la utilización de tecnologías de este tipo se fue expandiendo de manera paulatina a diversos sectores, a tal punto que, a hoy ya no integran únicamente estrategias de seguridad pública, sino que además se implementan para verificar identidades en el marco de programas de seguridad social, responsabilidades bancarias, educación y elecciones, entre otros.[7]

En los últimos años, la ADC se ha involucrado en el monitoreo y el estudio de políticas públicas basadas en la identificación de las personas mediante tecnologías biométricas, para advertir sobre los riesgos derivados de su potencial injerencia en derechos fundamentales, particularmente en la

privacidad y la libertad de expresión.[8]

A partir de este análisis se advierte también que estas herramientas se utilizan con escasa transparencia, omitiendo información sobre cómo funcionan los mecanismos utilizados para el manejo de los datos biométricos y quiénes tienen acceso a los mismos. El problema se agrava teniendo en cuenta que los marcos normativos tienden a ser insuficientes para dar respuestas a la complejidad que encarna la utilización de estas tecnologías.[9]

Complementariamente, la ADC ha expresado en reiteradas oportunidades su preocupación por la expansión de estas tecnologías en función de la seguridad pública, ya que su implementación se traduce ineludiblemente en una tendencia al control y la vigilancia de los espacios de acceso público. Para reflejar esta situación, desde la organización se impulsó la campaña “Con mi cara no”, con el objeto de crear conciencia sobre los riesgos que trae aparejados la tecnología de reconocimiento facial.[10]

Como componente específico para profundizar esta campaña a nivel federal, la ADC desarrolló “El mapa de la vigilancia”, en el que se identifican las provincias y los municipios dentro de Argentina en los que la ciudadanía corre el riesgo, actual o futuro, de que su rostro sea captado por cámaras de vigilancia con sistemas de reconocimiento facial incorporados. [11]

Esta iniciativa pone de relieve aspectos ciertamente cuestionables en lo relativo a los sistemas de reconocimiento facial, como el uso encubierto de los mismos, prescindiendo del consentimiento de la ciudadanía, y la excesiva confianza que se deposita en ellos, al punto de inferir que toda persona es culpable hasta que un algoritmo demuestre lo contrario, que en términos de debido proceso supone una inversión arbitraria de la carga de la prueba.[12]

Dentro del territorio argentino, la Ciudad de Buenos Aires es una de las

localidades con mayor ponderación de los sistemas de reconocimiento facial, reflejando una clara predisposición al control de los espacios públicos.

En 2019, el Gobierno puso en práctica el "Sistema de Reconocimiento Facial de Prófugos" (en adelante SRFP) mediante una resolución administrativa. De esta manera se introdujo una herramienta de enorme impacto en el ejercicio de los derechos fundamentales sin dar lugar a la intervención parlamentaria correspondiente.

Esta situación se modificó a mediados de 2020 a través del proyecto de ley N° 1686-D-2020, presentado en la legislatura con el objetivo de reformar la Ley N° 5.688 del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires.[13]

Desde el punto de vista de la afectación de derechos, es imprescindible mencionar que al poco tiempo de la implementación del SRFP, se registraron casos de personas identificadas erróneamente como prófugas de la justicia, y detenidas en diferentes espacios de la vía pública en calidad de sospechosas por delitos que no habían cometido. Uno de los casos más resonantes fue el de Guillermo Federico Ibarrola, que pasó seis días privado de su libertad luego de haber sido detenido en una terminal de ómnibus de la ciudad. Su detención se produjo a raíz de un alerta errónea del sistema de reconocimiento facial que lo vinculó a un hecho de robo ocurrido en otra localidad, con el que Ibarrola no tenía relación alguna.[14]

En este punto, no se puede obviar que la imprecisión de la tecnología es muchas veces tendenciosa, puesto que se alinea con la producción de sesgos, y en consecuencia habilita la toma de decisiones discriminatorias y de alto impacto en el ejercicio de derechos en perjuicio de grupos minoritarios. [15]

Otra de las críticas más contundentes a este sistema fue la omisión de una

evaluación de impacto, que habría permitido advertir afectaciones como las mencionadas, mediante un análisis de la viabilidad del SRFP en concordancia con los principios de necesidad y proporcionalidad, que son dos aspectos claves para legitimar toda restricción a derechos fundamentales.[16]

En el contexto de una creciente incorporación de herramientas tecnológicas de vigilancia en la Ciudad de Buenos Aires, sin los recaudos correspondientes, se tornó imprescindible la creación de la "Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia", que se consolidó a mediados de 2022.[17] Así, finalmente se le dio respuesta al reclamo de numerosas organizaciones de la sociedad civil que junto a la ADC, mostraron su preocupación por las irregularidades al interior de la justicia en el mecanismo de reconocimiento facial. [18] Cabe aclarar que la incorporación de esta comisión estaba prevista inicialmente como parte de la regulación del sistema de reconocimiento facial, y hasta ese entonces pendiente de cumplimiento por parte del parlamento porteño.

En lo que respecta a las características de composición y funcionamiento de la Comisión, es preciso dejar en claro que la ADC no considera asegurados los niveles suficientes de experticia e independencia. Por lo tanto su configuración actual no puede ser considerada una buena práctica. Sin embargo, el ejemplo puede ser utilizado para brindar recomendaciones acerca de cómo debería ser un organismo de supervisión efectivo.

Aquí se puede mencionar más concretamente la importancia de prever una composición multisectorial para la comisión de control, incluyendo organizaciones de la sociedad civil y otros grupos de expertos en la temática. Esto no se da en el caso de la Ciudad, ya que la integran únicamente legisladores locales.[19]

Complementariamente, es preciso asegurar la independencia de la comisión de control, ya que este factor guarda una estrecha relación con la fiabilidad de sus observaciones y recomendaciones. En vista de la presencia exclusivamente legislativa en el caso de la Ciudad de Buenos Aires, este aspecto parece quedar relegado, especialmente teniendo en cuenta que la regulación y el monitoreo de los sistemas de reconocimiento facial se encuentran bajo la órbita del mismo órgano.

Retomando el análisis de la pertinencia de las tecnologías de vigilancia, cabe recalcar que la ADC considera que no son propias del espacio público, por lo que no debería naturalizarse su utilización como un instrumento de control. No obstante, es fundamental acompañar la implementación práctica de aquellas que ya han sido desplegadas con mecanismos adecuados para la mitigación de riesgos.

En los casos mencionados en el presente apartado, el aumento en la utilización de las tecnologías de vigilancia produjo cuestionamientos en cuanto a la legitimidad, legalidad, modo de regulación e implementación de las mismas, así como a la falta de transparencia y rendición de cuentas estatal en relación a ellas. Más aún teniendo en cuenta el rol de garante que posee el Estado en relación al cumplimiento de los derechos humanos, y la consecuente responsabilidad de asegurar que el desarrollo tecnológico sea compatible con los mismos.[20]

En conclusión, las críticas alojan una demanda de coherencia al sector público, que debe dar el ejemplo en cuanto al cumplimiento de los estándares exigidos a otros sectores a la hora de monitorear la implementación de tecnologías de vigilancia. Esto quiere decir que si bien los organismos estatales pueden valerse de las facilidades que ofrece la tecnología a la hora de implementar sus políticas públicas, deben ser los primeros en asumir el compromiso de conducirse en un

marco de respeto por los derechos y garantías fundamentales de la ciudadanía.

Monitoreo en redes sociales

El monitoreo de las redes sociales es la práctica que engloba el seguimiento, la recopilación y el análisis de la información compartida en dichas plataformas por parte de fuerzas de seguridad y de operadores y operadoras judiciales. La recolección de información incluye, por ejemplo, el monitoreo de contenidos publicados y compartidos por usuarios y usuarias en grupos o páginas públicas o privadas y la obtención de todos los demás datos presentes en una determinada plataforma (incluyendo datos de comportamiento).[21] El acceso de las fuerzas de seguridad se realiza sin la necesidad de contar con credenciales especiales, una diferencia notoria respecto a otras prácticas como la extracción de información de dispositivos inteligentes mediante la utilización de software como se verá más abajo.[22]

El monitoreo se realiza a través de la utilización de un conjunto de técnicas y tecnologías como pueden ser: la revisión manual del contenido publicado; el análisis de búsquedas realizadas por usuarios y usuarias, *hashtags*, grupos, entre otras; el rastreo de las actividades o tipos de contenido publicado por ellos y ellas; el uso de herramientas de *scraping* para extraer contenido en una página web; e incluso la sistematización de alguna o varias de las técnicas anteriores mediante distintos tipos de software.[23]

De esta manera, las tecnologías empleadas permiten un monitoreo continuo de redes sociales a gran escala, una práctica que no sería posible de ser realizada por individuos de forma manual. Por lo tanto, representa un serio riesgo de vigilancia masiva de grupos en situación de vulnerabilidad o de determinados tópicos que se busque monitorear, sobre todo si incluye herramientas para

analizar e interpretar la información recolectada en tendencias y patrones de actividades.[24]

En el caso de Argentina, las fuerzas policiales han utilizado estas técnicas en formas que afectan la libertad de expresión y la protesta social.[25] En el 2020, se cuestionó específicamente el uso de las mencionadas prácticas durante la pandemia de la COVID-19[26] por encontrarse contrariadas directamente con disposiciones vigentes de la Ley de Inteligencia Nacional.[27] De esta manera, las fuerzas policiales no deben llevar adelante vigilancia masiva de manera indiscriminada, sin una individualización de personas presuntamente sospechosas por la comisión de tipos penales determinados.

En concurrencia con la mencionada situación el Estado argentino elaboró un "Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas"[28] con el objetivo de regular la actividad policial en redes sociales mientras esté vigente la emergencia sanitaria. La presentación del documento fue realizada en una reunión junto a organizaciones de defensa de derechos humanos[29] donde se invitó a los presentes a realizar aportes y consideraciones a tener en cuenta.

El protocolo dispuso en su artículo 2 que: "Las tareas de prevención del delito en el espacio cibernético se llevarán a cabo únicamente mediante el uso de fuentes digitales abiertas", entendiéndose a éstas por: "medios y plataformas de información y comunicación digital de carácter público no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias."[30]

La ADC envió un aporte[31] al Ministerio de Seguridad sobre la mencionada disposición donde sostuvo que la discusión sobre la temática debe realizarse de

manera amplia, robusta y participativa. Esto significa la necesaria intervención de todos los sectores que pueden ser alcanzados por las técnicas en cuestión y que la discusión no debe guiarse de manera exclusiva por la situación de emergencia. Por otra parte se resaltó que es imperioso que este tipo de disposiciones provengan de un órgano legislativo para asegurar así el cumplimiento del principio de legalidad.

Además, la ADC marcó otras consideraciones como la tipicidad de la conducta antijurídica en relación a derechos que se encuentran en conflicto como el de la libertad de expresión y el derecho a la protesta. Además es de destacar la importancia de una correcta delimitación de los tópicos que puedan estar incluidos en este tipo de monitoreo. La falta de precisiones en este punto afecta en primer lugar al principio de legalidad porque de manera previa y certera no fueron informados en qué situaciones podrá darse la intervención policial. En segundo lugar se encuentra limitado el principio de proporcionalidad en tanto la ausencia de pautas específicas otorga un extenso margen de discrecionalidad para decidir los delitos que requerirán la utilización de estas técnicas.

El protocolo además fue cuestionado por la Agencia de Acceso a la Información Pública (AAIP)[32] quién sostuvo que la norma no especifica cómo las tareas de ciberpatrullaje funcionarán en la práctica; ni en particular (i) qué categorías de datos se recolectarán, (ii) cómo se asegurará que la información recopilada sea fiable, y (iii) qué consecuencias tendrá el tratamiento de los datos para sus titulares. Por este y otros motivos, la AAIP recomendó que el Protocolo sea suspendido hasta que sea revisado para adecuarlo a los estándares del derecho humanos a la privacidad.[33]

Luego del establecimiento del protocolo se realizaron mesas consultivas integradas por autoridades del Ministerio de Seguridad, organizaciones sociales, organismos de derechos humanos y representantes del Congreso de la

Nación.[34] La finalidad de estos encuentros fue establecer una agenda de análisis y monitoreo de las investigaciones policiales realizadas en el marco de la pandemia del Covid-19. Además resultaron una oportunidad para que las organizaciones presentes manifestaran inquietudes respecto al software utilizado y al seguimiento de la situación judicial sobre las personas afectadas.

Actualmente el protocolo no se encuentra vigente,[35] el Estado argentino consideró que ya no se configuraba la situación excepcional[36] que dio sustento a la aplicación de la medida. De todas maneras, y contemplando los más de dos años de vigencia, resulta aún más imperiosa la necesidad de tomar decisiones sobre la utilización de este tipo de prácticas con una necesaria reflexión sobre qué situaciones fácticas abarca, de qué modo y con un constante diálogo con la protección de los derechos de la ciudadanía. En particular, el proceso contó con instancias consultivas a sociedad civil y organismos que no fueron suficientes para abordar un debate que resulte en decisiones constitutivas sobre los cambios propuestos. En este sentido, para que sean consideradas buenas prácticas, las propuestas de mesas consultivas o los llamados a contribuciones deben estar acompañadas de una planificación de puesta en acción de las discusiones y aportes que se realicen.

Extracción de información de dispositivos móviles.

Las herramientas de extracción forense de dispositivos móviles permiten a las fuerzas policiales, agencias gubernamentales y empresas privadas acceder a la información disponible en un teléfono celular, incluso si los datos se han cifrado, eliminado o cargado a la nube.[37]

En los últimos años se ha reportado el uso de estas herramientas para investigar y perseguir a personas y manifestantes en diversas regiones conocidas por tomar medidas contra la disidencia política y la comunidad LGBTIQ+.[38] Hay

evidencias, además, de que estás tecnologías han presentado vulnerabilidades que podrían poner en duda la fiabilidad y seguridad de la información obtenida a partir de las mismas.[39]

En la Argentina, estás son algunas de las dependencias que utilizan estas herramientas: Gendarmería Nacional Argentina, Policía Federal Argentina, Policía de Seguridad Aeroportuaria, Ministerio Público de la Ciudad Autónoma de Buenos Aires, Policía de la Ciudad Autónoma de Buenos Aires, Ministerio Público de Salta, Ministerio Público Fiscal de Santiago del Estero, Gabinete Científico del Poder Judicial de Chaco, Ministerio Público de Chubut, Ministerio Público de la Provincia de Buenos Aires, Ministerio Público de Córdoba, Ministerio Público de Jujuy y Ministerio Público de Santa Fe.[40]

A través de la utilización de estas prácticas se accede a fotos, videos, agendas, contactos, detalle de lugares visitados, registro de llamadas, mensajería, resúmenes bancarios, correos electrónicos, notas personales y aplicaciones de todos los tipos, tanto de los y las titulares del celular como de terceros. En consecuencia, resulta evidente la vulneración al derecho a la privacidad de las personas y a que, posiblemente, el Estado abuse de las mencionadas prácticas de extracción y análisis de datos limitando la garantía del debido proceso de la ciudadanía.

Actualmente, en Argentina, no existe regulación específica sobre el momento y la forma de utilización de las herramientas de extracción forense para teléfonos celulares dentro del proceso judicial. Ante la ausencia de regulación toma especial relevancia la interpretación judicial, es decir, lo que los jueces y las juezas y operadores judiciales deciden en los casos concretos que les toca resolver. Teniendo en consideración, las diferencias que puedan surgir incluso ante situaciones similares, se pueden ver afectados principios jurídicos tales como el de legalidad, limitación de la finalidad, exactitud y calidad, conservación

limitada, seguridad de los datos y confidencialidad, tanto para las personas imputadas como para terceras personas cuya información también se encuentra en sus celulares.

Recomendaciones y buenas prácticas

Perspectiva integral de derechos humanos - Marco legal

Es necesario establecer un marco legal acorde a las nuevas formas de criminalización de la protesta, obtención de prueba e investigación durante los procesos judiciales y ante la actuación de las fuerzas de seguridad. En virtud de una perspectiva integral de protección de derechos humanos, los marcos normativos no podrán disminuir el ejercicio de los mismos ni utilizar formas legales que no cumplan con los altos estándares internacionales establecidos.[41]

Es fundamental, evitar el uso desproporcionado de figuras penales existentes en la aplicación de situaciones no antes contempladas para continuar asegurando el derecho de las personas a manifestarse. La criminalización de acciones legales y legítimas puede resultar en la estigmatización de las personas que participan en la protesta. Los estándares de derechos humanos nos indican que únicamente puede ser perseguido aquel discurso que esté dirigido a producir una acción ilegal inminente y que cuente con posibilidades ciertas de hacerlo.

El marco normativo que dé lugar al establecimiento de tecnologías en herramientas y prácticas de vigilancia deberá respetar los procesos democráticos de discusión en cumplimiento del principio de legalidad. Es menester respetar el rango legislativo de las disposiciones y el rol del Poder Legislativo como el órgano encargado de regular razonablemente los derechos fundamentales que se encuentran en tensión en las mencionadas situaciones.

Las disposiciones legislativas deberán poseer precisión a la hora de regular el

uso de las tecnologías fijando límites claros en virtud de la necesidad y la proporcionalidad de la herramienta en cuestión. En este sentido, tanto la finalidad de la implementación como aquellas excepciones que permitan cualquier tipo de exceso deben ser taxativas y eludir al máximo la utilización de conceptos ambiguos que den lugar a confusiones o interpretaciones que perjudiquen los derechos de la ciudadanía.

Finalmente deberá contemplarse prioritariamente la seguridad de los datos personales a la hora de administrar las tecnologías de vigilancia y monitoreo, especialmente teniendo en cuenta que de la mano de la creciente sofisticación de las mismas viene un incremento sustancial en la cantidad y la variedad de los datos personales recolectados, y por ende una mayor responsabilidad en cuanto al resguardo de estos.

Evaluación de impacto

La implementación y planificación de políticas públicas que incluyan acciones de vigilancia y monitoreo de la ciudadanía deben incluir evaluaciones de impacto en derechos como parte de los procesos de debida diligencia. Estas consisten en un análisis minucioso de las herramientas a implementar, a los fines de determinar las posibilidades reales o eventuales de vulneración de los derechos humanos como consecuencia de las mismas, y diseñar estrategias de prevención o mitigación de esos riesgos.[42]

Debido proceso

La utilización de las prácticas y herramientas deben realizarse en el marco de un debido proceso penal respetuoso de los derechos humanos de todas las partes afectadas, garantizando su confiabilidad y asegurando que la evidencia obtenida sea de calidad. Se deben detallar específicamente estándares de procedimiento y funcionamiento de las herramientas utilizadas para garantizar su debido

control y la posibilidad de oponerse ante una manipulación y/o utilización errónea y/o ilegal.

Transparencia

En un escenario como este, la transparencia en cuanto a los alcances de los mecanismos disponibles debe ser parte del compromiso que asuman los Estados, así como la rendición eficaz de cuentas cuando se produzcan afectaciones a la privacidad de los y las titulares de los datos.

Establecer sistemas transparentes implica conocer la elección de la tecnología o mecanismo a utilizar y la contratación por parte de los Estados. Además incluye conocer cómo funcionan los procedimientos mediante los cuales las fuerzas de seguridad y de la ley pueden acceder a la información. Aunque estas herramientas están protegidas por secreto comercial, debe existir un equilibrio frente a garantizar el derecho de defensa y la privacidad de las personas.

La admisibilidad de estas herramientas en un proceso judicial debe estar condicionada a que se garantice una metodología confiable y que los resultados que se obtienen no hayan sido alterados. Además, los informes deben incluir un porcentaje sobre el margen de error en el que puede incurrirse en el uso de estas tecnologías. Los márgenes de error deben ser considerados por las autoridades a los fines de valorar la información y estar disponibles para las y los afectados. Además, como principio aplicable a los datos personales en general, la información extraída y que no es relevante debe conservarse limitadamente, y debe existir una directiva clara sobre su eliminación permanente.

Supervisión y monitoreo

Dada la complejidad que encarnan las tecnologías de vigilancia, es fundamental

añadir a la identificación previa de los riesgos una instancia de control continuado para advertir afectaciones en el marco de la utilización de las mismas. Esto puede sintetizarse en la creación de una comisión externa de supervisión y mesas consultivas que evalúen el funcionamiento de las herramientas tecnológicas empleadas para la vigilancia, y se expidan ante las inconsistencias con el marco normativo y las afectaciones a los derechos de la ciudadanía.

Resulta fundamental para garantizar el funcionamiento eficaz de esta instancias, prever la multisectorialidad en la composición, incluyendo miembros de la sociedad civil y organizaciones expertas en materia de tecnología y vigilancia. Adicionalmente, de la independencia en estos espacios dependerá en gran parte la fiabilidad de sus decisiones. Por lo tanto, es esencial que su integrantes no provengan en su totalidad de un mismo sector u organismo.

Capacitación y formación

Las características propias de las herramientas de extracción de información requieren una capacitación permanente para integrantes de fuerzas de seguridad y para operadores y operadoras judiciales especialmente respecto al funcionamiento, riesgos y finalidad del uso.

Además debe garantizarse siempre la intervención significativa humana durante los procedimientos para garantizar la protección de las personas frente a la toma de decisiones arbitrarias ante el reemplazo de técnicos y técnicas forenses por sistemas semi automatizados de decisión.

Notas

1. Resolución aprobada por el Consejo de Derechos Humanos el 8 de julio de 2022. (s. f.). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/406/53/PDF/G2240653.pdf?OpenElement
2. Solicitud de Aportes del Especial sobre los derechos a la libertad de reunión pacífica y de asociación https://www.ohchr.org/en/calls-for-input/2023/call-inputs-development-practical-tools-assist-law-enforcement-bodies
3. ADC. Avanza la regulación del reconocimiento facial en la Legislatura porteña. (2020)
4. Lio, V. G. Cámaras de seguridad y prevención del delito: La utilización de la videovigilancia en la ciudad de Buenos Aires (2015)
5. Appiolaza, M.*Gian Guido Nobili: las cámaras de seguridad no reducen el miedo al delito.* (2022)
6. ADC Tecnologías de Vigilancia en Argentina. (2021)
7. Ibid.
8. ADC "Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina" (2019)
9. Ibid.
10. Impulso Baires "Con mi cara no: La campaña creada por ADC para concientizar sobre la tecnología de reconocimiento facial" (2021)
11. https://conmicarano.adc.org.ar/
12. TN " 'Con mi cara no': una campaña alerta sobre el uso de reconocimiento facial en las calles argentinas" (2021)
13. ADC. Avanza la regulación del reconocimiento facial en la Legislatura porteña. (2020)
14. El País "Seis días arrestado por un error del sistema de reconocimiento facial" (2019)
15. ADC. Avanza la regulación del reconocimiento facial en la Legislatura porteña. (2020)
16. Ibid.
17. Télam-Agencia Nacional de Noticias. Crearon una comisión de seguimiento del sistema de vigilancia biométrica (2022)
18. DHyTecno "Se creó una comisión de seguimiento para el sistema de vigilancia biométrica de la Ciudad de Buenos Aires" (2022)
19. Télam-Agencia Nacional de Noticias. Crearon una comisión de seguimiento del sistema de vigilancia biométrica (2022)
20. ADC ¿Cómo implementar la debida diligencia en derechos humanos en el desarrollo de tecnología? (2020)
21. ADC. Guía de Protesta (2021)
22. ADC. Seguidores que no vemos – Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT). (2018)
23. ADC. El Examen Periódico Universal: una oportunidad única para mejorar la situación de los derechos humanos en Argentina. (2022)
24. Privacy International. Social Media Intelligence, (2017)
25. Para más información referirse a: ADC. El Examen Periódico Universal: una oportunidad única para mejorar la situación de los derechos humanos en Argentina. (2022)
26. Perfil. Nota periodística sobre declaraciones de la Ministra de Seguridad (2020)
27. La Ley de Inteligencia Nacional Nº 25.520 En su artículo 4to, incisos 2 y 3, señala que ningún organismo de inteligencia podrá "obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción" (inc.2); ni tampoco "influir de cualquier modo en la situación

institucional, política, militar, policial, social y económica del país...en la opinión pública, en personas, en medios de difusión o en asociaciones o agrupaciones legales de cualquier tipo." (inc.3).
28. Ministerio de Seguridad. Resolución 144/2020 "Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas" (2020)
29. Página 12 El "ciberpatrullaje" en la mira de los organismos (2020); Infobae Los detalles del protocolo de "ciberpatrullaje" que impulsa el Gobierno: qué busca regular y cuáles son los puntos más cuestionados (2020)
30. Artículo 2
31. ADC Sobre la necesidad de una ley para regular la investigación en fuentes abiertas y redes sociales. (2020)
32. Autoridad de protección de datos personales de Argentina
33. Agencia de Acceso a la Información Pública Respuesta a Nota -2020-41096462-APN-UGA-MSG - Mesa Consultiva para la evaluación y seguimiento del Protocolo General para la Prevención Policial del Delito con uso de Fuentes Digitales Abiertas (2020)
34. Ministerio de Seguridad Se reunió por primera vez la Mesa Consultiva para prevenir delitos con fuentes digitales abiertas (2020)
35. Ministerio de Seguridad de la Nación. Resolución 720/2022 (2022)
36. Del considerando de la Resolución 720/2022: "Que el artículo 3° del mencionado protocolo establece como finalidad "la prevención policial del delito en el espacio cibernético cuyo acaecimiento sea previsible en función de la pandemia" y, por ello, la vigencia del documento se encuentra sujeta a la duración de la emergencia sanitaria."
37. ADC¿Quién revisa tu teléfono? Parte II. (2022)
38. Hong Kong.Human Rights Activists Urge Israel to Stop Spy Tool Exports to Hong Kong Police.(2020) Venezuela. Despite Sanctions, Israeli Firm Cellebrite Sold Phone-hacking Tech to Venezuela. (2020) Rusia Rusia habría utilizado software israelí para hackear teléfonos de los manifestantes de Moscú. (2019) Etiopía Ethiopia Obtains Phone-hacking Tech From Israeli Firm Cellebrite (2022) Uganda Israeli Firm Cellebrite Sold Phone-hacking Tools to Uganda's Brutal Dictatorship (2022)
39. Signal Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective. (2021) Benjakob, O. Sensitive FBI, Interpol Info Leaked From Israeli Firm Cellebrite, Court Documents Show.(2022)
40. ADC ¿Quién revisa tu teléfono?. (2021)
41. Argentina ha ratificado distintos instrumentos internacionales que protegen la libertad de expresión y la libertad de asociación como la Declaración Universal de Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Civiles y Políticos; y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, entre otros
42. ADC ¿Cómo implementar la debida diligencia en derechos humanos en el desarrollo de tecnología? (2020)