Datysoc
LABORATORIO DE DATOS Y SOCIEDAD

Consulta para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212

Documento elaborado por Patricia Díaz
Co-cordinadora del Laboratorio de Datos y Sociedad | Datysoc

Cuestiones previas

Realizamos algunas sugerencias relacionadas con la estructura del documento:

- Dado que será un documento de una extensión considerable, sugerimos generar un índice con hipervínculos para mejorar su navegabilidad y usabilidad.
- Sugerimos colocar al final de cada línea un punteo con un resumen en el que figuren de forma específica y clara las recomendaciones de regulación.

Autorización: se autoriza al equipo de Agesic a copiar, adaptar y/o incorporar cualquier parte de este documento en la versión final que se presentará al Parlamento, sin necesidad de cita.

1. ¿Cuáles son las recomendaciones específicas que podría realizar desde su experiencia para promover las líneas definidas en el presente documento?

Expresamos que, de forma genérica estamos de acuerdo tanto con el análisis planteado como con los aspectos priorizados y con los lineamientos generales de la propuesta que se presenta en el borrador “Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212”. Aunque existe un aspecto central que el documento omite abordar de forma explícita y clara, se trata de una pregunta que seguramente varios legisladores tengan en mente: ¿Necesitamos una regulación general de la IA o debemos regular determinados usos de la IA o su uso en determinados sectores?

Entendemos que aún no están dadas las condiciones para una regulación generalista basada en la determinación de diferentes niveles de riesgo, la asignación de obligaciones diferenciadas para cada uno de esos niveles de riesgo y en la creación de nueva institucionalidad especializada para la IA. Hace falta entender mejor el panorama para regular, por eso **proponemos recomendar a los parlamentarios la creación de un foro para promover las líneas definidas en el presente documento, detectar otras prioridades a nivel nacional y formular recomendaciones por parte de diferentes actores sociales para una regulación adecuada y sostenible**.

De forma paralela a esta discusión, **sugerimos centrar los actuales esfuerzos regulatorios en la actualización del cuerpo normativo nacional vigente y en la regulación de los actuales usos de la IA por parte del gobierno que impliquen alto riesgo**.

De esta forma, y sin descartar la posible existencia de otros emergentes, destacamos al uso policial de la IA como un emergente de alto riesgo que amerita urgente regulación y proponemos la creación de una nueva línea: "*Linea uso de IA con fines de vigilancia policial y como prueba en el proceso penal*" (ver pregunta 4).

2. ¿Existen deficiencias o incongruencias desde el punto de vista regulatorio que impacten en los aspectos evaluados en las líneas definidas en el presente documento y no hayan sido considerados?

A continuación presentamos algunos aspectos que no han sido considerados en el documento y que entendemos deberían ser agregados:

Apartado "3. Línea Derechos Humanos"

Proponemos agregar las siguientes consideraciones en el apartado "**3.3 Diagnóstico preliminar en materia de IA y Derechos Humanos** ":

Sobre la Ley 18331 de Protección de Datos Personales (LPDP) y el Decreto 64/020.

Estamos de acuerdo con las apreciaciones del documento borrador en cuanto a que se deberían revisar los Arts. 13 y 16 de la LPDP. Entendemos que estas disposiciones no son suficientes por los siguientes motivos:

1) Derecho a la impugnación de valoraciones personales basadas en tratamiento automatizado de datos (Art. 16) sólo opera en el contexto de datos personales, aunque existe una infinidad de contextos en los que no opera. Un ejemplo ilustrativo: el mecanismo previsto en el Art. 16 no podría utilizarse para impugnar y obtener información de un sistema de IA que analice los datos de contaminación del agua y del aire en el que se entienda que está en riesgo la salud de un conjunto de ciudadanos.
2) El Art. 16 sólo habilita la impugnación de decisiones "**cuyo único fundamento** sea un tratamiento de datos personales". Basta con "colocar un humano en el medio" y decir que el sistema "asesora" pero que el humano toma la decisión para que caiga la aplicación del artículo. Frente a los conocidos "sesgos de automatización"[1] debería considerarse incluir alguna disposición que defina el concepto de "supervisión humana significativa"

[1]Informe "Hacia una supervisión significativa de los sistemas automatizados de toma de decisiones" (2022). Digital Future Society. Disponible en: https://digitalfuturesociety.com/es/report/hacia-una-supervision-significativa-de-los-sistemas-automatizados-de-toma-de-decisiones/

incluyendo aspectos mínimos requeridos como la formación de los actores que operan el sistema entre otros factores.

3) No debemos olvidar que los mecanismos de la LPDP y del Decreto 64/020 no consideran la protección de datos personales como un derecho colectivo, por lo que, en base a estas disposiciones, tampoco podrá exigirse a ninguna institución pública o privada que rinda cuentas sobre parámetros básicos de explicabilidad de sus sistemas automatizados frente a un riesgo potencial sobre los derechos fundamentales.
4) En el Decreto 64/020 los sujetos obligados no tienen obligación de publicar sus evaluaciones de impacto, sólo están obligados a compartirlas con la URCDP si de la evaluación surge un riesgo potencial y significativo (Art. 7).
5) Los Arts. 13 y 16 de la LPDP no especifican cuáles son los requisitos exigidos para que se configure la explicabilidad y no exige trazabilidad ni auditabilidad, por lo que se satisface esta obligación cuando la propia administración presenta explicaciones de forma unilateral.
6) Se necesitan normas que garanticen un mínimo de **transparencia, interpretabilidad y auditabilidad algorítmica** (Stoyanovich, Julia 2020)[2] entendiendo que:
    - **La transparencia algorítmica no es sinónimo de liberar el código fuente**,la publicación del código fuente ayuda, pero a veces es innecesaria y a menudo insuficiente. En algunos casos, la exigencia de liberar el código fuente puede resultar excesiva o lesionar derechos.
    - **La transparencia algorítmica requiere transparencia de datos**, la explicabilidad sólo puede lograrse en contexto de datos, los datos que se usan para el entrenamiento y testing, los datos que se van a usar para la implementación y validación del sistema (datasets de referencia), datos sobre performance y precisión del sistema. La transparencia de datos es necesaria para todos los sistemas automatizados, no solo para sistemas basados en *Machine Learning*.
    - **La transparencia de datos no es sinónimo de hacer públicos todos los datos**, deben liberarse los datos siempre que sea posible; en caso de no ser posible (por cuestiones de protección de datos, confidencialidad, propiedad intelectual, por ejemplo) también se puede: publicar las metodologías de selección o recopilación, acudir a conjunto de datos sintéticos, publicar resúmenes estadísticos o muestra, los datos que se utilizaron para el preprocesamiento, la procedencia de los datos e información sobre su calidad/representatividad y las fuentes conocidas de sesgo relevadas.

[2] Stoyanovich, Julia (2020). TransFAT. Translating fairness, accountability, and transparency into data science practice. Disponible en: https://pdfs.semanticscholar.org/061f/de41f92e6bd408b5722428bdcc8b2a7d0858.pdf

- **La transparencia procesable requiere interpretabilidad o comprensibilidad**, en definitiva, se trata de explicar los supuestos y efectos del sistema (no solo los detalles de operación) y de involucrar al público - técnico y no técnico.

Sobre la Ley 18381 de Acceso a la Información Pública (LAIP).

La LAIP debería incluir una disposición que introduzca el **derecho a ser informado sobre qué decisiones se toman de forma automatizada o con apoyo de un sistema automatizado por parte de la administración pública** y sobre cómo funcionan estos sistemas (tomando en cuenta lo expresado en el apartado anterior en relación a la transparencia, interpretabilidad y auditabilidad algorítmica y la conceptualización de "intervención humana significativa").

También debería incluirse una disposición que garantice el derecho a la interacción humana y presencial con la administración pública.

Apartado "4. Línea propiedad Intelectual"

Proponemos agregar las siguientes consideraciones en el apartado "**4.1 Consideraciones preliminares**":

> Actualmente, la mayoría de las actividades de desarrollo IA requieren el uso masivo de grandes volúmenes de datos y suelen incluir el uso de miles de imágenes, audios, textos, etc. protegidos por derechos de autor con fines de análisis computacional o entrenamiento de modelos. Entre estos usos podemos encontrar la aplicación de técnicas de minería de texto y datos (como el crowling, scraping y parsing), la creación de copias técnicas o efímeras con fines de entrenamiento de modelos, entre otras. De esta forma, para incentivar la innovación y generar un entorno jurídico seguro para investigadores y desarrolladores locales, se hace necesario incluir en las leyes de derechos de autor una excepción que habilite el uso de obras con fines de análisis computacional. Esta excepción debería incluir como restricción la condición de que esos usos no compitan con la normal explotación de las obras y que no dañen de forma injustificada los intereses de los autores.
>
> Tomando en cuenta que el software y las bases de datos también están protegidas por derechos de autor y por medidas de protección tecnológicas, será necesario regular de forma clara las relaciones entre los derechos de autor, el secreto comercial y la auditabilidad de los sistemas. La auditabilidad de los sistemas de IA es de especial interés público tanto por razones de ciberseguridad como de transparencia y explicabilidad y, muchas veces, requiere la vulneración de medidas de protección tecnológica para el ingreso

a los sistemas, la realización de copias de prueba o las actividades de ingeniería inversa.

Proponemos agregar las siguientes consideraciones en el apartado "**4.2 Selección de antecedentes internacionales**":

En cuanto a las excepciones al derecho de autor con fines de análisis computacional, el antecedente más reciente en el contexto de la OMPI es el informe sobre "Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor" (2023)[3]. Dicho informe fue solicitado a Raquel Xalabarder por el Comité de Derechos de Autor y Conexos (SCCR/OMPI) y en él la autora expresa:

> *"El papel de la lectura no humana (mecánica), como el análisis de inteligencia artificial (IA), está cobrando cada vez más importancia dentro de las metodologías de investigación. La minería de textos y datos (TDM) ha ganado protagonismo gracias a las tecnologías digitales. Gracias a las herramientas de TDM, los investigadores extraen información de una gran variedad de obras protegidas, desde trabajos académicos hasta música y publicaciones de prensa*." (traducción nuestra)

En ese mismo informe encontramos un Anexo con ejemplos de normas nacionales que contienen este tipo de excepciones al derecho de autor para actividades de investigación con fines de análisis computacional que ya están presentes en casi todas las legislaciones del Norte Global.

En cuanto a las excepciones al derecho de autor y a las medidas de protección tecnológica con fines de auditabilidad de los sistemas encontramos el informe del Grupo de Trabajo sobre Seguridad en la Economía Digital de 2022 de la OCDE[4]. En este informe se expresa que "*la ley de derechos de autor puede infringirse cuando la información divulgada contiene partes del código de software protegido por derechos de autor. Dicha protección de derechos de autor podría restringir el intercambio de información sobre vulnerabilidades con el proveedor original, lo que dificulta la implementación de las DCV-Difusión Coordinada de Vulnerabilidades- en muchos casos.*" En el documento se explica que la falta de actualización de las excepciones al derecho de autor y a las medidas de protección tecnológica implican riesgos legales para los auditores e investigadores de seguridad digital, y también se expresa que estas normas son usadas para amenazar con procedimientos jurídicos por parte de los propietarios del software que se pretende investigar.

[3] Xalabarder, Raquel (2023). "Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor". Disponible en: https://www.wipo.int/meetings/es/doc_details.jsp?doc_id=621815

[4] OECD (2022). OECD Policy Framework on Digital Security. Disponible en: https://www.oecd.org/publications/oecd-policy-framework-on-digital-security-a69df866-en.htm

Proponemos agregar las siguientes consideraciones en el apartado "**4.3 Diagnóstico preliminar en IA y Propiedad Intelectual**":

> La Ley de Derechos de Autor de Uruguay (Ley 9.739) no prevé excepciones al derecho de autor (ni al régimen de medidas de protección tecnológica) que habiliten el correcto desarrollo de las actividades de análisis computacional ni de auditorías, ya sea con fines de seguridad o con fines de explicabilidad. Es por eso que resulta necesario incluir una nueva excepción en el Art. 45 de la Ley de derechos de autor (Ley 9739) que habilite el uso de obras con fines de análisis computacional. También se sugiere agregar una excepción al derecho de autor (y a las medidas de protección tecnológica) para posibilitar el ingreso, copia y análisis de los sistemas con el fin exclusivo de permitir instancias de auditabilidad cuando un juez u otra ley así lo requiera. Estas excepciones deberán explicitar que quedan estrictamente prohibidos los usos competitivos o que perjudiquen injustificadamente al autor o titular de los derechos sobre las obras.

3. ¿Ha identificado potenciales mejoras o modificaciones a la regulación vigente que puedan colaborar en el desarrollo de la IA en Uruguay?

---

4. ¿Existen otros aspectos que no encuentra considerados y que deban analizarse?

A continuación se propone la inclusión de una nueva línea que constituye el mayor **emergente de uso de IA con alto riesgo de vulneración de los derechos fundamentales en Uruguay**, por lo que debería ser analizada de forma independiente y **amerita urgente regulación**:

Linea uso de IA con fines de vigilancia policial y como prueba en el proceso penal.

Consideraciones preliminares:

El uso de la IA con fines de prevención del delito y seguridad pública pone en riesgo los derechos de los ciudadanos por su potencial de discriminación y por tratarse de una tecnología altamente intrusiva, más allá de los posibles sesgos o fallos que impliquen riesgos de discriminación. Algunas de las preocupaciones

principales en torno al uso de estos sistemas por parte de la policía y en la justicia criminal son[5]:

La vulneración de la presunción de inocencia. El derecho a la presunción de inocencia en los procesos penales es un derecho humano fundamental. Sin embargo, el creciente uso de la IA en el ámbito de la justicia penal, y más especialmente el uso de vigilancia biométrica a distancia y de ciertos tipos de software policial predictivo, plantea interrogantes sobre el alcance de este derecho y sobre cómo deben construirse y utilizarse los sistemas de IA para protegerlo.

La preservación de la igualdad procesal y el debido proceso. Una de las principales preocupaciones planteadas en los estudios sobre determinados sistemas de IA es que resultan inaccesibles para un escrutinio adecuado por parte de los acusados y sus abogados. Esto tiene graves implicaciones para el principio de igualdad de medios procesales y el derecho a un proceso contradictorio, porque sin información sobre cómo se toma una decisión, es difícil prever cómo pueden los acusados cuestionar la exactitud y legalidad de la decisión. En este sentido, uno de los principales problemas que impiden la impugnabilidad suficiente de los sistemas de IA en los procesos penales es la falta de notificación. Si a una persona no se le notifica que ha sido objeto de una decisión automatizada por parte de un sistema de IA, no tendrá la posibilidad de impugnar dicha decisión, ni la información en la que se basó la decisión. A su vez, el fenómeno de las cajas negras es otro factor de riesgo en la aplicación de la IA ya que, para preservar el debido proceso y el derecho de igualdad procesal, el sistema y sus resultados deberán ser necesariamente explicables y libres de sesgo de forma demostrable.

La falta de formación obligatoria de los actores del sistema judicial: la formación de los actores del sistema judicial es imprescindible para determinar la admisibilidad y realizar una correcta valoración de los medios de prueba digital, además de dar sentido al concepto de “intervención humana significativa” en el contexto judicial. La formación no sólo es necesaria para los usuarios primarios de los sistemas de IA, como jueces y policías que los utilizan para fundamentar sus propias decisiones. La formación también debe estar disponible para los abogados de la defensa penal, para que estén en mejores condiciones de impugnar los sistemas de IA, cuando sea necesario.

Selección de antecedentes internacionales

El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de la ONU en su informe “La vigilancia y los derechos Humanos” (2019)[6] propone medidas drásticas. Hace un llamado urgente a

[5] Policy Paper: Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU (2022). Fair Trials. Disponible en: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf

[6] Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. «Informe sobre la vigilancia y los derechos humanos», A/HRC/41/35. (Asamblea General

establecer "*una moratoria inmediata sobre la venta y la transferencia a nivel mundial de los instrumentos que utiliza el sector de la vigilancia privada hasta que se establezcan estrictas salvaguardias de los derechos humanos en la regulación de esas prácticas y se pueda garantizar que los gobiernos y los agentes no estatales van a utilizar esos instrumentos de un modo legítimo*." y también solicita "*una regulación más rigurosa de las exportaciones de equipos de vigilancia y unas restricciones más estrictas de su utilización*".

En el "Reglamento de Inteligencia Artificial de la UE" (Art. 5 del Capítulo II "Prácticas de Inteligencia Artificial prohibidas")[7] **se prohíbe** el uso para aplicaciones policiales o de orden público de la identificación biométrica en tiempo real en lugares accesibles al público por parte de las fuerzas y cuerpos de seguridad, **salvo** en estos casos: búsqueda de víctimas potenciales de delitos; prevención de amenazas específicas y sustanciales sobre infraestructuras críticas o sobre personas físicas; prevención de ataques terroristas; y persecución de crímenes punibles con más de cinco años de privación de libertad. Antes será obligatorio valorar la probabilidad y escala del daño posible sin esos sistemas y del daño que esos podrían ocasionar; mediara **autorización judicial** o administrativa vinculante; y se impondrán limitaciones temporales, geográficas y personales.

Otro antecedente importante es la "Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales" [8]. Esta resolución aborda el uso de la inteligencia artificial (IA) en el ámbito del derecho penal, centrándose en su aplicación por parte de las autoridades policiales y judiciales. El documento subraya la necesidad de establecer un marco regulatorio robusto que garantice el respeto de los derechos fundamentales, la privacidad y la protección de datos. Además, enfatiza la importancia de la transparencia, la supervisión humana y la responsabilidad en el uso de sistemas de IA para prevenir sesgos y discriminaciones. La resolución también insta a que se realicen evaluaciones de impacto y auditorías regulares de estos sistemas para asegurar su conformidad con los estándares éticos y legales de la Unión Europea.

En esta Resolución, el Parlamento Europeo destaca el potencial de la IA para mejorar la eficiencia y eficacia en la lucha contra la delincuencia, pero también advierte sobre los riesgos asociados, como la posibilidad de errores judiciales y la

de las Naciones Unidas, 28 de mayo de 2019). Disponible en:. https://www.undocs.org/es/A/HRC/41/35

[7] Reglamento de Inteligencia Artificial de la Unión Europea aprobado por Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024 Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

[8] Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

violación de derechos humanos. La resolución propone la creación de un marco legal específico para el uso de la IA en el ámbito penal, que incluya directrices claras sobre la recopilación y el procesamiento de datos, así como medidas para garantizar la equidad y la no discriminación. Además, recomienda que las autoridades y profesionales del derecho reciban formación adecuada sobre el uso y las implicaciones de la IA, asegurando así una aplicación justa y segura de estas tecnologías en el sistema judicial.

Diagnóstico preliminar

El Ministerio del Interior ha venido construyendo un ecosistema de vigilancia automatizada en apoyo al cumplimiento de sus cometidos basada tanto en IA como en otro tipo de sistemas. Este ecosistema no ha sido acompañado por la debida regulación ni por criterios de transparencia proactiva que aporten confianza sobre su funcionamiento. No existe ninguna regulación relacionada con el uso policial de los sistemas recientemente adquiridos por el Ministerio del Interior. Por ejemplo, el de reconocimiento facial automatizado, el software UCINET (software de inteligencia sobre fuentes abiertas como redes sociales), el sistema ShotSpotter (sistema que implica la colocación de micrófonos en las calles para que una IA detecte disparos) o inclusive un software de analítica de cámaras para "determinar conductas sospechosas que puedan advertir al policía antes de que se produzca el delito".

En Uruguay, el control del uso de las bases de datos personales utilizadas en las actividades de "seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito" no están alcanzadas por las obligaciones que establece la Ley 18331 de Protección de Datos Personales (LPDP Art. 3 Lit. B y Art. 25)[9].

Con respecto al software de Reconocimiento Facial Automatizado (RFA) que el Ministerio del Interior adquirió en febrero de 2020 vía licitación pública, resaltamos que esta adquisición se encuentra relacionada con la aprobación de la creación de una base de datos de identificación facial para su tratamiento con fines de seguridad pública a cargo de la Secretaría del Ministerio del Interior (arts. 191 y 192 de la Ley de Presupuesto 2020). De esta forma se habilita el uso de las fotografías de rostros (e información asociada a ellas) de las cédulas de identidad y los pasaportes de la base de la Dirección Nacional de Identificación Civil (DNIC) para crear una base biométrica con una finalidad diferente a la de identificación. Son muchas las cuestiones que surgen de esta contratación y habilitación masiva para el uso de

[9] "No obstante, cabe indicar que, aun en los casos indicados en el párrafo anterior, se ha interpretado por parte de la URCDP que igualmente resultan aplicables con carácter general los principios de la protección de datos personales" Ver consulta al Consejo Ejecutivo de la URCDP publicada en: Informe "Fuera de Control. Uso policial del reconocimiento facial automatizado en Uruguay". Datysoc (2022), pag. 49. Disponible en: https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

datos biométricos de toda la población ¿Con qué fines exactos es que se contrató el sistema?, ¿Quién autoriza el uso del sistema de RFA?, ¿Cómo se auditará el uso del sistema?, ¿Cómo se controlará el acceso al sistema?, ¿Cómo debe proceder un oficial ante un match biométrico en los diferentes contextos de uso?, ¿Cuándo puede aceptarse un match biométrico como prueba?, ¿Cómo se valorará esta prueba?, ¿Cómo se abordará la posibilidad de sesgos en el sistema?, ¿Cuándo y cómo se informará al imputado de la existencia de este tipo de prueba?, ¿Cómo se abordarán las diferencias entre un match biométrico en ambiente controlado y uno en ambiente no controlado?, ¿Cómo se eliminarán estos datos personales cuando ya no sean necesarios? Nada de esto se ha definido aún y la mayoría de estas decisiones **deberían fijarse a través de normas de rango legal precisas y públicamente accesibles**.

También vale la pena destacar que ni en el Código del Proceso Penal o en la Ley de Procedimiento Policial contamos con ninguna regulación sobre admisibilidad o valoración de la prueba digital, ni con protocolos públicos sobre el uso de la IA adquirida por el Ministerio del Interior, ni con la formación de los actores judiciales en torno al funcionamiento de esta IA.

Recomendaciones regulatorias sobre el uso policial de la IA

Siguiendo las recomendaciones de la Relatoría de Libertad de Expresión de la ONU, se sugiere imponer una moratoria en la adquisición de software de vigilancia hasta que no exista una base legal que regule adecuadamente el ecosistema de vigilancia policial.

Con el objetivo de establecer una regulación estricta sobre su uso y brindar garantías contra los actos discriminatorios y contra su uso abusivo o arbitrario deberían introducirse las modificaciones necesarias en el Código del Proceso Penal y en la Ley de Procedimiento Policial para regular el tema de forma adecuada, incluyendo:

- La obligación de realizar un análisis de impacto (en lo posible público) sobre los derechos fundamentales antes de adquirir soluciones de IA con fines de vigilancia, así como conocer y declarar de antemano los fines exactos para los que se contrata.
- Establecimiento de líneas rojas en cuanto a qué usos están estrictamente prohibidos a la policía y qué usos requieren orden judicial,
- La posibilidad de exigir la auditabilidad y explicabilidad algorítmica, la trazabilidad, protocolos de control de acceso y la descripción de responsabilidades detalladas sobre quienes usan estos sistemas de vigilancia.
- El entrenamiento adecuado de los funcionarios policiales, jueces y fiscales sobre el funcionamiento y limitaciones del sistema mediante una certificación obligatoria.

Recomendaciones específicas relacionadas con vigilancia biométrica y reconocimiento facial:

- La prohibición del enrolamiento masivo de toda la población en el sistema de reconocimiento facial adquirido por el Ministerio del Interior. Esto implica la derogación de los arts. 191 y 192 de la Ley de Presupuesto 2020, estos artículos violan el principio de presunción de inocencia.
- La prohibición del uso de vigilancia biométrica en tiempo real y sin orden judicial en espacios públicos.
- Los mecanismos obligatorios de análisis de impacto y de evaluación de riesgo junto con mecanismos de rendición de cuentas y seguimiento.
- Regulación específica de la admisibilidad, valoración y diligenciamiento de los matches biométricos como métodos de investigación y como prueba digital.