LIBERTAD VS. SEGURIDAD: NUEVAS TENSIONES A PROPÓSITO DEL CIBERPATRULLAJE Y LA CREACIÓN DE LA UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD[*]

Por Marcelo Alfredo Riquert[1]

Sumario: 1. Introducción. 2. Los nuevos límites al ciberpatrullaje. 3. La nueva UIAAS y sus funciones. 4. Balance provisorio. 5. Anexo documental: I. Resolución 428/2024 del Ministerio de Seguridad. II. Resolución 710/2024 del Ministerio de Seguridad. III. Prácticas de IA prohibidas según la LIA europea.

1. Introducción

Llamaba la atención recientemente Javier A. De Luca sobre un dato de la realidad al que a veces no prestamos la atención debida. En efecto, nos decía que la democracia argentina no es la misma que a fines de 1983, pero no sólo por los cambios jurídicos e institucionales que se fueran sucediendo, sino porque han cambiado las bases de la interacción humana debido a las nuevas formas de comunicación impuestas por las modernas tecnologías[2].

Y es así. Lo vivimos en los recientes procesos electorales y se trata de algo que se proyecta sobre nuestra cotidianeidad sin que a veces lo percibamos cabalmente. Desde el Ministerio de Seguridad de la Nación, a través de dos resoluciones de la ministra, Dra. Patricia Bullrich, se han tomado decisiones de singular trascendencia que podría decirse han sido pasadas por alto sin que las preceda una necesaria discusión pública ni tampoco que cobre vuelo una vez conocidas[3]. Sin embargo, ambas pueden tener alto impacto en la

---

[*] Artículo originalmente publicado en el blog del autor, a quien se agradece por autorizar su reproducción https://riquertdelincuenciainformatica.blogspot.com/2024/08/libertad-vs-seguridad-nuevas-tensiones.html.

[1] Abogado y Doctor en Derecho (UNMDP). Máster de Derecho Penal (U. Salamanca, España). Director del Área Departamental Penal y de la carrera de posgrado "Especialización en Derecho Penal" (categorizada "A", por la CONEAU), Facultad de Derecho, Universidad Nacional de Mar del Plata.

[2] De Luca, en su trabajo *"La democracia y el derecho penal ante las nuevas tecnologías"*, pub. en "Sistema Penal e Informática", M.A.Riquert director, C.C. Sueiro coordinador, Hammurabi, Bs.As., Nº 7, 2024, pág. 28.

[3] Podría decirse que recién varios días después de conocerse algún sector de la prensa ha alertado sobre el particular. Por ejemplo, en el diario "Perfil", nota titulada *"La Unidad de Inteligencia Artificial aplicada a Seguridad de Patricia Bullrich: cuáles son las dudas y las advertencias de los especialistas"*, pub. en la edición digital del 31/03/2024, disponible en https://www.perfil.com/noticias/politica/la-unidad-de-inteligencia-artificial-aplicada-a-seguridad-de-patricia-bullrich-cuales-son-las-dudas-y-las-advertencias-de-los-especialsitas.phtml; en el diario "Pagina 12", nota titulada *"Decretos, resoluciones y degradaciones"*, edición digital del 01/08/2024, disponible en https://www.pagina12.com.ar/757061-decretos-resoluciones-y-degradaciones . También hubo alguna repercusión en medios internacionales, como el caso del británico "The Guardian", con la nota titulada *"Argentina will use AI to 'predict future crimes' but experts worry for citizens' rights",* pub. en su edición digital del 02/08/2024, disponible en https://www.theguardian.com/world/article/2024/aug/01/argentina-ai-predicting-future-crimes-citizen-rights#:~:text=Argentina-,Argentina%20will%20use%20AI%20to%20'predict%20future%20crimes'%20but,experts%20worry%20for%20citizens'%20rights&text=Argentina's%20security%20forces%20have%20announced,warned%20could%20threaten%20citizens'%20rights.

calidad de nuestra vida como ciudadanos por su potencial de afectación a alguno de los derechos que le son inherentes. Así, por mencionar lo más evidente, la intimidad, la dignidad humana y la libertad de expresión. Pero, se verá, no sólo esos. Me refiero a las Resoluciones Nros. 428/2024 y 710/2024, publicadas respectivamente en los meses de mayo y julio pasados[4].

Puede advertirse que con la del mes de mayo la ministra retoma una iniciativa propia, de su anterior gestión en la misma cartera, me refiero a la Res. 2018-31 APN-SECSEG MSG del 26/7/2018 –que fuera muy criticada[5]-, cuyo art. 1° instruía a las áreas de investigación de ciberdelitos de las fuerzas policiales y de seguridad a tomar intervención en numerosos tópicos que conformaban una suerte de catálogo que iba desde la venta de armas, a las infracciones aduaneras hasta el hostigamiento a menores, por internet. Asimismo, se indicaba que los actos investigativos debían limitarse a sitios de acceso público, haciendo especial hincapié en redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de internet, darkweb y demás sitios de relevancia de acceso público, fijando como límite las acciones que vulneren o entorpezcan el derecho a la intimidad, Ley 25326 y normativa reglamentaria. Había sido derogada por la Res. 144/2020, mediante la que se fijó el protocolo de ciberpatrullaje que rigió durante la pandemia por el COVID-19[6].

---

[4] Se ha reproducido su texto en forma íntegra en el Anexo Documental, al final del trabajo.

[5] Así, por ejemplo, Nora Cherñavsky, quien la calificó como oscuramente habilitante de la actividad de ciberpatrullaje (en su trabajo *"¿Qué hay nuevo sobre el Ciber patrullaje en fuentes abiertas?"*, disponible desde el 17/6/2020 en su blog "Ciberdelitos", disponible en https://ciberdelito.com/2020/06/17/que-hay-de-nuevo-sobre-el-ciber-patrullaje-en-fuentes-abiertas/). El calificativo de oscura no sólo se corresponde con su falta de claridad e imprecisiones sino también porque no se cumplió con el trámite de publicación en el B.O. según fuera más tarde denunciado, por lo que se estuvo usando sin conocimiento social de su existencia (fuente: noticias periodísticas tituladas *"Ciberpatrullaje: ¿Qué es legal vigilar en las redes y por qué?"*, pub. en el diario "Página 12", edición digital del 11/07/2020, disponible en https://www.pagina12.com.ar/277830-ciberpatrullaje-que-es-legal-vigilar-en-las-redes-y-por-que; *"Hallaron la resolución que usó Bullrich para hacer inteligencia en las redes sociales"*, pub. en el medio virtual "Plan B Noticias", disponible desde el 10/07/2020 en https://www.planbnoticias.com.ar/index.php/2020/07/10/hallaron-la-resolucion-que-uso-bullrich-para-hacer-inteligencia-en-las-redes-sociales/).

Por su parte, Juan Argibay Molina y Marcos Candiotto recuerdan que sus problemas de falta de transparencia fueron advertidos por la Asociación por los Derechos Civiles (ADC) en su informe del año 2018, el que se indicó que consultaron al Ministerio de Seguridad nacional acerca de tal actividad y el protocolo de actuación implementado para su concreción y la "Dirección de Investigaciones de Ciberdelitos" respondió *"que no tenía formulado un concepto de manera oficial pero que, no obstante, las fuerzas de seguridad realizaban tareas orientadas a detectar la comisión de delitos en redes sociales"*. Lo hizo sin brindar detalles concernientes a bajo qué protocolo de actuación estas tareas eran desarrolladas (cf. su obra *"Ciberpatrullaje"*, ed. Hammurabi, Bs.As., 2020, pág. 56; e-book disponible en https://biblioteca.hammurabidigital.com.ar).

[6] Como destacó Christian Sueiro, entre otros múltiples impactos en nuestras prácticas sociales durante la pandemia, la tecnología se usó para controlar contagios mediante el uso de IA en modelos que permitían predecir con precisión la forma de propagación del virus y también, por vigilancia electrónica, la detección de personas con síntomas compatibles con posibles contagios (cf. su trabajo *"La inteligencia artificial aplicada a la vigilancia electrónica de personas en la pandemia COVID-19"*, pub. en AAVV "Derecho Penal y Pandemia. XX Encuentro de la Asociación Argentina de Profesores de Derecho Penal. Homenaje al Prof. Julio B. Maier", Ediar, Bs.As., 2021, pág. 266).

En tren de exponer algún grado de contradicción, es posible señalar que, en 2020, por entonces desde el llano, la Ministra expuso una abierta crítica del tardíamente rectificado fallido de quien estaba a cargo de la cartera, Sabina Frederic, que aludió a la posibilidad de medir el "humor social" auscultando lo que acontecía en las redes sociales[7]. Evidentemente, con errático devenir, ahora se considera otra vez la actividad como útil, necesaria y virtuosa, por lo tanto, valiosa al punto de ser nuevamente impulsada desde su gestión ministerial incluyendo entre los posibles usos la previsión de "disturbios" (cf. art. 4 inc. f), Res. 428/2024), que no deja de ser otra forma de consagrar lo mismo.

Podría decirse que, a través de la nueva regulación para el desarrollo de tareas de prevención o inteligencia por las fuerzas de seguridad con uso de fuentes digitales abiertas (Res. 428/2024) y de crear una *"Unidad de Inteligencia Artificial aplicada a la seguridad"* (Res. 710/2024, en adelante se usará la sigla UIAAS), se pone de manifiesto una vez más la conocida tensión entre libertad y seguridad[8]. Esto se produce en momentos en que ha cobrado una suerte de plenitud aquella advertencia de Winfried Hassemer respecto a estar viviendo una época en que la disposición a *"cambiar libertad por seguridad"* arrecia incluso en las modernas sociedades democráticas occidentales[9].

Claro que una cosa es que la sociedad decida, debates mediante y con suerte de consentimiento informado, ceder parcelas de su libertad para sentirse más segura y otra muy distinta es que se cercenen libertades incrementando notablemente el grado de control social bajo argumento de brindar mayor seguridad. Entonces, una primera crítica ineludible es que desde el Ministerio de Seguridad se ha resuelto avanzar sobre temas sensibles en lo que hace a la calidad de ciudadanía sin que hubiera mediado una explicación

---

[7] Baste como referencia la nota periodística titulada *"Patricia Bullrich: "Lo que ha dicho Sabina Frederic es ilegal y es espionaje"*, pub. en el diario "La Nación", edición digital del 08/04/2020, disponible en https://www.lanacion.com.ar/politica/patricia-bullrich-lo-ha-dicho-sabina-frederic-nid2352374/. Una semana después dejó claro que no objetaba el ciberpatrullaje en sí mismo sino su uso para medir la temperatura social (puede verse la nota periodística titulada *"Argentina. Patricia Bullrich: Yo tenía diferencias con la ministra Frederic, pero con el ciberpatrullaje la banco"*, pub. en el portal "Resumen Latinoamericano. La otra cara de las noticias en Latinoamérica y el tercer mundo", disponible desde el 15/04/2020 en https://www.resumenlatinoamericano.org/2020/04/15/argentina-patricia-bullrich-yo-tenia-diferencias-con-la-ministra-frederic-pero-con-el-ciberpatrullaje-la-banco/)

[8] Puede ampliarse sobre los plurales aspectos en que actualmente se manifiesta en la reciente obra de AAVV *"La tensión entre libertad y seguridad. Una aproximación socio-jurídica"*, dirigida por Ma. José Bernuz Beneitez y Ana I. Pérez Cepeda, Servicio de Publicaciones de la Universidad de La Rioja, España, Colección Jurídica Nº 22, 2023.

[9] En función de lo señalado por Hassemer (en *"La autocomprensión de la Ciencia del Derecho Penal frente a las exigencias de su tiempo"*, pub. en AAVV "La ciencia del Derecho Penal ante el nuevo milenio", versión española coordinada por Francisco Muñoz Conde (versión alemana por Eser-Hassemer-Burkhardt), tirant lo blanch, Valencia, 2004), había realizado similar recordatorio en la ponencia presentada en el XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal (Rosario, junio de 2011), titulada *"Informática y derecho penal: ¿entre el control social y el delito?"*, disponible en el blog "Riquert Delincuencia Informática" desde el 15/12/2011: https://riquertdelincuenciainformatica.blogspot.com/2011/12/?m=0. Asimismo en una versión ampliada de tal ponencia titulada *"Delincuencia informática y control social: ¿excusa y consecuencia?"*, pub. en "Revista Jurídica", Facultad de Derecho de la UNMDP, Año 6, N° 6, 2011, págs. 67/99 y en la revista jurídica virtual "Derecho Penal" de la Universidad de Friburgo, dirigida por el prof. José Hurtado Pozo, edición del mes de febrero de 2012, sección "Artículos", disponible en http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20120208_01.pdf

y diálogos previos con los sectores interesados especializados acerca del alcance y mejor modo de concretar medidas que pueden ser necesarias y útiles pero que también pueden afectar derechos fundamentales y son de delicada implementación.

Al calor de la novedad, en este trabajo me propongo brindar unas primeras reflexiones sobre bondades y defectos de ambas resoluciones que, insisto, tienen gran potencialidad de afectación sobre derechos constitucionalmente garantizados que, por eso, es importante se limite en su reglamentación y establezcan controles externos que permitan asegurar su cumplimiento[10].

Puede adelantarse que, si se atiende a las exposiciones de motivos y algunas disposiciones de la parte resolutiva de ambos instrumentos, esto parece no haber pasado inadvertido para la autoridad ministerial en cuanto la Res. 710 señala que la UIAAS *"adecuará sus misiones y funciones a las pautas, principios, criterios, recomendaciones y directivas para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos aprobadas por RESOL-2024-428-APN-MSG"* (cf. art. 5). A su vez, en la Res. 428 a la que se remite hay dos referencias limitadoras de la actividad:

1º) el artículo inicial que prevé que las fuerzas policiales y de seguridad federales deberán adecuar su conducta a las pautas, principios, criterios, recomendaciones y directivas que se establecen para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos y que dichas tareas preventivas se llevarán a cabo únicamente mediante el uso de sitios web de acceso público y fuentes digitales abiertas entendiéndose estas como los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implica una transgresión 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;

2º) el art. 4º, en cuanto fija como prohibiciones para tales tareas: a) obtener información, producir inteligencia o almacenar datos sobre personas o usuarios por el sólo hecho de su raza, fe religiosa, acciones privadas u opinión política; b) emplear métodos ilegales, prohibidos, invasivos y violatorios de la dignidad de las personas para la obtención de información; c) comunicar o publicitar información que viole los principios descriptos en el artículo anterior, como así también incorporar datos o información falsos.

Sin embargo, cuando se mira el listado de propósitos y competencias que se asignan en ambas resoluciones, puede advertirse que en varios casos se avanza habilitando actividades que, también reciente, se han prohibido o limitado fuertemente en otras sociedades de nuestro entorno cultural que se citan como modelos que se estaría siguiendo. En concreto, se verá que se incluyen sin mayores precisiones sobre quién será el desarrollador/proveedor tecnológico ni las características de los sistemas asistidos por IA que se usarán, actividades que se vedan en la Unión Europea, donde el Parlamento Europeo

[10] Por la importancia de que exista posibilidad de control externo no puedo asignar mayor trascendencia a la regla que impone una suerte de autocontrol, como sería el art. 5° de la Res. 428/2024, que dice: *"El uso de softwares o cualquier dispositivo o herramienta tecnológica de tratamiento de la información automatizada basada en inteligencia artificial, aprendizaje automático, sistema experto, redes neuronales, aprendizaje profundo o cualquier otra que en el futuro se desarrolle se ajustará a las estrictas necesidades de la actividad regulada en este protocolo. Su uso deberá ser supervisado por el MINISTERIO DE SEGURIDAD"*.

ha aprobado en marzo de 2024 la propuesta de "Reglamento de Inteligencia Artificial", una verdadera "Ley de Inteligencia Artificial" (LIA), pionera en el mundo[11], en cuyo Capítulo II se refiere a las "Prácticas de inteligencia artificial prohibidas", que son precisadas con largo detalle en los ocho parágrafos del art. 5[12]. Se ha establecido que sus previsiones entrarán en vigencia en forma escalonada, plazos a contar desde el 01/08/2024, siendo lo primero que cobrará operatividad las prohibiciones, cuya ventana es la más corta, de tan solo seis meses. En lo que sigue, también se irá avanzando sobre este contraste.

2. Los nuevos límites al ciberpatrullaje

Con motivo de su regulación durante la vigencia de la pandemia por el COVID-19 me ocupé de esta práctica que, en general, provoca importantes discusiones[13]. En ése caso se trataba de otra resolución del Ministerio de Seguridad, N° 144/2020, por la que se había aprobado el *"Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas"*, que la integraba como Anexo (art. 1°). Por art. 1º de la Res. 720/2022[14] se dispuso la derogación, perdiendo vigencia en noviembre de 2022.

La preocupación por el modo en que esta actividad se regule podría decirse que se verifica sin fisuras en la doctrina que se ha abocado a la cuestión. Sin ir más lejos, recientemente Narayan Acosta y Juan Molinas resaltan que, en función de los derechos en juego, la técnica de ciberpatrullaje no puede habilitarse sin limitaciones y que el Estado debe guiarse por criterios de racionalidad y proporcionalidad en su implementación. De allí que apunten como un primer límite a estas prácticas que sólo se las permita como técnica de prevención general de algunos delitos en particular (es decir, no individual, no a una persona concreta, para lo que sin duda se requiere resolución judicial fundada) y siempre siguiendo pautas objetivas de actuación[15].

En general, puede decirse que es factible identificar un grupo de delitos graves respecto de los que, por esa característica, pareciera razonable y podría habilitarse la tarea preventiva de ciberpatrullaje en fuentes abiertas. En el caso del derogado Protocolo regente durante la pandemia se había distinguido en el art. 3 en dos grupos. Uno, "específico", en

---

[11] Se trata de la resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de "Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))".

[12] Se texto se ha transcripto en el Anexo documental, al final del trabajo. La contradicción entre la resolución ministerial argentina y las previsiones de la LIA son resaltadas en la nota periodística titulada *"Entró en vigor en Europa la primera regulación de las inteligencias artificiales"*, pub. en el diario "Página 12", edición digital del 02/08/2024, disponible de https://www.pagina12.com.ar/757127-entro-en-vigor-en-europa-la-primera-regulacion-de-las-inteli

8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otro acto legislativo de la Unión".

[13] La versión más actualizada de mi abordaje está en la obra *"Inteligencia artificial y derecho penal"*, prologada por E. Raúl Zaffaroni, Ediar, Bs.As., 2º edición, 2024, cap. IV, págs. 267/289.

[14] Pub. en el BO del 31/10/2022.

[15] Acosta y Molinas, en su trabajo *"Cuando las fuerzas de seguridad se transforman en 'followers': el ciberpatrullaje (OSINT/SOCMINT)"*, pub. en AAVV "Sistema penal e informática", M. A. Riquert director – C.C. Sueiro coordinador, vol. 6., Hammurabi, Bs.As., 2023, págs. 193/194.

cuanto recogía conductas clara y directamente vinculadas con la cuestión sanitaria –que es un sector de infraestructura crítica-, a saber: a) Comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; b) Venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente[16]; c) Ataques informáticos a infraestructura crítica —especialmente a hospitales y a centros de salud—; d) Indicios relativos a los delitos previstos en los artículos 205, 239 y concordantes del Código Penal[17].

Hasta allí, nada que discutir ya que, como resaltó Fernando Miró Llinares, la crisis por el COVID-19 derivó en cambios de intereses, necesidades y actividades cotidianas de la población y esto en nuevas oportunidades para los ciberdelincuentes, que se adaptaron y aprovecharon, lo que se concretó sobre todo por cambio de objetivo y ciberlugar. Así, en lo que aquí interesa, con relación a la adaptación de objetivo, fue el sistema sanitario el que se constituyó como de mayor interés, lo que se reveló a partir de relevamientos que indicaron para el primer cuatrimestre de 2020 un incremento del 70% en los ataques sufridos por dicho sector respecto de igual período del año anterior, en particular de la modalidad "ransomware" contra hospitales y otras instituciones dedicadas a la lucha contra el coronavirus -porque la urgencia en evitar el colapso ofrecía mayores garantías de pago-, así como contra centros de investigación relacionados con el desarrollo de vacunas y tratamientos –víctimas preferentes de accesos ilegítimos para llegar a esa información de alto valor económico-[18].

Sin embargo, luego, usando la fórmula *"en tanto se advierta que resulten sensibles al desarrollo de la emergencia pública en materia sanitaria"*, se había habilitado las tareas de prevención policial a posibles conductas delictivas (enumeradas con escaso rigor técnico) cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos con el fin de realizar: a) Trata de personas; b) Tráfico de estupefacientes; c) Lavado de dinero y terrorismo; d) Acoso y/o violencia por motivos de género, amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación; e) Delitos relacionados con el grooming y la producción, financiación, ofrecimiento, comercio, publicación, facilitación,

---

[16] Un dato por demás interesante sobre esto proporciona Javier I. Zaragoza Tejada, quien señala que sólo durante la situación de confinamiento en España, donde se declaró el 14 de marzo de 2020 por RD 463/2020, se localizaron cerca de 12000 webs fraudulentas que comercializan vacunas o remedios milagrosos para luchar contra el coronavirus (en su trabajo *"Ciberpatrullaje e investigación tecnológica en la red"*, pub. en AAVV "Cibercrimen III", dirigido por Dupuy y Corvalán, coord. por Kiefer, ed. BdeF, Montevideo-Buenos Aires, 2020, pág. 210).

[17] Sobre estos delitos, también en el contexto de la pandemia, me extendí en el trabajo *"¿Qué delitos se pueden cometer si no se cumplen las normas de aislamiento social preventivo obligatorio?"*, pub. en *"Erreius on line"*, ed. Erreius, 26 de marzo de 2020, versión digital disponible en: http://ius.errepar.com/sitios/ver/html/20200325145812189.html

[18] De revés, Miró indicó que el paralizado sector hotelero ofreció una clara disminución de ataques (en su trabajo *"Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos"*, pub. en "IDP. Revista de Internet, Derecho y Política", Universitat Oberta de Catalunya, Nº 32, febrero de 2021en *"Crimen, cibercrimen…"*, págs. 9/10).

divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes[19]. Era claro que, más allá de ser graves, algunos de estos delitos no tenían relación directa con la pandemia y de allí que mediara crítica por su inclusión.

Si cotejamos con el vigente art. 2 de la Res. 428/2024, en particular su inc. o)[20], puede advertirse que se habilita a las fuerzas policiales y de seguridad federales a desarrollar labores preventivas en el espacio cibernético con relación a cualquier delito. No sólo eso, sino que los dos últimos incisos, p) y q), agregan la tarea de búsqueda de personas incluidas en el *"Programa Nacional de Coordinación para la Búsqueda de Personas Ordenadas por la Justicia"* (o el que en el futuro lo reemplace) y de personas desaparecidas y extraviadas en el marco del *"Sistema Federal de Búsqueda de Personas Desaparecidas y Extraviadas"*. Tenemos en concreto entonces una resolución que no fija límite alguno por la calidad del delito para la realización del ciberpatrullaje y que, además, lo integra a la búsqueda de personas con pedido de captura judicial o de desaparecidas y extraviadas. Si volvemos unos pasos atrás, en general se suele recoger una opinión positiva acerca de la actividad cuando se la vincula con su utilidad preventiva o necesidad investigativa en criminalidad grave, pero no sucede lo mismo cuando hablamos de delincuencia menor, respecto de la que podría operar como un motivo adicional para profundizar la asimétrica criminalidad que existe sobre tal sector, en comparación con el ejercicio de poder punitivo que recae sobre la grave, sobre todo, en versión de "cuello blanco".

Desde una mirada realista, no debe soslayarse que la búsqueda de datos de relevancia dentro de la información pública es utilizada habitualmente en la investigación penal. Como puntualizan Daniela Dupuy y Catalina Neme, con ello se hace referencia a los rastros o huellas online que los usuarios han ido dejando a lo largo del tiempo en la red, por voluntad propia, al utilizar aplicaciones de escritorio y móviles, aceptando las condiciones de uso y privacidad que le impone el proveedor de servicios en el que se va a registrar y publicar información personal. Resaltan además que este tipo de información, en muchos casos, puede llegar a ayudar a identificar a un usuario investigado más que la titularidad de una dirección IP, ya que algunos pueden utilizar programas de enmascaramiento de IP o bien la dirección IP puede corresponderse a un nateo[21]. Las nombradas consideran que, lejos de configurar inteligencia criminal, el ciberpatrullaje es una buena herramienta

---

[19] Sobre este último grupo de actividades, destaca Zaragoza Tejada que, además de los rastreos en redes abiertas, es usual que la investigación en el ciberespacio se canalice a través de metabuscadores que monitorean las redes P2P y permiten localizar archivos de contenido ilícito (previamente identificados por su "hash"), así como las direcciones de IP de los usuarios que, en ése momento, están remitiéndolos. Su generalización es tal que ONG dedicadas a combatir estos ilícitos, como en USA el *"National Center for Missing & Exploted Children"* (NCMEC), los usan para producir sus reportes sobre explotación sexual de menores online (ya citado, pág. 211).

[20] Concretamente, luego del largo listado previo, le brinda una suerte de carácter meramente ejemplificativo ya que dice: *"Cualquier otro delito del que se pueda obtener noticia a través del ciberespacio"*.

[21] Dupuy-Neme, en su trabajo *"ABC de la investigación de cara al juicio oral"*, pub. en AAVV "Acosos en la red a niños, niñas y adolescentes", Dupuy directora-Neme coordinadora, Hammurabi, Bs.As., Colección Cibercrimen/1, 2020, pág. 287. Aclaran que la tecnología NAT corresponde a los servidores de conexión de los usuarios de Internet móviles de una empresa que al conectarse a Internet generan tráfico de IP privadas y establece la conexión para navegar en Internet, así, al tratarse de direcciones IP dinámicas, todo el universo de clientes tiene acceso a las mismas, imposibilitando su identificación (nota al pie 24).

aceptada hace varios años por la jurisprudencia internacional para prevenir ciberdelitos. En todo caso, plantean, lo que se debe es analizar en cada caso concreto la metodología utilizada y si la actividad se extralimitó del ámbito público y permitido, a la esfera íntima y prohibida, al menos sin autorización judicial[22].

Comparto la postulación. Y puede decirse que la Res. 428/2024, conforme su art. 3º y más allá de las prohibiciones ya indicadas que establece el art. 4º, se ajusta al parámetro de fuentes digitales abiertas (inc. b) y remarca que la labor preventiva se deberá adecuar con estricto acatamiento a los diversos lineamientos que parten de las facultades dispuestas por la Constitución Nacional, Pactos Internacionales de Derechos Humanos, Leyes Nacionales y sus reglamentaciones –así, la LPDP Nº 25326 con particular énfasis cuando se trate de publicaciones de niñas, niños y adolescentes-, Leyes y Decretos orgánicos de las Fuerzas Policiales y de Seguridad Federales y sus normas reglamentarias y complementarias (incs. "a" y "g") e incluyen una serie de restricciones que, en algunos casos, son bastante porosas o imprecisas, como por ejemplo, que la judicialización de las conductas prevenidas requerirá de un análisis en función de las características comunicacionales propias del medio en que se realizan y del presunto infractor (inc. c). Otras, resaltan una obviedad: que no judicializarán aquellas conductas susceptibles de ser consideradas regulares, usuales o inherentes al uso de Internet y que no evidencien la intención de transgredir alguna norma (inc. d) o que el ciberpatrullaje no podrá interferir con una garantía constitucional como la libertad de expresión (inc. h). Se explicita el posible uso de un "agente revelador" con autorización judicial y conforme pautas de la ley 27.319 (inc. e) y se veda la acumulación de información proveniente de investigaciones previas realizadas, indicando que una vez concluida la actividad preventiva o decidida la no judicialización, deberá destruirse el material y datos obtenidos (inc. f). Finaliza señalando la necesidad de estar capacitado del personal que intervenga (inc. i) y que el Ministerio de Seguridad publicará la normativa en sus redes sociales y dará a conocer regularmente toda información relacionada con la cantidad de casos y personas objeto de la prevención (inc. j).

No obstante la indicación del inc. b del art. 3 transcripto en orden al *"uso de fuentes abiertas digitales"*, como puntualizaron Argibay Molina y Candiotto refiriéndose a la norma símil derogada, no se evitan discusiones tanto a nivel doctrinario como jurisprudencial porque, básicamente, determinar si una fuente de información es "pública" o "privada" puede no resultar sencillo y debe ser evaluado a la luz de los derechos fundamentales[23]. Un dato de singular interés que resaltan es que este buceo por fuentes abiertas puede resultar mucho más intrusivo para la intimidad que otras investigaciones convencionales, en particular, porque lo que se va subiendo a la red queda allí y, entonces, la búsqueda recupera un hilo de una profundidad histórica en el que el compromiso de aquellos

[22] Ob.cit., pág. 304.

[23] Juan Argibay Molina y Marcos Candiotto, ya citados, pág. 25. En función de lo afirmado en el texto principal, ambos autores llaman la atención sobre la importancia de identificar, por lo menos, tres niveles de acceso a datos alojados en la web: 1°) el de "acceso libre", integrado por aquellas fuentes a las que se accede sin ningún tipo de restricción (por ej., Boletín Oficial); 2°) el "semipúblico y no pago", que comprende el acceso a bases de información que exigen al usuario registrarse para tener acceso a los datos allí alojados (por ej., LinkedIn); 3°) el "semipúblico y pago", en el que el usuario debe, además de registrarse, abonar un canon para acceder a la información ofrecida como, por ej., Nosis (ob.cit., pág. 33).

derechos es, con evidencia, mayor[24]. Llevan razón, además, cuando en términos de posible afectación de derechos fundamentales señalan que, paradójicamente, la velocidad con que avanza la tecnología en la creación de herramientas que facilitan la tarea de síntesis y análisis de información, no va acompañada de evaluaciones profundas respecto de los conflictos y problemas que la utilización de estas herramientas puede involucrar[25].

La importancia de discutir y clarificar sobre qué, por qué y para qué se va a hacer "inteligencia", en el caso particular se potencia porque al ser la conceptualización de la inteligencia de fuentes abiertas (Open Source Intelligence u "OSINT") imprecisa y no atrapar su concepto en toda su extensión, se dificulta la posibilidad de analizar las tensiones que podría generar la utilización de estas herramientas por parte de agentes estatales[26]. En el caso concreto, el Ministerio de Seguridad deja todo en sus propias manos ya que, conforme el art. 6º de la resolución en comentario, es el que establecerá los lineamientos y prioridades estratégicas para las tareas preventivas. Identifica algún indicador objetivo de propia elaboración para fijarlos, como serían las estadísticas de los reportes enviados a la "Dirección de Ciberdelito y Asuntos Cibernéticos" (que es de la que dependerá la UIAAS), y agrega un genérico "otras fuentes", sin mayor precisión. Es decir, podría ser cualquiera que se le ocurriera al responsable de turno.

Para comprender la trascendencia del punto es importante no perder de vista que, sin importar el color político dominante del momento, la OSINT ha llegado para quedarse y, como enfatiza Agostina Miquelarena, ofrece una renovada caja de herramientas para la investigación digital. La nombrada, ofrece un pormenorizado detalle de los distintos instrumentos y servicios web, estructurando la "caja de herramientas" que la abastece en nueve compartimentos: a) motores de búsqueda; b) redes sociales; c) correos electrónicos; d) nombres de usuario; e) números de teléfono; f) documentos; g) imágenes; h) nombres de dominio; h) direcciones IP. La sola mención de títulos expresa con elocuencia que el nutriente de la OSINT es la confluencia de múltiples fuentes que quedará en manos, a disposición de los organismos de seguridad, en el descripto marco de imprecisiones y falta de controles[27].

No es todo, ya que dicho art. 6º también señala se considerarán para dar lineamientos o fijar prioridades las denuncias ciudadanas recibidas a la "Línea 134" que versaren sobre los delitos mencionados en la propia resolución que, ya se vio, son todos los previstos en nuestro digesto punitivo. Un dato relevante para valorar esta inclusión es que tal línea es la habilitada para recibir denuncias anónimas y que el gobierno, ante distintas movilizaciones y paros nacionales de protesta, la ha potenciado como medio canalizador de noticias de amenazas para participar en estos[28].

---

[24] Ob.cit., pág. 47.

[25] Ob.cit., pág. 46.

[26] Argibay Molina-Candiotto, ob.cit., pág. 34.

[27] Puede verse la profusa descripción del contenido de los compartimentos en el trabajo de Miquelarena, titulado *"La inteligencia de fuentes abiertas: una renovada caja de herramientas para la investigación digital"*, pub. en AAVV "La investigación penal en el entorno digital", Marcos Salt y Jonathan Polansky directores, Hammurabi, Bs.As., Nº 1, 2023, págs. 158/179.

[28] Entre múltiples fuentes, puede consultarse la nota periodística titulada "De cara al paro nacional, el Gobierno volvió a habilitar la línea 134 para denunciar amenazas", pub. por el diario "Ámbito", edición digital

Otro motivo de preocupación es que la Res. 428/2024 carece de una previsión análoga al art. 9 ° del Protocolo vigente durante la pandemia por el COVID-19, por el que expresamente se prohibió la intervención de áreas de inteligencia criminal y del personal de inteligencia[29]. No solo no la tiene sino que el art. 11 parece dejar una puerta abierta para que esto suceda en cuanto prevé que la Dirección de Ciberdelito y Asuntos Cibernéticos (o el área que en el futuro la reemplace), conformará equipos interdisciplinarios de trabajo para actualizar la normativa o complementarla, los que podrán incluir a otras agencias del Estado, asociaciones civiles sin fines de lucro, personas de relevancia en el campo de las ciencias informáticas o empresas comerciales[30].

Como no estamos frente a una novedad real -se ha visto existieron previas regulaciones del ciberpatrullaje-, hay una suerte de "historia" de críticas y validaciones.

En tren crítico se ha señalado que, aparte de invadir la privacidad, estas técnicas producen un efecto inhibidor en el discurso afectando la libertad de expresión de los usuarios y usuarias. La observación apunta a que las personas que creen que el gobierno está monitoreando sus mensajes son más propensas a autocensurarse. Así, se elude o evita escribir o discutir sobre ciertos temas, como los políticos y sociales que podrían contribuir positivamente al discurso público. De este modo, también se amenaza el uso de las redes sociales como espacio donde puedan explorarse nuevas identidades, posiciones y argumentos[31]. Desde la Fundación "Vía Libre", que fue convocada por la entonces autoridad ministerial durante el proceso de elaboración del Protocolo regente en la mencionada pandemia, se expidieron en sentido crítico señalando que *"Apreciamos que le han hecho mejoras al primer borrador, que era impresentable. Celebramos la derogación del protocolo de Bullrich también. Pero la práctica está fuera del marco legal y una resolución de este tipo no puede ir por encima de la ley"*. En particular, entendieron que se sigue disfrazando lo que son tareas de inteligencia bajo un cambio de nombre: "*Llaman tareas preventivas a lo que*

---

del 16/01/2024, disponible en https://www.ambito.com/politica/de-cara-al-paro-nacional-el-gobierno-volvio-habilitar-la-linea-134-denunciar-amenazas-n5923004

[29] En los Considerandos de la Res. N° 144/2020 se aclaraba que una regulación del uso de las mismas fuentes para tareas de inteligencia excede las competencias normativas del Ministerio de Seguridad, invocándose los arts. 7 y 13 de la L. 25520 y el art. 4°, Anexo I, del Dto. N° 950/02.

[30] Entiendo que no puede compararse esto con lo que significaba en términos de transparencia en la Res. 1440/2020 la conformación de una Mesa Consultiva en el ámbito de la Unidad de Gabinete de Asesores del Ministerio de la Seguridad para hacer la evaluación de la observancia del Protocolo General y las reglamentaciones específicas adoptadas por las fuerzas policiales y de seguridad para darle cumplimiento (art. 3°, Res. citada). En particular porque se preveía que dicha Mesa Consultiva se integrara con representantes de diversas áreas del PE, de ambas Cámaras del Congreso Nacional, de los Ministerios Públicos Fiscal y de la Defensa, Poderes Judiciales y Defensorías del Pueblo, dejándose abierta la posibilidad no sólo de consultar a organismos de Derechos Humanos, de Prevención de la Tortura y otros actores de la sociedad civil, sino de invitarlos a participar en las reuniones periódicas (art. 4°, Res.).

[31] Así, en la nota *"Ciberpatrullaje en Argentina: los riesgos del monitoreo de redes sociales para los derechos humanos"*, subida en el sitio web de la ONG "Accesnow" por Gaspar Pisanú el 12 de mayo de 2020. Disponible en: https://www.accessnow.org/ciberpatrullaje-en-argentina-los-riesgos-del-monitoreo-de-redes-sociales-para-los-derechos-humanos/

antes denominaban ciberpatrullaje. Esto sigue siendo inteligencia y como tal debe regularse por la ley de inteligencia, que prohíbe expresamente esa práctica"[32].

Del otro lado, se ha expuesto que es mejor que la actividad se transparente y se fijen protocolos que la delimiten con precisión[33], ya que no es más que una derivación lógica del impacto de las tecnologías. Así, dice Zaragoza Tejada que *"…de la misma manera en que hace poco más de 20 años las fuerzas y cuerpos de seguridad del Estado se veían obligados a patrullar las calles realizando labores de prevención e investigación de los hechos delictivos, la nueva realidad social obliga a que dichas funciones sean desempeñadas, también, en el mundo virtual"*[34]. Recuerda el nombrado que los rastreos en redes abiertas para la prevención y persecución de la explotación sexual de menores como de los delitos de ciberterrorismo, ha sido validad por numerosa jurisprudencia del Tribunal Supremo español (por ejemplo, STS 173/2018)[35].

3. La nueva UIAAS y sus funciones

Pasando al tratamiento de la Res. 710/2024, en su artículo 3° se indica la misión de la UIAAS es *"la prevención, detección, investigación y persecución del delito y sus conexiones mediante la utilización de la inteligencia artificial".* A su vez, el artículo 4º fija cuáles son las funciones que se le asignan en orden al cumplimiento de tal misión. Iremos repasándolas y comentándolas en forma individual. Pero, aclaración previa, basta una mirada superficial sobre la conformación y las funciones asignadas para el cumplimiento de la misión para plantearse la primera objeción general que emerge ineludible y es la pregunta sobre quién será el que controle al controlador y cómo se evitarán los posibles desvíos de la información sensible que se recopilará. Al fin y al cabo, la UIAAS funcionará en la *"Dirección de Ciberdelito y Asuntos Cibernéticos"*, dependiente de la Unidad de Gabinete de Asesores del propio Ministerio (art. 1º), y estará encabezada por el titular de aquella Dirección e integrada por las áreas de las Fuerzas Policiales y de Seguridad Federales competentes en la materia, cuyos representantes serán designados por la autoridad máxima de cada una de esas fuerzas (art. 2).

Teniendo entonces esta objeción genérica presente en todas y cada una de las funciones, veámoslas en particular.

3.1. Art. 4º, inc. *"a. Patrullar las redes sociales abiertas, aplicaciones y sitios de Internet, así como la llamada "Internet profunda" o "Dark-Web", en orden a la investigación*

---

[32] Cf. las opiniones vertidas por una de las integrantes de "Vía Libre", Beatriz Busaniche, según se refleja en la nota publicada en su sitio web el 3 de junio de 2020, titulada *"Constitucionalidad e inteligencia, las observaciones al protocolo para ciberpatrullaje"*, disponible en https://www.vialibre.org.ar/2020/06/03/constitucionalidad-e-inteligencia-las-observaciones-al-protocolo-para-ciberpatrullaje/

[33] En esta línea, los nombrados Argibay Molina y Candiotto entendieron que la publicación del protocolo regente durante la pandemia fue *"un avance pues da forma jurídica a una práctica que, hasta el momento, se llevaba a cabo en la penumbra"* (ya citados, pág. 61).

[34] Zaragoza Tejada, trabajo citado, pág. 210.

[35] Antes citado, pág. 211.

de delitos e identificación de sus autores, así como la detección de situaciones de riesgo grave para la seguridad, en el marco de la Constitución Nacional y legislación vigente…".

Es decir que se asigna también a la Unidad la función de ciberpatrullaje con extrema amplitud e imprecisión: investigar delitos e identificar sus autores, pero también una misión "preventiva" como sería la detección de situaciones de riesgo grave para la seguridad. La Constitución, no podría declamarse de otro modo, sería el límite.

Pero lo que se está autorizando a la nueva estructura es a hacer de modo permanente tareas de inteligencia indiscriminadas (*¿qué conductas constituyen un riesgo grave para la seguridad?*), sin hipótesis delictiva concreta ni control judicial (ni de ninguna otra naturaleza). Es decir que este primer y genérico inciso permite advertir que el Ministerio habilita dentro de su estructura un organismo con desbordante poder intrusivo respecto de lo acontece en la sociedad. Esto en un momento en que gran parte de la vida comunitaria transita justamente por las redes sociales u otras instancias tecnológicas (como podría ser el metaverso).

3.2. *"…b. Identificar y comparar imágenes en soporte físico o virtual".*

Se trata de tareas para las que las nuevas tecnologías ofrecen claras ventajas y que pueden contribuir a una labor investigativa de mayor eficacia, una ayuda para esclarecer hechos. Lo que debe precisarse es cuales son las fuentes de las bases usadas para cotejo y el origen de las imágenes que deben identificarse y compararse. Sobre esto se dirá algo más al analizar los siguientes incisos del artículo en consideración.

3.3. *"…c. Analizar imágenes de cámaras de seguridad en tiempo real a fin de detectar actividades sospechosas o identificar personas buscadas utilizando reconocimiento facial".*

No puede soslayarse que se insiste en la habilitación de una actividad que tiene ya una larga historia de discusión tanto en el ámbito local (ejemplo más elocuente, la judicialización de la Resolución 398 del Ministerio de Justicia y Seguridad de la CABA, que rige desde abril de 2019), como internacional[36] (donde también la actividad está siendo sometida a escrutinio judicial). En este último, ha incluido en numerosos lugares su directa prohibición (por dar un solo ejemplo correspondiente a uno de los países que se invocan con regulaciones inspiradoras de la resolución en comentario, en la ciudad de San Francisco[37], USA, desde 2019)[38].

En síntesis, en la base de la discusión, lo que singularmente alienta el uso de estos sistemas es que no existe normativa que los regule o bien existe alguna que no solo es

---

[36] Sobre el estado de la discusión sobre el uso de herramientas de reconocimiento facial en nuestro país me he extendido en la obra *"Inteligencia artificial y derecho penal"*, ya citada, 2ª edición, págs. 170/192.

[37] Fuente: entre múltiples publicaciones periodísticas, puede consultarse la nota titulada *"San Francisco, primera ciudad en prohibir la tecnología de reconocimiento facial en EE UU"*, pub. en el diario español "El País", edición digital del 15/05/2019, disponible en https://elpais.com/tecnologia/2019/05/15/actualidad/1557904606_766075.html

[38] En términos de los fallos y sesgos en los algoritmos de reconocimiento facial, es insoslayable sugerir el documental Prejuicio cifrado (Coded Bias), dirigido por Shalini Kantayya (EE. UU.). Fue estrenado en el Festival de Sundance de 2020 y está disponible en Netflix. Allí puede verse explicar a Joy Buslamwini cómo detectó patrones de disfuncionalidades por género y raza en diversos algoritmos. La informática y activista canadiense es fundadora de la Algorithmic Justice League.

parcial (así, la genérica omisión del control y supervisión de los controladores), sino que se ha dispuesto sin un debate previo acorde a la jerarquía de los derechos que se pueden poner en juego con la expansión de la tecnología de reconocimiento facial, que son, al menos, la libertad personal así como de expresión y de asociación (basta pensar en su posible uso para la represión del opositor político), la intimidad, la privacidad y la autodeterminación informativa. Es claro, se trata de otro escenario en el que se expresa la tradicional tensión entre eficacia y garantías. Sin ingresar en los que todavía son problemas de errores de identificación que derivan en la privación de la libertad ambulatoria[39] y que, con seguridad, en poco tiempo se irán solucionando por el avance tecnológico, es cierto que se trata de una herramienta que puede mejorar la eficacia en la persecución delictiva, la cuestión es cómo esa eficacia se logra sin sacrificar en ese altar los derechos fundamentales.

En términos de prohibiciones, merece singular destaque la reciente LIA europea, en su art. 5, parág. 1, inc. *e)*, justamente incluye*:*

> *"…la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión";* mientras que el inc. f) incluye la veda de *"la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad"*.

No puede soslayarse, todo lo vinculado a la biometría está severamente restringido en la LIA, que la habilita en muy acotados casos vinculados al "ámbito de aplicación de la ley". Así puede verse que, en el mismo artículo y parágrafo, el inc "g" dice que está prohibida:

> *"…la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no abarca el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la aplicación de la ley…"*.

El siguiente inciso, "h", prevé que:

> "*…el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:*
>
> *i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas;*

---

[39] Baste recordar como ejemplo de error en el mencionado sistema implementado en la CABA, a pocos días de su entrada en funcionamiento, el caso "Ibarrola", que tuvo gran repercusión mediática. Producto de una incorrecta identificación una persona fue detenida seis días tras haber sido acusado de haber cometido un robo agravado en 2016 en Bahía Blanca. El error se debió a una carga equivocada en el sistema que provocó la consecuencia indicada: un ciudadano fue detenido por varios días cuando no pesaba sobre él ningún pedido de restricción, exclusivamente a partir de su reconocimiento facial. Entre otras publicaciones periodísticas puede consultarse la titulada *"Un hombre estuvo seis días preso por un error policial"*, pub. en "Infobae", edición digital del 02/08/2019, disponible en https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-preso-por-un-error-del-sistema-de-reconocimiento-facial/

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista;

iii) la localización o identificación de una persona sospechosa de haber cometido una infracción penal a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la aplicación de la ley".

Por cierto, no es todo. El parág. 2 del mismo art. 5 prosigue regulando el posible uso de sistemas de identificación biométrica señalando que:

"2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra h), debe llevarse a cabo únicamente para los fines establecidos en el apartado 1, letra h), para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra h), del presente artículo deberá satisfacer garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con la legislación nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y relativas a las personas. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad encargada de la aplicación de la ley ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se lleve a cabo sin demora indebida".

El siguiente parágrafo, el tercero, sigue adicionando condiciones de operatividad a una identificación biométrica a los fines de lo señalado en el primero, letra "h", y en el anterior. En este caso sujetándola a la existencia de autorización judicial o de una autoridad administrativa independiente, a la vez que fijando las reglas de cooperación en los siguientes términos:

"3. A los efectos del apartado 1, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se otorgará previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de 24 horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos que figuran en el apartado 1, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. No podrá adoptarse ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de la información de salida del sistema de identificación biométrica remota «en tiempo real».

La extensa transcripción, a la vez que permite conocer la norma completa, sirve para marcar con elocuencia el contraste no sólo de contenido sino también de profundidad para analizar la situación que se regula ante la lacónica previsión local que se comenta.

3.4. *"…d. Utilizar algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos".*

Se trata de otra actividad que tiene un largo historial de cuestionamientos en el ámbito internacional, tanto sea en su versión de vigilancia predictiva[40], como en la de apoyo de decisiones judiciales con valoración de riesgos[41].

3.4.a. En el primer aspecto, tecnología mediante, como enfatiza Miró Llinares, ha cambiado la cultura de la performance policial, y se invierte cada vez más dinero para tener recursos que permitan almacenar y procesar la creciente información. Menciona como ejemplo paradigmático al predictive policing o "PredPol"[42], un conjunto de inteligencia artificial policial (IAP) basado en la aplicación de técnicas cuantitativas para identificar objetivos de interés policial con el propósito de reducir el riesgo delictivo mediante la prevención de futuros delitos o la resolución de otros pasados[43].

Si bien no analiza individuos sino datos relativos al tiempo y lugar donde acontecen los delitos, se basa en tres máximas: victimización repetida (si hubo un robo exitoso en un lugar, se repetirá), victimización casi repetida (riesgo para el vecino del que fue robado por compartir las mismas características) y agrupamiento geográfico (los delincuentes operan

---

[40] Sobre el particular me extendí en la obra *"Inteligencia artificial y derecho penal"*, 2º edición, 2024, págs. 158/169.

[41] Sobre el particular me extendí en la obra *"Inteligencia artificial y derecho penal"*, 2º edición, 2024, págs. 192/210.

[42] Se trata de un software producido por la empresa de vigilancia predictiva "Geolítica" (hasta 2021, PredPol Inc.). El algoritmo inició como un proyecto entre la Policía de la ciudad de Los Ángeles (LAPD) y la Universidad de California en la misma ciudad (UCLA).

[43] Fernando Miró Llinares, *"Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots"*, pub. en "Revista de Derecho Penal y Criminología", UNED, 3º época, Nº 20, Madrid, 2018, págs. 99-100. Puede ampliarse sobre PredPol (y similares) en la obra de Cathy O'Neil, donde refiere, a modo de ejemplo, su impacto a partir de 2013 en la pequeña localidad de Reading, Pensilvania, Estados Unidos, y, del otro lado del Atlántico, en la británica Kent, al explicar en los casos concretos cómo plasma el que llama "bucle de retroalimentación pernicioso" que magnifica la criminalización de los sectores de mayor pobreza. Es claro, la delincuencia de cuello blanco de Wall Street no se puede combatir mejorando el patrón de patrullaje de una cuadrícula para tornarlo más eficiente, lo que solo tiene sentido si lo que se persiguen son infracciones al orden público (Cathy O'Neil, *"Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia"*, trad. de Violeta Arraz de la Torre, Ed. Capitán Swing, Madrid, España, 2018, cap. 5 "Víctimas civiles. La justicia en la era del big data").

dentro de una zona en la que tienden a agruparse). Entonces, se disponen mayores cantidades de policías en barrios a los que llegan algorítmicamente persuadidos de que detectarán delitos y estarán predispuestos a hacerlo, lo que provocará que incluso lo hagan respecto de hechos menores que, en otro contexto, no hubieran advertido. Hay, dice Danesi, una suerte de profecía autocumplida: el registro de las infracciones —aun leves— reafirma las predicciones, y se genera el famoso "bucle de retroalimentación pernicioso" del que habla Cathy O'Neil[44].

Se trata, en definitiva, de una herramienta que vendría sencillamente a profundizar la selectividad tradicional sobre la criminalidad patrimonial torpe a partir del sesgo producto de la orientación que habitualmente tienen las bases que proveen la información a procesar mediante el algoritmo. En esta línea, bien alerta Javier A. De Luca en cuanto que los sistemas de IA no son completamente confiables ni tampoco neutros, derivándose errores tanto de la mala calidad de los datos utilizados como de una defectuosa programación del algoritmo, que será influenciado por las debilidades humanas brindando resultados xenófobos, racistas o misóginos. Tendremos respuestas que vendrán teñidas por el discurso hegemónico del lugar único que se asume como "correcto", con el consecuente peligro para la diversidad[45].

Leonardo P. Palacios llama la atención sobre algo de sumo interés en torno al problema de los "sesgos". Recuerda que ya la *"Declaración de Toronto sobre la protección de los derechos a la igualdad y a la no discriminación en los sistemas de aprendizaje automático"*[46], redactada por numerosas ONG en 2018, advirtió sobre su impacto en sistemas de vigilancia policial, sistemas de bienestar social, provisión de asistencia médica, plataformas en línea. Además, el documento concientiza sobre la promoción del derecho positivo al disfrute de los avances en ciencia y tecnología, y la responsabilidad de los Estados y de las empresas en torno al desarrollo de la IA[47].

Se advierte entonces, nada realmente nuevo en definitiva en la problemática de la actividad que la resolución propicia. Si se avanzara con esto, otra de las cosas que no sabemos es si se hará con desarrollo propio de tecnología o se adquirirá un paquete a un proveedor externo nacional o internacional.

3.4.b. En el segundo aspecto, simplificando, se trata de herramientas con base en el historial de comportamiento del procesado o condenado y en datos estadísticos, que informan un pronóstico para la toma de decisiones tan importantes como la concreción del régimen penitenciario, la concesión de la libertad condicional, la reubicación del reo en uno u otro régimen penitenciario, entre otras. Uno de los softwares predictivos más conocidos –y también más cuestionados, con resultados judiciales diversos- es "COMPAS" (Correctional Offender Management Profiling for Alternative Sanctions), desarrollado por

---

[44] Cecilia C. Danesi, en *"El imperio de los algoritmos. IA inclusiva, ética y al servicio de la humanidad"*, Galerna, Bs.As., 2022, págs. 240-241.

[45] De Luca, antes citado, pág. 32.

[46] Disponible (en inglés) en http://www.accessnow.org/the-toronto-declarationprotecting-the-rights-to-equality-and-non-discrimination-in-machine-learningsystems

[47] Leonardo P. Palacios, en su trabajo *"Derechos Humanos e Inteligencia Artificial"*, pub. en AAVV "Inteligencia Artificial y Derecho", dirigido por Federico M. Álvarez Larrondo, Ed. Hammurabi, Bs.As., 2020, p. 119.

"Equivant" (antes llamada Northpointe), que es usado en varios sistemas judiciales de diferentes estados en USA[48].

Desde una mirada favorable, se indica que el uso de las evaluaciones de riesgo basadas en datos en las sentencias penales tendría como ventaja que permiten que los tribunales reduzcan las penas de prisión o no se apliquen en el caso de condenados con muy baja probabilidad de reincidir. Desde el lado crítico, la sombra que se proyecta desde el inicio es si, bajo la etiqueta de la "valoración de riesgos", esto no es más que la versión tecnológica de los pronósticos de "peligrosidad", que ya no se formulan sobre mera base clínica (de escaso soporte empírico y poca validez predictiva) sino actuarial (no es una predicción individual sino por valores de conjuntos de sujetos con factores análogos). Esto ofrecería menores tasas de error o, en otras palabras, un método de predicción de mayor fiabilidad, pero no exento de "falsos positivos" (es decir, pronósticos de delincuencia no concretados) y "falsos negativos" (al revés, predicción de no delinquir incumplida)[49].

En tren de explicitar los problemas consecuentes a su uso, el primero más evidente es la posible afectación al derecho de defensa en juicio. Como explica Jonathan A. Polansky, estos programas contienen algoritmos (códigos fuente) que son los que les indican qué tareas deben llevar a cabo y de qué forma hacerlo. Las empresas desarrolladoras obtienen beneficios económicos por la comercialización de sus productos, lo que les genera la necesidad de cuidar que los códigos fuente se mantengan en secreto para no perder su ventaja o lucro ante otras compañías o los mismos Estados (clientes), que podrían copiarlos. Así, nos dice, los códigos fuente son similares a la fórmula de la Coca-Cola, y las empresas reclaman sobre ellos que se respete el "secreto empresarial" que, en Estados Unidos, se considera la información privada de empresas que, de publicitarse, podría afectar gravemente el desarrollo de sus negocios. Para no dar a conocer los algoritmos que desarrollan, muchas compañías deciden no registrarlos ni patentarlos. Resalta Polansky que el "secreto empresarial" en dicho país ostenta una protección similar a la de los derechos de autor, pero con una diferencia relevante: mientras que, para patentar un algoritmo, se requeriría darlo a conocer, el "secreto empresarial" permite proteger los códigos fuente sin exponerlos al público. Para justificarlo, muchas compañías afirman que, de no protegerse tales secretos, se acabaría la innovación en herramientas para la Justicia, en tanto el sector privado ya no tendría incentivos para el desarrollo de nuevos productos[50].

Se entiende claramente el punto de vista comercial pero la cuestión es que el mencionado secreto sobre cómo funciona el algoritmo cobra singular interés cuando este último se usa en un proceso penal, donde está fuera de toda duda que, en nuestro orden jurídico y muchos otros análogos, el derecho de defensa (art. 18, CN) implica que el sujeto pasivo, vale decir, el imputado, tiene la facultad de controlar la prueba que se use en su

---

[48] Una reciente mirada crítica sobre COMPAS nos ofrece Nora A. Cherñavsky en su trabajo *"Inteligencia artificial y 'Big data' jurídica. Decisiones automatizadas. Modelos de aplicación en general y en el ámbito jurídico"*, pub. en "Sistema Penal e Informática", M.A. Riquert director, C.C. Sueiro coordinador, Hammurabi, Bs.As., Nº 7, 2024, págs. 33/55.

[49] Cf. María Sánchez Vilanova, en su trabajo *"La presunción de inocencia ante las herramientas estructuradas de valoración del riesgo"*, La Ley, n.º 2, Madrid, abril de 2021, pág. 2.

[50] Cf. Jonathan A. Polansky, en su obra "*Garantías constitucionales del procedimiento penal en entorno digital"*, Hammurabi, Bs.As., 2020, págs. 101-102.

contra. Esto puede ser de suma pertinencia en ocasiones como la denegación de un derecho o beneficio, la mensuración de la pena, o el acceso a un instituto más benigno con base en el pronóstico de la herramienta de evaluación de riesgos. En esas oportunidades, la defensa va a querer saber cómo funciona el sistema en virtud del que se privó al imputado o condenado de algo.

No menos evidente, otra vez está presente aquí el tema de los sesgos que quedarán ocultos dentro de la "caja negra" algorítmica protegida por el secreto empresarial. No es necesario repetir lo expuesto sobre el particular, pero sí vale la pena insistir en que es otra de las cosas de las que la resolución se olvida.

3.5. *"…e. Identificar patrones inusuales en las redes informáticas y detectar amenazas cibernéticas antes de que se produzcan ataques. Esto incluye la identificación de malware, phishing y otras formas de ciberataque".*

Más allá de las menciones específicas a determinadas modalidades de ciberataques, valen las observaciones ya formuladas con relación al primer inciso.

3.6. *"…f. Procesar grandes volúmenes de datos de diversas fuentes para extraer información útil y crear perfiles de sospechosos o identificar vínculos entre diferentes casos".*

Es evidente que lo habilitado por este inciso es una masiva tarea de perfilamiento ("profiling") que se hará sobre toda la población distinguiendo "sospechosos" de "no sospechosos" a partir del procesamiento de "grandes volúmenes de datos de diversas fuentes" (*¿cuáles? ¿cómo se los obtuvo? ¿por qué esos y no otros?*), lo que es claramente inadmisible. Más aún si no se olvida de que la pretendida objetividad o neutralidad algorítmica no existe y que el perfilamiento se hará sobre las bases ideológicas que, en muchos casos, quedarán ocultas en la "caja negra". Esto significa, ni más ni menos, que podríamos pasar a ser "sospechosos" y profundizarse medidas de seguimiento intrusivo a nuestro respecto en base a una categorización concretada mediante parámetros imposibles de revisar ni cuestionar ni siquiera en forma tardía, que quedan ocultos dentro de las pautas de entrenamiento y autoaprendizaje del algoritmo.

En síntesis, el sistema brindará un dato irrefutable: "X" es sospechoso. Ese dato no controlable permitirá que se amplifique el control sobre un ciudadano por las fuerzas de seguridad. De eso se trata.

Frente a este orden de iniciativas no debiera perderse de vista que en el novedoso mundo virtual ya se habla de un derecho fundamental de nueva generación como es el *"derecho al entorno virtual"*, que viene a acompañar a los tradicionales de la intimidad, secreto de las comunicaciones y protección de datos personales, haciendo foco en que, por ej., si atendemos a la totalidad de la información que puede obtenerse del análisis de un dispositivo informático entendido como unidad de estudio conjunto, estamos frente a una altísima intromisión en el derecho de la vida privada del interesado[51]. Puede entenderse que si lo proyectamos a grandes volúmenes de información de diversas fuentes –tal lo que

[51] Cf. Zaragoza Tejada, en su trabajo *"Ciberpatrullaje e investigación tecnológica en la red"*, pub. en AAVV "Cibercrimen III", dirigido por Dupuy y Corvalán, coord. por Kiefer, ed. BdeF, Montevideo-Buenos Aires, 2020, págs. 217/218.

indica la norma comentada-, la situación es más grave. Zaragoza Tejada señala que el derecho al entorno virtual ha sido reconocido en distintas sentencias del Tribunal Supremo y del Tribunal Constitucional españoles[52] y también del Tribunal Constitucional alemán[53] y de la Corte Suprema de USA[54].

He indicado antes la contradicción de la nueva regulación nacional con la línea que se ha concretado en la Unión Europea con la reciente LIA. En efecto, en contraste con el propiciado perfilamiento masivo clasificatorio binario (sospechosos y no sospechosos), el art. 5, parág. 1, inc. c) del Reglamento europeo prohíbe:

> *"La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a personas físicas o a grupos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes: i) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos enteros de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente; ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este".*

A su vez, el inc. d) prohíbe:

> "*…la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de evaluar o predecir la probabilidad de que una persona física cometa una infracción penal basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la evaluación humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva".*

3.7. *"…g. Patrullar mediante drones áreas extensas, proporcionar vigilancia aérea y responder a emergencias".*

La lacónica referencia a "drones" no deja en claro de qué tipo de ellos se trataría porque podrían serlo, por ejemplo, totalmente autónomos o equipados con sensores térmicos o cámaras y micrófonos de gran alcance[55], lo que modifica sustancialmente su poder intrusivo en ámbitos de intimidad[56]. La referencia a áreas extensas es imprecisa en cuanto pareciera aludir a zonas despobladas pero nada descarta la posible interpretación contraria, es decir, que se patrullen vastas zonas pobladas.

---

[52] Zaragoza Tejada menciona a las STSS 823/2015, 342/2013 y 287/2017 (ob.cit., pág. 217, nota al pie Nº 8).

[53] Individualiza una sentencia del 27 de febrero de 2008 en la que se afirmó el nacimiento de un nuevo derecho fundamental a la garantía de la confidencialidad e integridad de los grupos informáticos con el fin de proteger la vida privada y personal de los sujetos de los derechos fundamentales contra el acceso por parte del Estado en el ámbito de las tecnologías de la información, en la medida en que lo haga en su conjunto y no sólo a los acontecimientos de comunicaciones individuales o datos almacenados (ob.cit., pág. 219).

[54] Menciona el caso "Riley vs. California", de junio de 2014 (ob.cit., pág. 219).

[55] Sobre las implicancias penales del uso de vehículos aéreos no tripulados (VANT) o drones, me he extendido en la obra *"Inteligencia artificial y derecho penal"*, 2º edición, págs. 319/346.

[56] Como recuerda Gustavo E. Aboso, el empleo de drones para obtener imágenes del interior de una vivienda debe ser catalogado como un allanamiento conforme art. 18 de la CN y, por lo tanto, necesitado de orden judicial habilitante (en su obra *"Evidencia digital en el proceso penal"*, BdeF, Montevideo/Bs.As., 2023, pág. 239)

Tampoco se especifica si se podría hacer una vigilancia aérea intensiva e indiscriminada (por decirlo de algún modo, emular desde el aire en modo permanente el entramado de cámaras callejero) o el uso de drones estaría limitado a hipótesis delictivas concretas (que la noticia de un hecho presuntamente delictivo habilite se haga un seguimiento concreto desde el aire, por ejemplo, a un vehículo en fuga).

Pero, por encima de estas puntualizaciones que, si se quiere, serían de detalle, lo que aparece como problema más grave es que la resolución que se comenta habilita para la tarea judicial preventiva o investigativa un medio de prueba que no tiene recepción concreta en las normas procesales penales vigentes y este carácter de medio probatorio no regulado puede abrir paso a cuestionamientos sobre los resultados obtenidos mediante su uso por constituir una injerencia arbitraria de la privacidad, con amparo constitucional en el art. 19 de nuestra Carta Magna, con posibles nulidades como consecuencia[57].

3.8. *"…h. Realización de tareas peligrosas, como la desactivación de explosivos, mediante robots".*

Esta sería una de las actividades que ex ante no ofrecerían reparos. Usar robots para evitar riesgos humanos en actividades peligrosas como la concretamente ejemplificada es de evidente utilidad y beneficio[58].

3.9. *"…i. Mejorar la comunicación y coordinación entre diferentes Fuerzas Policiales y de Seguridad Federales y asegurar así que la información crítica se comparta de manera rápida y eficiente".*

Se trata de otro propósito que no ofrece reparos ex ante: es lógico que se busque mejorar la comunicación y la coordinación de fuerzas policiales y de seguridad para mejorar su capacidad de investigación y de prevención delictivas. Por supuesto que siempre queda como motivo de preocupación las condiciones de seguridad de la transferencia de información que se califica como "crítica".

Por la expresa remisión que existe hacia lo establecido en la Resolución 428/2024, puede anotarse como disposiciones de interés en lo vinculado con la seguridad de la información recabada a los arts. 8º (establece se deben adoptar medidas conducentes a garantizar las condiciones de registro, resguardo, trazabilidad, auditoría, comunicación a autoridad judicial, evitación de filtraciones e incluso destrucción de información no judicializada; lógicamente, habrá que ver cuáles son y cómo se reglamentan tales medidas) y 9º (fija la obligación de elaborar informes mensuales sobre las denuncias realizadas con base a la actividad habilitada por el protocolo).

3.10. *"…j. Analizar actividades en redes sociales para detectar amenazas potenciales, identificar movimientos de grupos delictivos o prever disturbios".*

Podría decirse que aquí hay más de lo mismo. Sin embargo, la inclusión de "prever disturbios" parece dirigida a controlar las expresiones de protesta social que, por cierto, no son en sí mismas delito sino válido ejercicio de un derecho. Es claro que un disturbio importa una turbación o alteración de la paz o de la concordia. Sin embargo, en la vida democrática,

---

[57] De tal opinión, Aboso, antes citado, pág. 238.

[58] Una explicación más amplia de las cuestiones de interés vinculadas a la robótica he realizado en la obra *"Inteligencia artificial y derecho penal"*, ya citada, 2º edición, págs. 92/105.

no puede equipararse sin más a una conducta delictiva. La protesta puede ser molesta, sobre todo para el detentador del poder, pero no necesariamente tiene que ser delictiva. Es una manifestación más de la libertad de expresión que puede estar canalizando reclamos por la afectación o la falta de concreción de diversos derechos sociales, como podría ser trabajo, educación, vivienda, salarios dignos, etc.

3.11. *"…k. Detectar transacciones financieras sospechosas o comportamientos anómalos que podrían indicar actividades ilegales".*

Se trata de una función claramente intrusiva en la actividad económica y financiera que, en principio, cabe preguntarse cómo se compatibilizaría con la vigencia del llamado "secreto bancario" y qué clase de actos son referidos como "comportamientos anómalos" indicativos de posibles ilegalidades.

Hay diversos sistemas preventivos y alertas en delitos como el lavado de activos de origen delictivo, pero esta resolución intentaría generar una intervención del Ministerio de Seguridad por afuera de aquellos[59]. La Ley 25246, del año 2000, y sus modificatorias, creo la Unidad de Información Financiera (UIF) y estableció quienes son los sujetos obligados (art. 20), a producir la reportes de operaciones sospechosas (ROS), bajo parámetros precisos. Evidentemente, nada de esto o previsiones similares se han tenido en cuenta para un enunciado de propósito genérico que no podría pasar de expresión de deseo cuya operatividad concreta carece de marco legal que le brinde adecuado soporte.

4. Balance provisorio

Retomando lo señalado en la introducción, con llamativo escaso estrépito en una opinión pública preocupada en otras cosas, nos encontramos con una nueva regulación para el desarrollo de tareas de prevención o inteligencia por las fuerzas de seguridad con uso de fuentes digitales abiertas –lo que habitualmente se sintetiza hablando de "ciberpatrullaje"- (Res. 428/2024) y la creación de una *"Unidad de Inteligencia Artificial aplicada a la seguridad"* (Res. 710/2024). Esto se produjo sin que medie discusión ni debate público que preceda las decisiones que, además, se han mantenido dentro de que llamaríamos "soft-law", es decir, en un segundo nivel normativo y no en leyes, que sería lo esperable -al menos, en sus líneas maestras- cuando se trata de medidas que afectan la calidad de ciudadanía.

En ambos casos, el Ministerio de Seguridad avanza bajo invocación de necesidad en materia de seguridad y lograr una mayor eficacia tanto en la prevención como en la investigación y persecución del delito. De allí que, en varios casos, los propósitos que predica se busca alcanzar no luzcan en sí mismos inadecuados.

Sin embargo, en lo que precede se puesto en evidencia que en su generalidad lo que ha primado es la enunciación de que se habilitan numerosas actividades con claro potencial de afectación de derechos fundamentales, carentes de ser acompañadas de alguna

[59] Un análisis del art. 303 del CP he realizado en AAVV *"Código Penal de la Nación. Comentado y Anotado"*, bajo mi dirección, ed. Erreius, Bs.As., 2º edición, 2022, Tomo III (artículos 186 a 316), págs. 2367/2378.

precisión así como de limitaciones en función de principios de razonabilidad y proporcionalidad (claro ejemplo, se permite el ciberpatrullaje respecto de cualquier delito).

No se especifica tecnología, proveedores, formas de acceso y resguardo, trazabilidad, transparencia y varios etcéteras, todo lo que es imprescindible conocer porque lejos de la equivocada idea de una tecnología aséptica a aplicar, los algoritmos poseen sesgos ideológicos desde su diseño que condicionan los resultados que ofrecen. No hay, además, controles externos a la propia autoridad ministerial. Median huecos que habilitan tanto la persecución de la protesta social como el acceso a información vedada por organismos de inteligencia. En muchos supuestos se abre camino a la realización de usos de la tecnología que en países a los que cita como ejemplos para lo regulado, directamente han sido prohibidos (masivos perfilamientos para categorizar a la población entre sospechosos y no sospechosos) o fuertemente limitados (todo lo relativo al reconocimiento facial). Se brindaron varios ejemplos con la reciente regulación europea sobre IA, pionera a nivel mundial.

En síntesis, no se reproducirán todas y cada una de las críticas, sino que como balance provisorio se señala que estamos frente a resoluciones que generan inquietud y preocupación porque pueden importar una grave degradación de la calidad ciudadana en un estado democrático de derecho ya que, en muchos casos en forma explícita y en otros potencial, se habilitan actividades que colisionan o afectan intensamente derechos fundamentales como la libertad personal y de expresión, la intimidad y la privacidad, la dignidad humana, la defensa en juicio, entre otros, desequilibrando a la vez el juego de contrapesos y recíprocos controles institucionales que prevé la Constitución Nacional.

5. Anexo documental

A continuación se transcribe el texto de ambas resoluciones ministeriales en orden cronológico:

I. Resolución 428/2024 del Ministerio de Seguridad

RESOL-2024-428-APN-MSG

Ciudad de Buenos Aires, 27/05/2024

Visto el expediente EX-2024-46438216- -APN-DNCYAC#MSG, la Ley de Ministerios Nº 22.520 (t.o. Decreto N° 438 del 12 de marzo de 1992) y sus modificatorias, la Ley de Seguridad Interior N° 24.059, la Decisión Administrativa N° 340 del 16 de mayo de 2024 y la Resolución del Ministerio de Seguridad Nº 75 del 10 de febrero de 2022, y

CONSIDERANDO:

Que la Ley Nº 22.520 de Ministerios (T.O Decreto N° 438/92) y sus modificatorias asignan al MINISTERIO DE SEGURIDAD la facultad de entender en la determinación de la política criminal y en la elaboración de planes y programas para su aplicación, así como para la prevención del delito, incluyendo la investigación sobre el crimen organizado y los ilícitos complejos.

Que la Ley Nº 24.059 establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior.

Que el artículo 2° de la Ley Nº 24.059 define a la seguridad interior como “la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal

que establece la Constitución Nacional"; y el artículo 8° asigna el ejercicio de la conducción política del esfuerzo nacional de policía al MINISTERIO DE SEGURIDAD.

Que los ciberdelitos son una manifestación delictiva en constante expansión que afecta cada día a más personas físicas y jurídicas, economías, sistemas, servicios, infraestructuras críticas y, en consecuencia, es necesario generar mecanismos coordinados y proactivos para la investigación por parte de las fuerzas policiales y de seguridad federales.

Que la UNODOC - Oficina de las Naciones Unidas contra la Droga y el Delito- establece que la ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.

Que la ciberdelincuencia se distingue de los delitos comunes en que no posee limitantes físicas ni geográficas y puede cometerse de manera ágil y, en general, con menores riesgos para quien delinque.

Que la Agencia de la Unión Europea para la Cooperación Policial (EUROPOL) considera que el ciberdelito es todo delito que solo se puede cometer usando computadoras, redes computarizadas, video juegos y todo tipo de tecnología que permita un manejo de situaciones a distancia.

Que el uso de esas herramientas incluye la posibilidad de comisión de delitos comunes facilitados por Internet y las tecnologías digitales.

Que la Ley Nº 26.388, de delitos informáticos, ha incorporado al sistema penal argentino las siguientes modalidades delictivas: a) Daño informático; b) Fraude informático; d) Difusión de imágenes de abuso sexual infantil; e) "Violación de Secretos y de la Privacidad"; f) Delitos contra la seguridad pública e interrupción de las comunicaciones; g) Falsificación de documentos electrónicos.

Que la Ley N° 27.411 aprobó el CONVENIO SOBRE CIBERCRIMINALIDAD del CONSEJO DE EUROPA adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, el cual tiene por objeto la prevención de los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos.

Que el citado convenio busca garantizar un adecuado respeto de los derechos fundamentales del hombre, como los garantizados en el PACTO INTERNACIONAL RELATIVO A LOS DERECHOS CIVILES Y POLÍTICOS DE LAS NACIONES UNIDAS (1966), así como en otros convenios internacionales aplicables en la materia que garantizan el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada.

Que, a nivel internacional, se observa que la ciberdelincuencia y los delitos tecnológicos cobran mayor relevancia y, en consecuencia, organismos internacionales, regionales y los países adoptan medidas para prevenirlo e investigarlo.

Que INTERPOL ha expresado que en el ciberespacio las amenazas y los ataques pueden provenir de cualquier lugar y producirse en cualquier momento, lo que implica un gran desafío para el poder de policía.

Que, asimismo, en abril de 2021, los Estados Miembros de la ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU) concluyeron en que los Estados deberían reforzar las actividades de investigación y aplicación de las leyes relacionadas con los actos de asociación, complicidad y preparación para cometer delitos cibernéticos, con vistas a confrontar eficazmente a la cadena de la ciberdelincuencia y que, además, deberían mejorar la capacidad de las autoridades judiciales y de las fuerzas del orden para investigar y perseguir los delitos cibernéticos.

Que la Resolución del MINISTERIO DE SEGURIDAD Nº 977/19, aprobó el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos, el cual fuera actualizado por Resolución MS Nº 75/22.

Que dicho plan establece los lineamientos generales de las políticas públicas relacionadas con las responsabilidades referentes al ciberespacio y su impacto en la seguridad nacional

Que se necesitan adoptar acciones sostenibles y estratégicas que permitan afrontar de la forma más práctica los flagelos relacionadas con los delitos informáticos de manera integral.

Que, en virtud de lo expuesto, se aplicarán las pautas generales cuyo objetivo es dotar de herramientas jurídicas las técnicas investigativas en materia de ciberdelitos o delitos con presencia de la tecnología o utilización de tecnologías.

Que, en otro orden, el artículo 183 del CÓDIGO PROCESAL PENAL DE NACIÓN dispone que "las Fuerzas de Seguridad deberán investigar, por iniciativa propia, en virtud de denuncia o por orden de autoridad competente, los delitos de acción pública, impedir que los hechos cometidos sean llevados a consecuencias ulteriores, individualizar a los culpables y reunir las pruebas para dar base a la acusación".

Que el artículo 235 del nuevo CÓDIGO PROCESAL PENAL FEDERAL establece en su parte pertinente que la investigación de un hecho que revistiera carácter de delito se podrá iniciar a consecuencia de la prevención de alguna de las Fuerzas de Seguridad.

Que, a su vez, el artículo 243 del mismo código establece que los funcionarios y agentes de la policía u otra fuerza de seguridad que tomaren conocimiento de un delito de acción pública deben informarlo al representante del MINISTERIO PÚBLICO FISCAL inmediatamente después de su primera intervención y continuar, en su caso, la investigación, bajo control y dirección de este órgano.

Que, mediante la Resolución de la SECRETARÍA DE SEGURIDAD N° RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018, se instruyó a las áreas de investigación de ciberdelitos de las fuerzas policiales y de seguridad que se encuentran bajo la órbita del MINISTERIO DE SEGURIDAD "…a tomar intervención, específicamente, en todo lo inherente a los siguientes tópicos: Venta o permuta ilegal de armas por Internet. Venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito. Hechos que presuntamente se encuentren vinculados con la aplicación de la Ley Nº 23.737. Difusión de mensajes e imágenes que estimulen o fomenten la explotación sexual o laboral, tanto de mayores como de menores de edad, y que prima facie parecieran estar vinculados con la trata y tráfico de personas. Hostigamiento sexual a menores de edad a través de aplicaciones o servicios de la web. Venta o permuta de objetos que, presumiblemente, hayan sido obtenidos en infracción a las disposiciones aduaneras. Hechos que presuntamente transgredan lo normado en los artículos 4, 5, 6, 7, 8 y 9 de la Ley N° 26.388. lavado de activos, o cualquier delito

Que, los actos investigativos deberán limitarse a sitios de acceso público, especialmente en redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de Internet, Dark-Web y espacios de relevancia de acceso público, bajo los parámetros de la ley 25.326.

Que la Resolución de la SECRETARÍA DE SEGURIDAD N° 2018-31-APN-SECSEG#MSG fue derogada y reemplazada por la Resolución del MINISTERIO DE SEGURIDAD N° 144/2020 que aprobó el "PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS".

Que por medio de la Resolución MS N° 720/22 se derogó la Resolución MS N° 144/20, que adolecía de serios defectos de hermenéutica, con lo cual la materia quedó sin regulación.

Que resulta necesario brindar a las Fuerzas Policiales y de Seguridad Federales que dependen de este Ministerio herramientas técnico legales adecuadas que simplifiquen sus tareas cotidianas de investigación.

Que el servicio permanente de asesoramiento jurídico de la jurisdicción ha tomado la intervención que le corresponde.

Que la suscripta es competente para el dictado de la presente medida en virtud del artículo 22 bis de la Ley de Ministerios (t.o. 1992) y sus modificaciones.

Por ello,

LA MINISTRA DE SEGURIDAD

RESUELVE:

ARTÍCULO 1°.- Las Fuerzas Policiales y de Seguridad Federales deberán adecuar su conducta a las siguientes pautas, principios, criterios, recomendaciones y directivas para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos. Dichas tareas preventivas se llevarán a cabo únicamente mediante el uso de sitios web de acceso público y fuentes digitales abiertas entendiéndose estas como los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de

seguridad, cuyo acceso no implica una transgresión 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.

ARTÍCULO 2°.- Las Fuerzas Policiales y de Seguridad Federales desarrollarán labores preventivas en el espacio cibernético en relación con los siguientes temas:

a. Infracciones y conductas contempladas en la Ley N° 23.737.

b. Amenazas y otras formas de intimidación o coacción.

c. Infracciones a la Ley N° 20.429.

d. Hechos contemplados en la Ley N° 26.388.

e. Venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito, de violaciones a la Ley N° 22.362 u obtenidos en infracción a las disposiciones aduaneras.

f. Falsificación y comercialización de instrumentos públicos en sitios web y otros espacios virtuales.

g. Infracciones a la Ley N° 14.346.

h. Conductas que puedan comportar situaciones de acoso o violencia por motivos de género.

i. Amenaza o extorsión de dar publicidad a imágenes o datos no destinados a la publicación o sin consentimiento de quienes figuran en tales imágenes.

j. Delitos relacionados con el acoso sexual y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes.

k. Trata de personas y Tráfico de Personas.

l. Lavado de dinero.

m. Terrorismo.

n. Venta libre de elementos para los cuales se requiera autorización o dispensa legal.

o. Cualquier otro delito del que se pueda obtener noticia a través del ciberespacio.

p. Búsqueda de personas incluidas en el “PROGRAMA NACIONAL DE COORDINACIÓN PARA LA BÚSQUEDA DE PERSONAS ORDENADA POR LA JUSTICIA” o el que en el futuro lo reemplace.

q. Búsqueda de personas desaparecidas y extraviadas en el marco del Sistema Federal de Búsqueda de Personas Desaparecidas y Extraviadas.

ARTÍCULO 3º.- La labor preventiva se deberá adecuar con estricto acatamiento a los siguientes lineamientos:

a. Las actividades preventivas deberán ajustarse a las facultades dispuestas por la Constitución Nacional, Pactos Internacionales de Derechos Humanos, Leyes Nacionales y sus reglamentaciones, Leyes y Decretos orgánicos de las Fuerzas Policiales y de Seguridad Federales y sus normas reglamentarias y complementarias.

b. Utilización de fuentes digitales abiertas.

c. La judicialización de las conductas prevenidas requerirá de un análisis en función de las características comunicacionales propias del medio en que se realizan y del presunto infractor.

d. Se excluirán de la lista para su presunta judicialización aquellas conductas susceptibles de ser consideradas regulares, usuales o inherentes al uso de Internet y que no evidencien la intención de transgredir alguna norma.

e. La utilización de un “agente revelador” deberá contar con autorización judicial y ajustarse a las pautas de la ley 27.319, sus ampliaciones y modificaciones.

f. Las Fuerzas Policiales y de Seguridad Federales no podrán acumular información recabada con motivo de las investigaciones previas realizadas y, una vez concluida la actividad preventiva o decidida la no judicialización, deberá destruirse el material y datos obtenidos.

g. El personal policial interviniente deberá ajustarse a lo normado en la Ley de Protección de Datos Personales N° 25.326. Queda expresamente prohibido el tratamiento sin autorización judicial de datos sensibles -en los términos del artículo 2° de la ley precitada- y de las publicaciones efectuadas por niñas, niños y adolescentes. Cuando surja la certeza o presunción de que la tarea de prevención policial del delito en el espacio cibernético se esté desarrollando ante un menor de edad, se suspenderá y dejará constancia de ello en el libro de registro

con aviso a la autoridad responsable de la tarea, excepto cuando en el mismo momento se advirtiere que existe riesgo de vida para el menor.

h. El ciber-patrullaje no podrá interferir con la libertad de expresión constitucionalmente garantizada.

i. El personal de las Fuerzas Policiales y de Seguridad Federales estará capacitado en procedimientos, herramientas y metodologías adecuados a los principios establecidos en el presente.

j. El MINISTERIO DE SEGURIDAD publicará la presente normativa en sus redes sociales. Asimismo, se dará a conocer regularmente toda información relacionada con la cantidad de casos y personas objeto de la prevención.

ARTÍCULO 4º.- En las tareas de prevención policial del delito con uso de fuentes digitales abiertas se encuentra prohibido:

a. Obtener información, producir inteligencia o almacenar datos sobre personas o usuarios por el sólo hecho de su raza, fe religiosa, acciones privadas u opinión política.

b. Emplear métodos ilegales, prohibidos, invasivos y violatorios de la dignidad de las personas para la obtención de información.

c. Comunicar o publicitar información que viole los principios descriptos en el artículo anterior, como así también incorporar datos o información falsos.

ARTÍCULO 5°.- El uso de softwares o cualquier dispositivo o herramienta tecnológica de tratamiento de la información automatizada basada en inteligencia artificial, aprendizaje automático, sistema experto, redes neuronales, aprendizaje profundo o cualquier otra que en el futuro se desarrolle se ajustará a las estrictas necesidades de la actividad regulada en este protocolo. Su uso deberá ser supervisado por el MINISTERIO DE SEGURIDAD.

ARTÍCULO 6°.- El MINISTERIO DE SEGURIDAD establecerá los lineamientos y prioridades estratégicas para las tareas preventivas. Para ello servirán como indicador, entre otras fuentes, las estadísticas de los reportes enviados a la Dirección de Ciberdelito y Asuntos Cibernéticos, o el área que en el futuro la reemplace, y las denuncias ciudadanas recibidas a la Línea 134 que versaren sobre los delitos mencionados en el presente.

ARTÍCULO 7°.– La presente norma será de aplicación obligatoria para las Fuerzas Policiales y de Seguridad Federales.

ARTÍCULO 8°.- Las labores preventivas se desarrollarán en el marco de las directivas u órdenes de servicio emitidas por los responsables de las respectivas Fuerzas Policiales y de Seguridad Federales, las que deberán adoptar las medidas conducentes a garantizar:

a. El registro y resguardo de las directivas de puesto u órdenes de servicio elaboradas para el ejercicio de esta función.

b. El asiento y seguridad de los informes producidos por el área.

c. La trazabilidad y auditoría de las labores realizadas.

d. La comunicación de las actuaciones de prevención realizadas a las autoridades jurisdiccionales competentes.

e. La destrucción de la información obtenida y recabada cuando esta no fuera judicializada.

f. La adopción de medidas de resguardo de la información obtenida y su protección frente a posibles filtraciones.

ARTÍCULO 9°.- Mensualmente, las Fuerzas Policiales y de Seguridad Federales deberán remitir un informe de gestión a la Dirección de Ciberdelito y Asuntos Cibernéticos, o el área que en el futuro la reemplace, sobre las denuncias que hayan realizado en el transcurso del mes anterior. Dicho informe deberá contener individualizadas las causas que hayan sido iniciadas en virtud del presente protocolo.

ARTÍCULO 10.- Instrúyase a los Titulares de la POLICÍA FEDERAL ARGENTINA, la POLICÍA DE SEGURIDAD AEROPORTUARIA, la GENDARMERÍA NACIONAL, la PREFECTURA NAVAL ARGENTINA y el SERVICIO PENITENCIARIO FEDERAL a adecuar sus procedimientos a las directrices impartidas en la presente normativa.

ARTÍCULO 11.- La Dirección de Ciberdelito y Asuntos Cibernéticos, o el área que en el futuro la reemplace, conformará equipos interdisciplinarios de trabajo, los cuales podrán incluir a otras agencias del Estado,

asociaciones civiles sin fines de lucro, personas de relevancia en el campo de las ciencias informáticas o empresas comerciales, a los efectos de actualizar la normativa o complementarla.

ARTÍCULO 12.- La presente medida entrará en vigencia a partir de su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

ARTÍCULO 13.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Patricia Bullrich

e. 28/05/2024 N° 33171/24 v. 28/05/2024

Fecha de publicación 28/05/2024

II. Resolución 710/2024 del Ministerio de Seguridad

RESOL-2024-710-APN-MSG

Ciudad de Buenos Aires, 26/07/2024

VISTO el Expediente N° EX-2024-72915289- -APN-UGA#MSG, la Ley de Ministerios (texto ordenado por Decreto N° 438 del 12 de marzo de 1992) y sus modificatorias, el Decreto N° 50 del 19 de diciembre de 2019 y sus modificatorios, la Decisión Administrativa Nº 340 del 16 de mayo de 2024, la Resolución del MINISTERIO DE SEGURIDAD Nº 428 del 27 de mayo de 2024, y CONSIDERANDO:

Que la Ley de Ministerios (t.o. 1992) establece la competencia del MINISTERIO DE SEGURIDAD en todo lo concerniente a la seguridad interior, a la preservación de la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías en un marco de plena vigencia de las instituciones del sistema democrático.

Que el avance de la tecnología, en particular de la Inteligencia Artificial, representa uno de los cambios socio-tecnológicos más relevantes para la población en general.

Que países como Estados Unidos de América, China, Reino Unido, Israel, Francia, Singapur, India, entre otros, son pioneros en la utilización de la Inteligencia Artificial en sus áreas de gobierno y Fuerzas de Seguridad.

Que los mencionados países utilizan la Inteligencia Artificial en Análisis de Video y Reconocimiento Facial, Predicción de Crímenes, Ciberseguridad, Análisis de Datos, Drones y Robótica, Comunicación y Coordinación, Asistentes Virtuales y Automatización, Análisis de Redes Sociales y Detección de Fraude y Anomalías.

Que su utilización puede mejorar significativamente la eficacia y eficiencia de las distintas áreas del MINISTERIO DE SEGURIDAD y las Fuerzas Policiales y de Seguridad Federales, ayudándoles a responder más rápido y con mayor precisión a las amenazas y situaciones de emergencia.

Que estos países están a la vanguardia en la integración de tecnologías de inteligencia artificial para fortalecer la seguridad y protección de sus ciudadanos, mejorando su eficiencia y efectividad. Que por ello resulta indispensable aplicar la Inteligencia Artificial en la prevención, detección, investigación y persecución del delito y sus conexiones.

Que conforme la Decisión Administrativa Nº 340/24, le corresponde a la Dirección de Ciberdelito y Asuntos Cibernéticos: 4. Asistir a la UNIDAD GABINETE DE ASESORES en la implementación y operatividad del CENTRO DE INVESTIGACIONES DEL CIBERDELITO DE ALTA TECNOLOGÍA (CICAT) creado por la Resolución MSGN° 139/22.

Que mediante la Resolución del MINISTERIO DE SEGURIDAD Nº 428/24 se aprobaron las pautas, principios, criterios, recomendaciones y directivas para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos.

Que la conformación de Unidades de Trabajo está basada en criterios de racionalidad y eficiencia, dando lugar a estructuras dinámicas y adaptables a los cambios.

Que conforme lo expuesto deviene oportuna y necesaria la creación de una UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS) en la órbita de la Dirección de Ciberdelito y Asuntos Cibernéticos dependiente de la UNIDAD GABINETE DE ASESORES de este Ministerio.

Que la presente medida no implica erogación presupuestaria alguna.

Que el servicio de asesoramiento jurídico de este Ministerio ha tomado la intervención de su competencia.

Que la suscripta es competente para el dictado de la presente medida en virtud de las facultades conferidas en el artículo 4º, inciso b), apartados 6 y 9, y 22 bis de la Ley de Ministerios (T.O. 1992).

Por ello,

LA MINISTRA DE SEGURIDAD

RESUELVE

ARTÍCULO 1°.- Créase la UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS), que funcionará en la Dirección de Ciberdelito y Asuntos Cibernéticos dependiente de la UNIDAD GABINETE DE ASESORES.

ARTÍCULO 2°.- La UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS) estará encabezada por el Director de Ciberdelito y Asuntos Cibernéticos e integrada por las áreas de las Fuerzas Policiales y de Seguridad Federales competentes en la materia, cuyos representantes serán designados por la autoridad máxima de cada una de esas fuerzas.

ARTÍCULO 3°.- La UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS) tiene como misión la prevención, detección, investigación y persecución del delito y sus conexiones mediante la utilización de la inteligencia artificial.

ARTÍCULO 4°.- Son funciones de la UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS), en orden a la misión señalada en el artículo anterior:

a. Patrullar las redes sociales abiertas, aplicaciones y sitios de Internet, así como la llamada “Internet profunda” o “Dark-Web”, en orden a la investigación de delitos e identificación de sus autores, así como la detección de situaciones de riesgo grave para la seguridad, en el marco de la Constitución Nacional y legislación vigente.

b. Identificar y comparar imágenes en soporte físico o virtual.

c. Analizar imágenes de cámaras de seguridad en tiempo real a fin de detectar actividades sospechosas o identificar personas buscadas utilizando reconocimiento fácil.

d. Utilizar algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos.

e. Identificar patrones inusuales en las redes informáticas y detectar amenazas cibernéticas antes de que se produzcan ataques. Esto incluye la identificación de malware, phishing y otras formas de ciberataque.

f. Procesar grandes volúmenes de datos de diversas fuentes para extraer información útil y crear perfiles de sospechosos o identificar vínculos entre diferentes casos.

g. Patrullar mediante drones áreas extensas, proporcionar vigilancia aérea y responder a emergencias.

h. Realización de tareas peligrosas, como la desactivación de explosivos, mediante robots.

i. Mejorar la comunicación y coordinación entre diferentes Fuerzas Policiales y de Seguridad Federales y asegurar así que la información crítica se comparta de manera rápida y eficiente.

j. Analizar actividades en redes sociales para detectar amenazas potenciales, identificar movimientos de grupos delictivos o prever disturbios.

k. Detectar transacciones financieras sospechosas o comportamientos anómalos que podrían indicar actividades ilegales.

ARTÍCULO 5°.- La UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS) adecuará sus misiones y funciones a las pautas, principios, criterios, recomendaciones y directivas para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos aprobadas por RESOL-2024-428-APN-MSG.

ARTÍCULO 6°.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Patricia Bullrich

e. 29/07/2024 N° 48636/24 v. 29/07/2024

Fecha de publicación 29/07/2024

III. Prácticas de IA prohibidas según la LIA europea

"…Artículo 5. Prácticas de IA prohibidas

1. Quedan prohibidas las siguientes prácticas de IA:

a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un grupo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que una persona tome una decisión que de otro modo no habría tomado, de un modo que provoque, o sea probable que provoque, perjuicios considerables a esa persona, a otra persona o a un grupo de personas.

b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona o un grupo específico de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con el objetivo o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho grupo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra.

c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a personas físicas o a grupos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos enteros de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de evaluar o predecir la probabilidad de que una persona física cometa una infracción penal basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la evaluación humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no abarca el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la aplicación de la ley;

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas;

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista;

iii) la localización o identificación de una persona sospechosa de haber cometido una infracción penal a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la aplicación de la ley.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra h), debe llevarse a cabo únicamente para los fines establecidos en el apartado 1, letra h), para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra h), del presente artículo deberá satisfacer garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con la legislación nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y relativas a las personas. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad encargada de la aplicación de la ley ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se lleve a cabo sin demora indebida.

3. A los efectos del apartado 1, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se otorgará previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de 24 horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos que figuran en el apartado 1, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. No podrá adoptarse ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de la información de salida del sistema de identificación biométrica remota «en tiempo real».

4. Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

5. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión y la notificación relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de aplicación de la ley. Los Estados miembros notificarán dichas normas a la Comisión a más tardar 30 días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

6. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley con arreglo al apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado.

7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley elaborados basados en datos agregados relativos a los Estados miembros atendiendo a los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de aplicación de la ley conexas.