UNIVERSIDAD NACIONAL DE LA MATANZA

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TESIS DE MAESTRÍA

Título: **Fundamentos del Ciberpatrullaje Asistido por IA en la Lucha contra el Ciberdelito**

Autor: **Esp. Ing. Diego Javier Romero**

Director: **Mg. Ing. Jorge Esteban Eterovic**

2024

Resumen

En este trabajo se analizará el concepto de ciberpatrullaje como una actividad de vigilancia e investigación que llevan a cabo las fuerzas de seguridad en el ciberespacio. Para analizar este tema, se examinará, de manera pormenorizada, cada uno de los conceptos que tienen que ver con esta cuestión, como es el caso de la ciberseguridad, de la privacidad de los usuarios y también de la protección de los derechos que se pueden ver vulnerados. A su vez, se tendrán en consideración leyes, resoluciones internacionales y nacionales que versan sobre la seguridad de la información y la privacidad. También, se analizarán los riesgos y los desafíos que plantea el ciberpatrullaje para los derechos humanos, especialmente para la libertad de expresión y la privacidad de los usuarios, y se ahondarán las implicaciones éticas, políticas y sociales del ciberpatrullaje. Se tratará, además, la cuestión de la preservación y el análisis de las evidencias digitales como resultado del ciberpatrullaje. Asimismo, se analizará la importancia de la evolución del ciberpatrullaje con respecto a la integración de la Inteligencia Artificial (IA) y se hará énfasis sobre el cifrado y la seguridad con relación al ciberpatrullaje. Finalmente, se focalizará sobre la incidencia de la ética de la IA en la aplicación de la ley y las posibles observaciones que se le puedan realizar a la IA para consolidar el ciberpatrullaje y evitar, así, delitos.

Palabras clave: ciberpatrullaje, cibercrimen, ciberdelito, ética digital, privacidad, inteligencia artificial (IA)

Abstract

In this work, the concept of cyber patrolling will be analyzed as a surveillance and investigation activity carried out by security forces in cyberspace. To analyze this topic, each of the concepts that have to do with this issue will be examined in detail, such as cybersecurity, user privacy and also the protection of the rights that can be see violated. In turn, laws, international and national resolutions that deal with information security and privacy will be taken into consideration. Also, the risks and challenges that cyber patrolling poses for human rights will be analyzed, especially for freedom of expression and user privacy, and the ethical, political and social implications of cyber patrolling will be delved into. The issue of preservation and analysis of digital evidence as a result of cyber patrolling will also be discussed. Likewise, the importance of the evolution of cyber patrolling will be analyzed with respect to the integration of Artificial Intelligence (AI) and emphasis will be placed on encryption and security in relation to cyber patrolling. Finally, it will focus on the impact of AI ethics on law enforcement and the possible observations that can be made to AI to consolidate cyber patrolling and thus prevent crimes.

Keywords: cyber patrol, cybercrime, digital ethics, privacy, artificial intelligence (AI)

Índice

Capítulo 1 - Introducción

En la actualidad, se observa una realidad definida por una interconexión digital sin precedentes. Esta situación tiene sus aspectos tanto positivos como negativos. Por ejemplo, los criminales están explotando esta evolución para identificar y atacar vulnerabilidades en los sistemas, en las redes y en las infraestructuras digitales. Esta dinámica está generando un impacto económico y social considerable, que afecta por igual a gobiernos, a empresas e inclusive a los individuos corrientes en todo el mundo. En este sentido, esta transformación digital ha abierto nuevas potencialidades para la innovación y la comunicación, pero también ha ampliado sustancialmente el campo de acción para las actividades delictivas que comprometen la seguridad y la estabilidad de las estructuras críticas a nivel global.

Para dar un ejemplo concreto de esta coyuntura, se puede indicar que el *phishing*, el *ransomware* y las filtraciones de datos son paradigmas de las amenazas informáticas que acontecen en la actualidad puesto que, de manera constante, surgen nuevos tipos de delitos cibernéticos. Así, los ciberdelincuentes son cada vez más ágiles y organizados, dado que explotan las nuevas tecnologías, adaptando sus ataques y cooperando de nuevas maneras. Los delitos cibernéticos no conocen ni respetan fronteras nacionales y, por este motivo, atraviesan y cruzan fronteras y los delitos evolucionan rápidamente. Los delincuentes, las víctimas y la infraestructura técnica abarcan múltiples jurisdicciones, lo que plantea muchos desafíos a las investigaciones y los enjuiciamientos.

En este contexto surge el ciberpatrullaje, una actividad de vigilancia que consiste en monitorear, analizar y recolectar información de fuentes digitales abiertas, como las redes sociales, con el fin de prevenir o investigar delitos. Sin embargo, esta práctica también implica riesgos y desafíos para los derechos humanos, especialmente para la privacidad y la libertad de expresión de los usuarios de internet. Desde el punto de vista legal, el ciberpatrullaje debe estar regulado por normas claras, precisas y proporcionales, que establezcan los límites, las garantías y los controles necesarios para evitar abusos o arbitrariedades por parte de las autoridades. Además, debe respetar los principios de legalidad, necesidad y proporcionalidad, que son fundamentales para proteger los derechos de las personas en el ámbito digital.

En Argentina, el ciberpatrullaje ha generado controversia y debate, debido a que desde hace años no existe una ley específica que lo regule y, asimismo, se han conocido casos de persecución o criminalización de expresiones en las redes sociales. En 2020, el Ministerio de Seguridad derogó la Resolución 31/2018 que habilitaba el ciberpatrullaje y la reemplazó por la Resolución 144/2020 que busca establecer criterios más transparentes y participativos, con la intervención de organizaciones de la sociedad civil. Sin embargo, esta resolución no resolvió todas las cuestiones que plantea el ciberpatrullaje y, por este motivo, es necesario una revisión de las bases de esta cuestión.

En este sentido, es necesario un debate amplio y definitivo sobre el ciberpatrullaje, que involucre a todos los actores interesados y que tenga en cuenta un marco ético, así como también los estándares internacionales de derechos humanos. De esta forma, se podría definir un marco legal adecuado que garantice la seguridad, pero también el respeto a la dignidad, la intimidad y la libertad de las personas en el entorno digital.

Ahora bien, para analizar el ciberpatrullaje, es imprescindible analizar algunos conceptos que ayudarán a definir de manera más precisa ese ámbito, a saber: ciberseguridad, ciberespacio y, puntualmente, dos conceptos que se ven impelidos a partir de la utilización del ciberpatrullaje: la privacidad y, por sobre todas las cosas, los derechos humanos. En este trabajo se elaborará un examen acerca de estos conceptos para alcanzar una base sólida que permita indagar acerca del tema de este trabajo.

A su vez, se hará mención a una cuestión fundamental a la hora de analizar el tema de la seguridad informática en estos tiempos: la Inteligencia Artificial (IA) y, sobre todo, como se efectuó la integración de la IA al ciberpatrullaje. En este estudio, se indagará sobre cómo la IA está adquiriendo una relevancia creciente en el ámbito de la seguridad cibernética, proporcionando recursos y métodos novedosos para protegerse contra peligros cada vez más complejos. Principalmente, se analizará el contexto actual, en el cual el ciberdelito representa una de las amenazas más representativas vinculadas a la seguridad global y se identificará como organismos gubernamentales o privados están aplicando, de forma gradual, tecnologías de IA para mejorar sus actividades de ciberpatrullaje.

Otro tema que será analizado es un asunto complejo: cómo la misma tecnología de IA utilizada por los profesionales de la seguridad informática está siendo, al mismo tiempo, empleada por delincuentes. Es fundamental identificar cómo los profesionales en ciberseguridad aplican la IA para implementar prácticas sólidas de seguridad cuando, de forma simultánea, esta tecnología es utilizada por grupos criminales en línea, como *hackers* con motivaciones ideológicas y por atacantes respaldados por algunos Estados, los cuales pueden aprovechar las mismas técnicas para superar las defensas y evitar ser detectados.

Por estos motivos, se mencionará cuáles son las formas correctas de implementación y aplicación de la IA en cuestiones de ciberseguridad y, también, se relevarán los requisitos en que se produce el cifrado de la comunicación. Esta situación debe ser atendida, dado que los hechos de delincuencia informática implican la necesidad imperiosa de utilizar herramientas de cifrado de las comunicaciones en el marco de las tecnologías informáticas, para generar las condiciones necesarias a la hora de permitir que se adicione una capa de inviolabilidad técnica no normativa a los actos comunicativos intermediados por las tecnologías.

Capítulo 2 - Marco Teórico

No se puede hablar de ciberseguridad, de ciberpatrullaje o de vulneración de los derechos a partir de la vigilancia, si no se habla del ciberespacio, es decir, del ámbito donde se desarrolla esa actividad. De esta manera, se plantea un escenario en el que generalizaciones como ciberseguridad y ciberespacio deben ser definidas adecuadamente para comprenderlas en su justo contexto. De todos modos, no se tiene un acabado conocimiento acerca de hasta qué punto pueden afectar la vida cotidiana de los ciudadanos, tanto a nivel personal como profesional. Los conceptos de ciberseguridad y ciberespacio son términos muy complejos, dado que ciberseguridad implica un nuevo paradigma de seguridad global de los escenarios que se van a ver afectados por la impronta que introduce la existencia y la utilización del ciberespacio.

En este sentido, la Organización de Estados Americanos (OEA) dispone de un Programa de Seguridad Cibernética, cuyo principal objetivo radica en promover que los Estados miembros adopten estrategias nacionales de seguridad cibernética (OEA, 2020). No obstante, ese programa no brinda un concepto propio de ciberseguridad. Inclusive, para el caso argentino, la Resolución del JGM N° 580/11 que crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) menciona el concepto de ciberseguridad, pero no le reporta ninguna definición rigurosa.

Por su parte, la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de la Organización de las Naciones Unidas (ONU) para las tecnologías de la información y la comunicación (TIC), define a la ciberseguridad en la Recomendación X.1205, de la siguiente manera:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios y los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. (UIT, 2008)

La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad.

La UIT propone unos aspectos mediante los cuales se podría dividir el enfoque de la definición de ciberseguridad, que variará de acuerdo con los fines de quienes hacen uso del término. De esta manera, se podría concebir a la ciberseguridad como la misión de las fuerzas de seguridad para proteger las infraestructuras, las redes, los datos y los usuarios nacionales, para, de esa manera, investigar, prevenir y abordar el delito digital (ciberdelito). También, puede definirse como una actividad de vigilancia realizada por una agencia de inteligencia. El concepto ciberentorno aportado por la UIT resulta equivalente al de ciberespacio.

El ciberespacio es un concepto que se emplea dentro de la comunidad de las TIC y se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicación e informáticos. Las TIC son un conjunto de tecnologías requeridas para el almacenamiento, recuperación, proceso y comunicación de la información, mediante diversos soportes tecnológicos tales como computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video, entre otros. En los últimos años, las TIC han tenido un valor inestimable en muchas disciplinas, pero sobre todo con respecto a la educación, puesto que su aporte ha sido fundamental y positivo (Fojón Chamorro y Sanz Villalba, 2010).

Para dar un ejemplo acerca del ciberespacio y la tecnología, con respecto a la defensa de un país, la UIT ha precisado el concepto de ciberespacio como una cuestión que excede lo trivial en el ámbito militar, dado que en los últimos tiempos se considera a este concepto como un dominio militar más, que se suma a los clásicos de Tierra, Mar, Aire y Espacio. Con respecto a este tema, es decir, a lo estrictamente militar, se debe indicar que el ciberespacio es el dominio global y dinámico compuesto por las infraestructuras de tecnologías de la información (incluida internet), las redes, los sistemas de información y telecomunicaciones (Quintana, 2016).

Ahora bien, para alcanzar una definición de ciberespacio que permita comprender las implicaciones referidas anteriormente, es fundamental recurrir al concepto de servicio, entendido como la prestación que recibe un usuario o consumidor por parte de un proveedor. En

consecuencia, el ciberespacio es el conjunto de medios y procedimientos basados en las TIC y configurados para la prestación de servicios.

Una característica importante para examinar el tema del ciberpatrullaje es la cuestión de la seguridad en sí. Este fenómeno posee una modalidad transnacional que suele soportar los procesos delictuales y/o criminales. En este sentido, la Organización de Estados Americanos (OEA) ofrece una perspectiva sobre el progreso alcanzado desde su primera edición. Establece que las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías (OEA, 2020, p. 10). Se debe resaltar, que en los respectivos Estados Miembros de la OEA, la ciberseguridad se ha visto afectada considerablemente en diversas formas, ya sea por amenazas tradicionales o por las nuevas amenazas emergentes del siglo XXI.

Dada la temática escogida, resulta esencial discernir el concepto de seguridad en el ciberespacio. Por un lado, se establece como una cualidad que percibe un determinado actor, respecto a una situación dada en su contexto, y por el otro, como aquellas acciones llevadas a cabo por el actor en cuestión, a los efectos de alcanzar una situación ideal. La seguridad sería tanto una situación ideal que en forma simplificada podría caracterizarse como de ausencia de amenazas, o como el conjunto de medidas y políticas conducentes a ese objetivo (Bartolomé, 2006, p. 21). Así, al hablar de seguridad, es factible encontrar un conjunto de diversos términos, donde se destacan la seguridad informática, seguridad de la información y ciberseguridad.

La cantidad de información requerida estará sujeta a la estrictamente necesaria para caracterizar y poder gestionar la tipología de las amenazas, evitando especialmente la recolección y procesamiento que afecte la privacidad de las personas. A tal efecto, se mantendrá una plataforma segura y confidencial de colaboración en materia de incidentes de ciberseguridad con el objeto de agregar la información pertinente y, en conjunto con otros órganos públicos y privados, se establecerá una red de trabajo.

Cuando se hace referencia al ciberpatrullaje y se lo entiende como la vigilancia y monitoreo de actividades en el ciberespacio por parte de las fuerzas de seguridad se generan

complejidades, dado que pueden verse vulnerados ciertos derechos. Debe indicarse que esta situación ha generado un intenso debate en Argentina. La tensión entre la seguridad pública y la privacidad individual es evidente y notoria, especialmente cuando se trata de garantizar las libertades fundamentales en el contexto de la digitalización de la sociedad.

Es fundamental analizar la constitucionalidad de estas prácticas de vigilancia por parte de las fuerzas de seguridad, dado que se puede cuestionar cómo se pueden establecer parámetros objetivos para construir una sospecha razonable que justifique la intrusión del Estado en la privacidad de los individuos a través de las TIC. Con la sociedad de la información las distinciones sobre lo público, lo privado y lo íntimo se volvieron más ambiguas y difusas, y por ende, más problemáticas para el derecho y, especialmente, para el derecho penal y la investigación del delito (Monte y Sánchez, 2021, p. 1-2). Dada esta naturaleza, las primeras normativas que se han concretado en todo el mundo han sido ciertamente conservadoras, restringidas a marcos nacionales y sin una perspectiva internacional. A partir de allí, es necesario reforzar y consolidar mejores leyes para evitar tensiones.

Asimismo, es importante introducir una definición detallada del concepto de la IA dado que es una noción que atravesará todo este trabajo, sobre todo a partir de sus vínculos con la ciberseguridad.

La *National Cyber Security Centre* (NCSC) define a la IA como cualquier sistema informático que puede realizar tareas que normalmente se asocian a la inteligencia humana. Esto podría incluir la percepción visual, la generación de texto, el reconocimiento de voz o la traducción entre idiomas. Uno de los desarrollos recientes más notables en IA se produjo en el campo de la IA generativa: una herramienta que puede producir diferentes tipos de contenido, tales como texto, imágenes, vídeos y combinaciones de más de un tipo, en el caso de herramientas "multimodales" (NCSC, 2024). La mayoría de las herramientas de IA generativa están orientadas a tareas o dominios específicos, como es el caso de *ChatGPT*, un instrumento que permite a los usuarios "hacer una pregunta" como lo haría cualquier ser humano durante una conversación con un *chatbot* (aplicación software que simula mantener una conversación con una persona al proveer respuestas automáticas). Por su parte, herramientas como *DALL-E* pueden crear imágenes digitales mediante descripciones en lenguaje natural. En un futuro

podría ser posible, si continúa este desarrollo tecnológico, que modelos como estos puedan ser capaces de producir contenido para una gama más amplia de situaciones. En este sentido, empresas de tecnología como *Open AI* y *Google* notifican grandes rendimientos en una variedad de factores de referencia para sus respectivos modelos *GPT-4* y *Gemini*.

¿Cómo funciona la IA? La mayoría de las herramientas de IA se crean utilizando técnicas de aprendizaje automático (ML, del inglés *Machine Learning*) que consiste en que los sistemas informáticos encuentran patrones en los datos o resuelvan problemas de manera automática, prescindiendo de la programación realizada por un ser humano. El ML define mecanismos (algoritmos) para que los sistemas basados en IA "aprendan" en forma automática a partir de datos y, posteriormente, generalicen lo aprendido (NCSC, 2024).

Además, es importante hacer referencia a los modelos de lenguaje grande (LLM, del inglés *Large Language Model*) que son un tipo de IA generativa que puede producir diversos estilos de texto que interpretan y emulan el contenido creado por un ser humano. Para posibilitar esto, un LLM debe estar "entrenado" en una amplia cantidad de datos, que tiene que estar sustentados en texto, generalmente extraídos de internet. Dependiendo del LLM, este proceso puede incluir, potencialmente, páginas web y diversos contenidos de código abierto, específicamente: investigaciones científicas, libros y publicaciones en redes sociales. El proceso de formación del LLM cubre un volumen de datos muy vasto y, por este motivo, no es posible revelar la totalidad de este contenido, por lo cual, es factible que abarque material "discutible" o incorrecto en su modelo.

Como se ha podido advertir, cuando se hace referencia a la IA, es imposible no mencionar el concepto de *big data*. Esta noción se vincula a conjuntos de datos extremadamente grandes y complejos que sobrepasan la capacidad de las herramientas de procesamiento de datos tradicionales que se empleaban para capturar, almacenar, gestionar y analizar de manera efectiva información en un tiempo razonable. Se denomina *big data* al conjunto de procedimientos computacionales aplicados para analizar gran cantidad de datos con el fin de extraer información que presente ciertos patrones, relaciones y asociaciones relevantes para una organización (Márquez Díaz, 2020, p. 324).

Se debe indicar, que estos conjuntos de datos se caracterizan específicamente por su volumen, velocidad y variedad. Algunos investigadores, posteriormente, han adicionado otras características como la veracidad, el valor y la variabilidad. Estos seis adjetivos propios para el desarrollo de un proyecto de investigación pueden ser definidos de la siguiente manera: el "volumen", en el campo del *big data*, demanda grandes recursos de procesamiento y almacenamiento de información, que están representados en la "variedad" de los datos, que pueden ser de tipo estructurados y no estructurados. Con respecto a la "velocidad", hace referencia a la cantidad de datos que se generan periódicamente y requieren de una infraestructura tecnológica escalable que permita su disponibilidad y acceso en cualquier momento (Márquez Díaz, 2020, p. 324). Con respecto a la "veracidad" y "valor", es fundamental que los datos que se almacenan sean verdaderos y auténticos, porque en caso contrario, se estarían desperdiciando una gran cantidad de recursos computacionales que conducirían en resultados y toma de decisiones erróneas o equivocadas. En cuanto al "valor", se debe comprender en el sentido de extraer información relevante para definir estrategias y toma de decisiones. De este modo, es imprescindible que se apliquen y utilicen, de manera decidida, las peculiaridades específicas mencionadas en este apartado para, de esa manera, garantizar la información veraz y confiable para que pueda ser implementada en sistema de IA (Márquez Díaz, 2020, p. 325).

Capítulo 3 - Importancia de una Regulación

3.1. Normativa Internacional

Para concretar una tarea sólida y transparente sobre este tema, es fundamental establecer una legislación que regularice el ciberpatrullaje. Dicha normativa debe ser precisa y proporcionada, asegurando que las garantías procesales y los derechos humanos sean respetados. Esto implica un marco legal que delimite claramente las facultades de las fuerzas de seguridad, estableciendo límites y controles estrictos para evitar abusos.

En este sentido, es imprescindible, como se ha visto, una normativa asentada en una base que no vulnere los derechos de las personas. Para ello, es vital observar las regulaciones que se han establecido a nivel internacional. En EE. UU., en la Unión Europea y en el Reino Unido se ha constituido una serie de regulaciones sobre el tema analizado en este trabajo, que ha sido objeto de un pormenorizado análisis por parte de muchos países del mundo. Por ejemplo, en los EE. UU. se han sancionado normativas como la *"USA Patriot Act"* en el 2001; ley *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) en 2018; la Ley de Protección de la Privacidad en Línea para Niños (COPPA, del inglés *Children's Online Privacy Protection Act*) en 1998; la Ley de Privacidad en las Comunicaciones Electrónicas (ECPA, del inglés *Electronic Communications Privacy Act*) promulgada en el año 1986. En la Unión Europea se sancionaron normativas como el Reglamento 2016/679 en 2018. Este reglamento es conocido como el Reglamento General de Protección de Datos de la Unión Europea (GDPR, del inglés *General Data Protection Regulation*); mientras que en 2002 se promulgó la Directiva sobre Privacidad y Comunicaciones Electrónicas de la UE (*ePrivacy Directive*). Por su parte, en el Reino Unido se sancionó la Ley de Poderes de Investigación del Reino Unido de 2016 (*Investigatory Powers Act* 2016). Por otro lado, en la región es importante mencionar el caso de Brasil, particularmente, la sanción en 2018 de la Ley General de Protección de Datos Personales de Brasil (LGPD), que fue aprobada por el Parlamento de Brasil como Ley N.º 13.709 en agosto de 2018.

Luego de lo presentado hasta aquí, resulta relevante pensar una manera de indagar sobre el ciberpatrullaje, no para condenar su práctica puesto que es una herramienta necesaria en estos tiempos, sino para velar por los derechos de las personas, que en muchas ocasiones se ven

vulneradas debido al incorrecto manejo que hacen las fuerzas de seguridad con este tipo de vigilancia. Entonces, a partir de lo analizado, se puede sintetizar una idea de lo que se podría esperar de una sociedad en la que exista un ciberpatrullaje sólido y eficiente, pero que respete y se ajuste a las reglas que protejan la privacidad de las personas. De este modo, es menester pensar una regulación que podría ser implementada por cualquier país que desee constituir una legislación sólida que vele por los derechos de las personas en los casos de monitoreo por ciberpatrullaje.

3.2. Regulación en Argentina

En el caso de Argentina, se podrían adoptar e implementar nociones de las normativas internacionales y regionales para, posteriormente, pensar las maneras adecuadas para que el ciberpatrullaje no perjudique los derechos personales y la privacidad de las personas. No obstante, en los casos en los cuales se detecte algún tipo de abuso de los mecanismos de vigilancia, es importante conocer las herramientas legales para poder resolver estos inconvenientes.

Argentina debe valerse de las normativas que ya han sido probadas en su desempeño a nivel internacional, dado que hay países que poseen varios años de experiencia en el tema. De esta manera, es fundamental adaptar esas normativas a la idiosincrasia del país. En este sentido, por ejemplo, se podría tomar lo esgrimido por el *CLOUD Act* para permitirle a las autoridades nacionales que obliguen a las empresas tecnológicas con sede en el país para que suministren los datos solicitados que se encuentran almacenados en los servidores, independientemente de si éstos se hallan en el país o en el extranjero. Asimismo, habría que considerar lo indicado por el *Patriot Act*, dado que ampliaría el poder del Estado y las agencias de inteligencia para alcanzar la vigilancia y la búsqueda de datos, sobre todo para cuestiones de combate contra el terrorismo, puesto que proporciona a las autoridades un amplio acceso a los datos personales.

En Argentina, el ciberpatrullaje no está legislado específicamente, pero las actividades de prevención están amparadas bajo el "Protocolo General de Actuación para las Fuerzas de Seguridad y Policiales en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos", creado en 2016, que ha quedado efectiva a partir de la Resolución 144/2020.

Además, el Ministerio de Seguridad de Argentina ha propuesto un protocolo de ciberpatrullaje que se desarrolló en consulta con organizaciones de derechos humanos y sociales (Ybañez, 2020).

Como se ha señalado anteriormente, un buen ejemplo para ser tomado como modelo es el Reglamento General de Protección de Datos europeo, la ley GDPR de la UE. Adaptando esta ley a la realidad de Argentina, se podrían proteger los datos personales y la forma en la que las organizaciones los procesan, almacenan y, finalmente, destruyen, cuando esos datos dejan de ser útiles. Una de las peculiaridades de esta ley "es el principio de *accountability* (o responsabilidad proactiva) que sostiene que el responsable del tratamiento de datos no sólo debe cumplir con la normativa de protección de datos, sino que también debe poder demostrarlo y rendir cuentas de su proceder" (Ybañez, 2020).

Ahora bien, el tema tratado en este trabajo es un tema que está en constante progreso, dado que la tecnología avanza cotidianamente. Por ese motivo, los mecanismos de control deben ser reforzados a diario dado que los delitos se suceden a ritmos vertiginosos y dotándose de nuevas herramientas.

Con respecto a esta cuestión, algo que debe ser tenido en consideración en lo que respecta al ciberpatrullaje tiene relación con nuevas tecnologías como la IA y el *big data*, puesto que actualmente se utilizan estos instrumentos para cuestiones de ciberseguridad. Es primordial, que se implementen abordajes legales que aseguren la transparencia y el control sobre estas tecnologías para minimizar los riesgos a los derechos de las personas, englobando a la privacidad. Es imprescindible que se prevenga sobre el riesgo de dependencia acrítica en los algoritmos que, a lo largo del tiempo, podría conducir a una peligrosa vigilancia masiva y, tal vez, a la discriminación (Martín Ríos, 2022).

Esta consideración acrítica en los algoritmos hace referencia a una particularidad peligrosa y compleja: el desconocimiento con respecto al funcionamiento de la actividad algorítmica puede generar dos posturas excesivas y contradictorias, que se traducen en aceptar de manera incondicional las conclusiones del alcance de los algoritmos o, por el contrario, que se genere una desconfianza consolidada en relación con las respuestas que puedan ofrecer. Este énfasis en la transparencia de los mecanismos para atender los inconvenientes provocados por el

ciberpatrullaje son indispensables para un respeto exhaustivo de los derechos humanos de las personas para no llegar a vulnerarlos.

El último informe de *Freedom House* (organización no gubernamental con sede en Washington D. C. y con oficinas en cerca de una docena de países, que conduce investigaciones y promociona la democracia, la libertad política y los derechos humanos) indicó que las democracias "han registrado un monitoreo masivo de la población a través de las agencias gubernamentales que se están utilizando para nuevos propósitos sin las garantías adecuadas" (Ybañez, 2020). Esto significa que los organismos gubernamentales han hecho un uso abusivo con respecto a las libertades civiles y, también, indica una marcada reducción del espacio en línea para el activismo cívico. De este modo, se puede observar como el derecho a la privacidad contemplado en el artículo 12 de la Declaración Universal de Derechos Humanos "se ha visto desafiado por diversas conductas que los gobiernos, las empresas y los propios particulares han realizado con las fuentes abiertas, ámbito en el cual la frontera entre lo público y lo privado no se encuentra claramente delimitada". En este sentido, es imprescindible una educación ciudadana con respecto a sus derechos relacionados con los datos personales y el ciberespacio, puesto que en ciertas ocasiones los mismos ciudadanos entregan la privacidad cuando, por ejemplo, crean un perfil en una red social.

Así, el ciudadano debe robustecer su responsabilidad dinámica y activa, es decir, cada ciudadano debe tomar de manera proactiva el control y decidir qué hacer en cada momento, anticipándose a los acontecimientos. ¿Por qué es importante esto? Porque las herramientas tecnológicas se han instalado en la sociedad y se quedarán instaladas allí, arraigadas. De este modo, es importante que se incremente la consciencia de cada ciudadano, pero también debe consolidarse la eficiencia y la transparencia de las distintas agencias de control del Estado. Para ello, como se presentará a lo largo de este trabajo, es necesario crear una legislación vigorosa que regule el uso de herramientas de monitoreo de redes sociales por parte de los privados, los Estados y, especialmente, por sus fuerzas de seguridad.

En resumen, el ciberpatrullaje es una herramienta esencial para mantener la seguridad en el ciberespacio. No obstante, su implementación debe realizarse de manera que se respete y se proteja la privacidad de las personas. Sólo a través de un equilibrio minucioso entre estas dos

necesidades es como se podría aprovechar los beneficios del ciberpatrullaje mientras se protegen los derechos fundamentales de las personas en el ciberespacio.

Capítulo 4 - Vigilancia y Vulneración de Derechos

Es necesario destacar el rol sustancial que debe tener el Estado valiéndose de la ética para hacer frente a estas problemáticas. En este apartado, se propone un puntapié, una puesta en funcionamiento para comenzar a indagar acerca de la ética con respecto a la ciberseguridad, sobre todo en relación con el ciberpatrullaje, la privacidad y la vulneración de derechos. La ética aplicada es una rama de la filosofía que emerge en la relación de las diferentes esferas de la sociedad a partir de problemas morales y éticos.

En el momento actual, los avances tecnológicos e informáticos son cada vez más notorios y emergen debates complejos al respecto. En esos debates se analizan cuestiones como la informática, la ética y la información que se transmite a través de internet. La ética en relación con la ciberseguridad y la privacidad es un aspecto novedoso que merece una aguda reflexión en este país, puesto que comprender estos problemas ayudarían a mejorar el tema del ciberpatrullaje y los derechos de las personas.

Es fundamental proponer una nueva forma de saber, de reflexionar sobre los problemas morales de las tecnologías de la información que lleven a recomendaciones para la acción. Las sociedades que se encuentran interconectadas son “las que han exigido su nacimiento y actuación, son ellas las que precisan de este saber interdisciplinar para su acción en la vida pública, siendo un bien de primera necesidad para determinar la altura moral de una sociedad” (Romero Muñoz, 2017, p. 57). En la era digital es necesario un conocimiento mayor sobre las nuevas formas de transmitir información, que han cambiado, cambian y cambiarán la vida de los sujetos.

Es perentorio profundizar sobre el tema de la privacidad, ya que “la aceleración de la tecnología implica poder gestionar grandes cantidades de datos, informaciones y conocimientos, lo que a su vez lleva consigo importantes problemas de seguridad y privacidad” (Palos-Sanchez et al., 2018, p. 18). En este sentido, lo que resulta de esta idea, es que la tecnología de la información acelera sus pasos a un ritmo vertiginoso y se debe mantener la atención sobre la privacidad. También, se debe priorizar la cuestión de la privacidad cuando se habla de ciberpatrullaje porque, si bien es imprescindible que el Estado de un país coloque sus

focos en asegurar los derechos sobre los datos de los usuarios del ciberespacio muchas veces, como se vio en este trabajo, esta tarea se realiza a través del ciberpatrullaje y esa protección no debe vulnerar la privacidad de los ciudadanos. Es en este punto donde la ética del ciberespacio debe reforzarse y ser una prioridad para los funcionarios que se ocupan de este tema.

Todo lo que se ha hablado hasta aquí, refiere al carácter normativo que podría tener una regulación robusta a nivel nacional. No obstante, lo esencial en este caso, es indagar no sólo en las regulaciones sino en cómo se vulneran los derechos de las personas en cuanto a su privacidad, dado que ha quedado en manifiesto que a pesar de una normativa establecida, se puede llevar a cabo ciertas acciones que vulneran los derechos de la privacidad de las personas y que, en muchos casos, puede llevar a una vulneración de los derechos humanos de la sociedad civil que se puede ver perjudicada por leyes que violenten la manera en que se ejecute el ciberpatrullaje.

En este sentido, las fuerzas estatales que se ocupan de la seguridad informática presentan herramientas cada vez más específicas para perseguir delitos que también se comportan bajo herramientas cada más más modernas, transformándose en una suerte de competencia o carrera tecnológica. Por ejemplo, en el marco de la persecución policial contra la pedofilia o contra el *grooming* (acoso sexual de una persona adulta a una niña, un niño o un adolescente por medio de internet), las fuerzas se valen de la IA para construir perfiles falsos que, con el objetivo de ser atrayentes para determinados tipos de criminales, son utilizados como señuelos.

Sobre este aspecto, es necesario comprender que sucede algo similar "con los conocidos como *honey pots* o *honey monkeys*, aunque en estos casos el reclamo es el propio sitio web, creado *ad hoc* con idéntica finalidad" (Martín Ríos, 2022, p. 8). En los dos supuestos se corre el riesgo de que el margen con la provocación policial se desdibuje en un exceso y se frustre el proceso.

Hay un punto que es central en toda esta cuestión, el de la protección de los derechos de las personas con respecto al ciberpatrullaje. Es crucial atender el tema de los derechos humanos porque se encuentran protegidos, es decir, son derechos inalienables y fundamentales que todo individuo detenta por el mero hecho de ser humano y no pueden ser vulnerados con motivo de

ciertos monitoreos específicos en materia de ciberseguridad. Cuando se llevan a cabo tareas de ciberpatrullaje, los integrantes de las fuerzas de seguridad:

> Monitorean de forma masiva e indiscriminada palabras claves en publicaciones de usuarios de redes sociales con la supuesta finalidad de "anticiparse a la comisión de delitos". Tales prácticas que consisten en observar lo que las personas publican sin definir previamente qué se busca y a quienes se observa son conocidas como "excursiones de pesca" y están estrictamente prohibidas por leyes locales e internacionales. Estas prácticas, no cumplen salvaguardias básicas de derechos humanos tales como la legalidad, la necesidad y la proporcionalidad. (Pisanu, 2023)

Por tales motivos, estas acciones se encuadran en el marco de lo que se conoce como inteligencia de fuentes abiertas (OSINT, del inglés *open-source intelligence*) e inteligencia en redes sociales (SOCMINT, del inglés *social media intelligence*). ¿En qué medida corre riesgo la libertad de una persona cuando las fuerzas de seguridad realizan este tipo de operaciones? Por ejemplo, cuando se realiza el monitoreo de las redes sociales "por parte del gobierno implica importantes riesgos para la privacidad y la libertad de expresión de los usuarios" (Pisanu, 2023). De esta forma, esta cuestión no sólo incluye un monitoreo detallado de cuestiones privadas, sino que inclusive los contenidos públicos pueden manifestar una extensa cantidad de detalles sobre un usuario, ya sea porque revela sus opiniones, sus intereses, sus familiares, su trabajo, su economía, su ubicación, entre otras cuestiones.

En este sentido, se presenta algo que es una forma de reprensión: la autocensura, dado que en muchas ocasiones una persona puede "sentir", sospechar, que el gobierno está monitoreando sus mensajes y, de esa manera, se genera un efecto inhibidor, a través del cual la persona se cuida de emitir ciertos juicios, o redactar o dar conocer sus pensamientos de manera directa, por miedo a ser observado y, posteriormente, penalizado por eso mismo. Como se puede advertir, esto es un claro ejemplo de censura, de una magnitud tal, que lleva a la persona a autocensurarse sin que el Estado ejerza una prohibición de manera directa.

Aquí se plantea una disyuntiva bastante evidente: las normativas que se legislen sobre estos temas deben ser claras de manera manifiesta, puesto que la línea que delimita a la vigilancia de la protección es muy difusa. Esta pregunta ya la planteó el Centro de Estudios en

Libertad de Expresión y Acceso a la Información (CELE) cuando examinó el tema del Protocolo de la Resolución Nº 144/2020 del Ministerio de Seguridad de la Nación. Sobre este aspecto:

> El Protocolo levanta otra discusión relativa al encuadre debido a estas actividades: ¿son tareas de prevención del delito o tareas de inteligencia? Atento al impacto de estas prácticas en nuestros derechos fundamentales, en particular la afectación a los derechos de libertad de expresión y privacidad, es necesario que la naturaleza jurídica de la actividad esté claramente establecida. (CELE, 2020)

De este modo, si no queda delimitada categóricamente esa división, la vulneración de los derechos humanos se volvería muy palpable. En el caso de Argentina, la Constitución y los tratados internacionales de los derechos humanos establecen una serie de garantías procesales que protegen a los individuos frente a la acción del Estado. Entre estas garantías se encuentran: el derecho a la privacidad, la presunción de inocencia y el debido proceso. El ciberpatrullaje, por su naturaleza, puede entrar en tensión con estos derechos, puesto que implica una forma de vigilancia que podría considerarse invasiva.

¿Hay herramientas que se utilizan para el ciberpatrullaje y que son más nocivas que otras? Para profundizar sobre este aspecto importante del tema, es relevante destacar la importancia de la inteligencia de fuente abierta (OSINT), que es una práctica que se encuentra generalizada y que es incompatible con el estado de derecho. En este sentido, la inteligencia de fuente abierta vulnera dos aspectos elementales:

1. La privacidad de las personas: las personas, por más que saben que sus expresiones en la esfera pública pueden llegar a ser monitoreadas, como pueden ser las redes sociales, tienen una expectativa de privacidad en la que esperan que no se haga seguimiento de sus expresiones, ni se recolecte ni se haga un tratamiento de esa información porque eso constituye tareas de inteligencia.
2. Ejerce una forma de condicionamiento del discurso público: esto posee un impacto sobre el derecho de libertad de expresión de las personas. Como ejemplo de este punto, se pueden mencionar acciones de ciberpatrullaje que conllevan a allanamientos y a detenciones de personas por sus expresiones de “violencia política” en ciertas redes sociales (Busaniche, 2000, como se citó en De Amo, 2000).

La vulneración de la privacidad de las personas es un punto crítico y el ciberpatrullaje, en pos de la justicia, puede llegar a cometer ciertos atropellos o desviaciones. Es conveniente resaltar que las personas tienen el derecho privado de poder mantener en la sociedad una esfera particular de protección sobre su propia información, sobre sus propias pertenencias y sobre sus propias opiniones, no sólo en la esfera privada, sino en la esfera pública, es decir, ya sea en el marco de su intimidad, como en la calle o en las redes sociales. Lo que los organismos de defensa de los derechos de las personas reclaman es que, en la realidad, se impone una diferencia, que es que las autoridades "parecen desaparecer" cuando las personas se hallan vigiladas a través del ciberpatrullaje. Las personas no saben que son vigiladas ni cómo son vigiladas. ¿Por qué sucede esto? Porque no se puede advertir, observar, percibir lo que hacen los que vigilan, ni tampoco cómo lo hacen. Las personas no conocen, tampoco, qué hacen con la información que las fuerzas de seguridad toman de sus redes sociales cuando son vigiladas, ni cómo utilizan esa información.

En este sentido, sucede como si el poder público se esfumara y comenzara a abrirse un enorme espacio vacío, gris, donde entra en juego la arbitrariedad, lo fortuito, que puede desencadenar en el abuso de autoridad. En definitiva, parece ser un espacio sin garantías civiles. Es por estos motivos que se cree necesario regular de manera eficiente el ciberpatrullaje para que se lleve a cabo de manera segura, respetando los derechos humanos, para que las personas puedan conducirse en internet de manera segura, conociendo los límites y certezas y, lo más importante, si la persona comete un delito, sepa cuáles son las penas por ese delito cometido.

Las posibilidades de cometer abusos sobre los derechos humanos están latente constantemente mediante el uso del ciberpatrullaje, y es por esta causa que es imprescindible elaborar procedimientos de vigilancia que deberán "permanecer abiertos al escrutinio público y ser revisados regularmente" (Pisanu, 2023). Sin esta condición, la confianza de la sociedad en el gobierno puede verse seriamente afectada. Asimismo, si bien es necesaria la vigilancia dada la cantidad de delitos que se comenten en las redes con cada vez mayor asiduidad, no deben utilizarse mecanismos en base a engaños, es decir, "las autoridades no pueden obtener acceso a información usando perfiles falsos como señuelo" (Pisanu, 2023).

De esta manera, para prevenir este tipo de abusos, los programas para el monitoreo de redes sociales no se pueden implementar o llevar a la práctica de facto. Por el contrario, deben ser puestos a prueba, sometidos a un estricto examen de forma generalizada. Las fuerzas que realicen el ciberpatrullaje deben ser entrenadas y capacitadas, y deben estar preparadas para generar reportes cotidianos sobre el empleo y la competencia de esa clase de programas. Dichos programas de vigilancia deberán, al mismo tiempo, "ser sometidos a auditorías de rutina y el resultado final debe estar disponibles para el público para su revisión" (Pisanu, 2023).

Por su parte, sería relevante atender los requerimientos del CELS, que propone una serie de observaciones que pueden llegar a aportar una eficiente política de seguridad en materia de seguridad informática que se encuentre de acuerdo con los valores democráticos y tipificados de derechos humanos, en concreto, que se discutan y clarifiquen los alcances de regulaciones concordantes con herramientas y controles adecuados en materia de ciberpatrullaje. Esta institución citada no niega la importancia de este método de vigilancia, pero focaliza sobre la vulneración de derechos en ciertas prácticas como las que ya se han advertido anteriormente en este trabajo. Asimismo, se recomienda que las fuerzas federales de seguridad dejen de llevar a la práctica actividades de vigilancia de carácter indiscriminado en fuentes abiertas. Por último, se cree imperioso que se constituya una sólida y contundente "normativa general que discutan los protocolos para todas las policías provinciales" (CELS, 2020, p. 10).

En el mundo de las leyes, las autoridades sólo pueden obrar de acuerdo con lo que les está deliberadamente permitido. Esta regla es el principio de legalidad y es una de las bases más elementales de los sistemas jurídicos democráticos modernos. Así, las autoridades de seguridad pública estarían actuando de manera ilegal si realizan acciones que no tienen facultadas. Por lo tanto, el ciberpatrullaje parece ser una medida de vigilancia estatal, la cual sería algo que se encontraría prohibido de hecho sin un marco que la regule. A su vez, la Ley de Inteligencia Nacional (25.520) es clara en su artículo 4° (incisos 2 y 3) en prohibir exactamente el tipo de actividades que se realizan por medio del ciberpatrullaje (Chorny, 2020).

Dado que la vigilancia en internet se engloba dentro del ámbito de la ciudadanía y de la libertad de expresión, debe ser razonable y apropiada para ser considerada una restricción adecuada. Sólo se tiene conocimiento de ello si las actividades de vigilancia, por ejemplo, la

inteligencia o el ciberpatrullaje, pueden pasar este filtro, inclusive si estas actividades fueran ilegales. De este modo, la privacidad se ve comprometida porque el monitoreo a través de internet puede acceder a la privacidad de las personas que aparecen en las redes sociales. El gobierno de Argentina experimentó llevar a cabo "una analogía de que las redes sociales funcionan como el espacio público" (Chorny, 2020).

Por estos motivos, las autoridades estarían legitimadas para actuar. No obstante, las autoridades olvidarían que el derecho a la privacidad no se desvanece en el espacio público y que este mismo lugar es un lugar donde se pueden ver y fiscalizar las acciones de las autoridades. De este modo, se debe delimitar estrictamente el espacio público del privado, aun en materia de redes sociales, para que las personas puedan mantener su esfera de protección.

Por último, se cree importante adicionar que actualmente, más allá de las regulaciones que se establecieron en países puntuales y que se han mencionado en este trabajo, hay un marco internacional que garantiza que la vigilancia respete los derechos humanos. Particularmente, se hace referencia a los que se mencionan sobre la temática comprendida en este trabajo. Si se debe indicar uno de ellos sería *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, un texto creado por asociaciones ciudadanas de todo el mundo para articular como las normas y estándares internacionales de derechos humanos se aplican en el contexto de la vigilancia de las comunicaciones. Estos *Principios* sostienen que la vigilancia debe ajustarse a "13 Principios" para respetar los derechos humanos. Entre los más destacados se encuentran los principios de necesidad y proporcionalidad, según los cuales la vigilancia debe ser la única forma para conseguir un objetivo legítimo y proporcionada con el objetivo pretendido.

Esta cuestión es un imperativo para los Estados, dado que no hay nada más importante que la libertad de expresión en la base de las naciones, aun en momentos de crisis. Por estos motivos, Amnistía Internacional ha indicado que, a pesar de que los Estados estén atravesando tiempos extraordinarios o de crisis, el derecho de los derechos humanos sigue siendo aplicable. De hecho, el marco de los derechos humanos tiene por objeto garantizar un cuidadoso equilibrio de los distintos derechos para proteger a las personas y las sociedades en general. Así, este movimiento global que trabaja por la promoción y defensa de los derechos humanos resalta que

los Estados no pueden desatender los derechos como la privacidad y la libertad de expresión con cualquier pretexto, por ejemplo, la gestión de una crisis de salud pública. Por el contrario, los Estados deben velar por la garantía estricta de estos derechos y deben asegurar que toda restricción esté ajustada a la conservación y preservación de los derechos humanos ya instaurados (Amnistía Internacional, 2020).

En definitiva, ha quedado demostrado que el ciberpatrullaje es un mecanismo importante de las fuerzas de seguridad, para tener el control de ciertos delitos que se han visto generalizados a partir de internet pero, al mismo tiempo, ese mecanismo de monitoreo no puede violentar las garantías de los derechos de las personas, sino que deben ser empleados de manera cautelosa, profesional y sin un exceso del poder estatal. En su accionar, este poder sólo debe combatir al delito. De este modo, no puede, simultáneamente, vulnerar de tal forma los derechos humanos que las personas vean peligrar su libertad y se cuiden de manera desmesurada, por ejemplo, a través de la autocensura, por miedo a ser registrados por ese mecanismo de vigilancia.

Capítulo 5 - Preservación y Análisis de las Evidencias Digitales

Es imprescindible que una vez que se haya realizado el ciberpatrullaje, esos datos puedan ser almacenados y examinados. En consecuencia, una vez que se han relevado y examinado los datos, esa evidencia debe ser conservada y preservada. En definitiva, toda la prueba que se haya tomado debe ser almacenada con el objetivo de poder ser analizada posteriormente y, sobre todo, para asegurarla y protegerla. Lo fundamental es que esa información almacenada, relevada y analizada, debe quedar salvaguardada en un soporte informático para que pueda ser utilizada como prueba del delito que se ha cometido.

En este sentido, se debe indicar que el desarrollo pronunciado y sustancial, así como la condición activa que presenta el ciberdelito, requiere de una constante actualización de las prácticas de intervención por parte de los cuerpos forenses al momento de llevar a cabo las tareas de las pericias científicas. De esta manera, es primordial generar las condiciones para asegurar la preservación de la evidencia digital para que, posteriormente, esta evidencia se traduzca en pruebas que deberán ser analizadas en el proceso legal. Se debe indicar que en dicho proceso se aplicarán técnicas analíticas concretas que posibilitarán que se determinen, analicen, conserven y expongan esos datos digitales obtenidos de los dispositivos analizados.

Con respecto al análisis en sí de los datos recolectados, "el análisis digital forense es la aplicación de técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal" (Roatta et al., 2015, p. 2). Es imprescindible que este proceso esté constituido de esta manera para que pueda generar las condiciones para mantener la inviolabilidad de la evidencia digital, a partir de un sistema que facilite la legitimidad en cuanto a los procesos legales y, sobre todo, que tenga concordancia con la norma ISO/IEC 27037:2012. Esta norma es decisiva, dado que brinda las pautas para el correcto tratamiento de la evidencia digital, logrando una identificación, relevamiento, adquisición y preservación de los datos. Así, estos procesos deben diseñarse para mantener la integridad de la evidencia y con una metodología aceptable para contribuir a su admisibilidad en procesos legales (Roatta et al., 2015, p. 3).

De esta manera, la norma garantiza que las personas que son las encargadas de la evidencia digital la manipulen a partir de prácticas aceptadas por todos los organismos internacionales, con la finalidad de propiciar una investigación de una manera metodológica y, particularmente, justa, para preservar su fiabilidad y veracidad. Asimismo, es primordial establecer que la evidencia digital a la que se hace referencia puede obtenerse de diferentes tipos de dispositivos digitales, redes, bases de datos, etc. (Roatta et al., 2015, p. 3). De este modo, esta norma está dirigida a aquellos que exigen la determinación de la credibilidad de la evidencia digital que deben operar.

Particularmente sobre esta cuestión, sería conveniente desarrollar algunos aspectos de esta norma y de la subsiguiente, publicada en el año 2020. La norma ISO/IEC 27037:2012, denominada "Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital" establece pautas para la gestión de la evidencia digital en el contexto de la seguridad de la información. Concretamente, se dirige hacia la identificación, adquisición y preservación de la evidencia digital de manera que se mantenga su integridad y fiabilidad durante todo el proceso.

Esta norma es sustancial en lo que respecta a las garantías que requiere la evidencia digital al ser recopilada en investigaciones de seguridad de la información, para que sea válida y pueda ser utilizada de manera efectiva en los procesos legales, las auditorías internas o las investigaciones forenses. La norma brinda directrices pertinentes acerca de cómo recopilar y preservar datos digitales de manera que cumplan con los estándares de integridad y autenticidad requeridos por las autoridades legales y reguladoras.

Por otra parte, es importante señalar que la versión más reciente, la norma ISO/IEC 27037:2020, representa una actualización que refleja los avances y los cambios en el ámbito de la seguridad de la información y la tecnología digital desde la publicación de la versión anterior. Si bien sigue manteniendo los mismos principios fundamentales de identificación, adquisición y preservación de evidencia digital, la versión actualizada puede incluir mejoras en términos de claridad, precisión y relevancia para los desafíos y tecnologías emergentes.

La norma ISO/IEC 27037:2020 puede abordar temas fundamentales, tales como: (a) la gestión de la cadena de custodia; (b) la autenticidad de la evidencia digital en entornos altamente

distribuidos; (c) la consideración de la privacidad de los datos durante la adquisición de evidencia; y (d) la adaptación a nuevas tecnologías y modelos de almacenamiento de datos.

En definitiva, tanto la norma ISO/IEC 27037:2012 como su versión actualizada, la de 2020, son herramientas esenciales para garantizar la integridad y la fiabilidad de la evidencia digital en el contexto de la seguridad de la información, proporcionando directrices claras y actualizadas para la identificación, adquisición y preservación de datos digitales en investigaciones forenses y procesos legales.

Actualmente, se vive en una época de "extimidad", es decir, una propensión de las personas a hacer pública su intimidad que se ha ido desarrollado con la evolución de la tecnología. En definitiva, existe actualmente una gran exhibición de determinados datos y, por otro lado, existe la obligación "de preservar determinados datos como herramienta fundamental para poder decidir un plan de vida en un contexto de razonable libertad" (Asociación por los Derechos Civiles, 2017, p. 20).

Es esencial establecer una clara distinción entre pruebas de cargo y prueba de redireccionamiento, para poder definir adecuadamente ambos conceptos. Para la organización mencionada, esta diferenciación entre pruebas de cargo y prueba de redireccionamiento en la investigación es sustancial, puesto que en el sistema procesal argentino "los expedientes en una prueba de cargo pueden demorar mucho tiempo" (Asociación por los Derechos Civiles, 2017, p. 6). No obstante, surge un inconveniente que debe ser resuelto de manera eficaz. Este problema emerge cuando una evidencia digital que debe ser abordada para redirigir la investigación y pueda ser realizada en el mismo laboratorio que está ejecutando ese otro tipo de conocimientos especializados, esto es, la prueba de cargo. Por consiguiente, "la única manera de evitar listas de espera es dividir laboratorios que realizan pericias forenses conocidas como pruebas de cargo y otros laboratorios que se dediquen exclusivamente al apoyo en la investigación" (Asociación por los Derechos Civiles, 2017, p. 6). En este sentido, es importante indicar que, cuando se accede al secuestro de dispositivos, es frecuente el secuestro de elementos como teléfonos, memorias y *pendrives*. Sin embargo, se debe resaltar, que habitualmente no se procede al secuestro de impresoras y/o *smartwatches* para realizar el análisis de la información que pudieran contener, puesto que se desconoce que pueden contener información significativa.

Por otra parte, teniendo en consideración estas cuestiones, es fundamental desarrollar y profundizar sobre los conceptos para que no se generen errores teóricos sobre el tema. Por este motivo, se cree imperioso definir qué significa el elemento material, es decir, el componente físico de un sistema de información y la información que se encuentra contenida en ese soporte. Es fundamental generar las condiciones necesarias para establecer una distinción notoria y sensible entre el elemento material de un sistema informático o hardware, es decir, la evidencia electrónica, y la información contenida en este, es decir, la evidencia digital. Esta distinción es oportuna con ocasión de diseñar "los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital" (Acurio Del Pino, 2010, p. 3). Se debe indicar, que en este ámbito el hardware hace referencia a todos los componentes físicos de un sistema informático, en tanto que la información hace referencia a la totalidad de los datos, de los programas almacenados y de los mensajes de datos transmitidos utilizando el sistema informático.

Para comprender minuciosamente esta distinción llevada a cabo en el párrafo precedente, es imprescindible poder diferenciar el hardware de la información. En principio, el hardware provee evidencia electrónica. En este sentido, el hardware es una mercancía ilegal o el fruto del delito, así, "es una mercancía ilegal cuando su posesión no está autorizada por la ley" (Acurio Del Pino, 2010, p. 4). Es importante citar un ejemplo sobre esta cuestión, indicando el caso de los decodificadores de la señal de televisión por cable. La posesión de este componente es una violación a los derechos de propiedad intelectual y, además, conlleva un delito. Adicionalmente, "el hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción" (Acurio Del Pino, 2010, p. 4).

A su vez, el hardware es considerado un instrumento cuando cumple un papel clave en el proceso del delito. Se puede señalar que es utilizada como un arma o una herramienta, tal como si fuera un arma de fuego o un arma blanca. Como ejemplo de esto, se puede indicar a los *sniffers* y otros dispositivos diseñados, específicamente, para capturar el tráfico en la red o cuando se interceptan las comunicaciones[1].

[1] Se debe aclarar, que los *sniffers* son programas de captura de las tramas de una red de computadoras.

Finalmente, el hardware es considerada una evidencia, cuando no es una mercancía ilegal fruto del delito o un instrumento. De este modo, "es un elemento físico que se constituye como prueba de la comisión de un delito" (Acurio Del Pino, 2010, p. 4). Como ejemplo, se puede mencionar el caso del *scanner* que se emplea con el objetivo de digitalizar imágenes de pornografía infantil, cuyas particularidades únicas son utilizadas como elementos de convicción.

En lo que concierne a la información, se debe señalar que esta suministra evidencia digital, concretamente:

> La información es una mercancía ilegal o el fruto del delito cuando es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo, en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados. (Acurio Del Pino, 2010, p. 4)

Además, la información es un instrumento cuando es empleada como un medio para incurrir en una infracción penal. Un ejemplo claro de esto se genera en el caso de "los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado" (Acurio Del Pino, 2010, p. 5). En resumidas cuentas, funcionan y se desempeñan como un eslabón crucial en lo que respecta a la realización o al acatamiento de un delito.

Por último, con respecto a la información como evidencia, se puede señalar que es una categoría más vasta y robusta que las anteriores, puesto que muchas de las acciones cotidianas de los individuos dejan algún tipo de rastro digital. Así, una persona puede obtener mucha información como evidencia, concretamente "la información de los ISP's (proveedores de servicios de internet), de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos" (Acurio Del Pino, 2010, p. 5).

Es esencial conocer los dispositivos de almacenamiento de los datos relevados. Los dispositivos de almacenamiento son utilizados para conservar los mensajes de datos y la información de los dispositivos electrónicos. Estos dispositivos de almacenamiento se pueden dividir en tres clases, a saber: (a) dispositivo magnético (como son los discos duros o los

disquetes); (b) dispositivos de estado sólido (SSD, del inglés *solid-state drive*) o memoria solida (como son las memorias *flash* y dispositivos USB); (c) dispositivos ópticos (como es el caso de los discos compactos y DVD). Al mismo tiempo, hay una gran variedad de memorias USB en el mercado electrónico y diversos dispositivos de almacenamiento como es el caso de las tarjetas SD, *Compact flash*, Tarjetas XD, *Memory Stick*, entre otros.

Existe una serie de buenas prácticas en lo que respecta al almacenamiento de la evidencia, a saber:

- Recolección de las instrucciones de uso, de los manuales y de las notas de cada uno de los dispositivos encontrados;
- Documentación de todos los pasos al revisar y recolectar los dispositivos de almacenamiento;
- Apartar los dispositivos de almacenamiento de cualquier magneto, radio transmisor u otros dispositivos potencialmente dañinos. (Acurio Del Pino, 2010, p. 13)

Por otra parte, es imprescindible que el Estado conozca y comprenda estas cuestiones y que genere las condiciones necesarias para configurar un correcto y eficiente procedimiento con ocasión de llevar a cabo la recolección de la evidencia digital. El Ministerio de Seguridad publicó en 2023 el *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*. Este informe, determina una secuencia de cuestiones importantes, concretamente:

- Definir las pautas y los procedimientos al que se deberán atener los miembros de las Fuerzas Federales Policiales y de Seguridad a la hora del proceso de identificación, recolección, preservación, procesamiento y presentación de evidencia digital asociada a cualquier delito y, en particular, los ciberdelitos (delitos ciber asistidos y ciber dependientes);
- Determinar los procedimientos específicos de secuestro para el primer interviniente, clasificados por tipo de dispositivo electrónico, como es el caso de celulares, notebooks, equipos de escritorio, servidores, equipos de imagen de video, criptoactivos, *rigs* de minería y redes informáticas;

- Integrar los flujogramas de los procedimientos de secuestro para una consulta precisa e inmediata en el campo;
- Detallar las directrices para la intervención técnica-forense por parte del personal especialista en el laboratorio. (Ministerio de Seguridad, 2023, p. 3)

Este procedimiento destaca la importancia de consolidar una oficina especializada, con personal calificado para las intervenciones. De esta forma, la oficina especializada en actividades forenses de cada institución estatal llevará a cabo tareas técnico-periciales adecuadas y pertinentes a su función, en relación con los PEP digitales (potencial elemento de prueba, de carácter digital). Se debe aclarar que, como consecuencia de las particularidades de cada tipo de tecnología, los procedimientos que se aplican pueden llegar a presentar diferencias en cuanto al mismo. Esto se da de esta manera, dado que no son idénticas las tareas para la extracción de datos de un teléfono, de un equipo informático, o de otro dispositivo electrónico. El protocolo dispuesto por el ministerio indica que, entre las incumbencias y responsabilidades de la oficina especializada propuesta, el personal experto solamente procederá "a la creación de imágenes forenses o extracción, categorización (decodificación) de datos, generación de los reportes pertinentes junto con el informe técnico y actas de estilo, quedando expresamente excluida la realización de tareas de análisis respecto de la información extraída" (Ministerio de Seguridad, 2023, p. 20). Ahora bien, con respecto a la información que se extraiga, esta deberá ser enviada al área de análisis que corresponda: la autoridad judicial, la dependencia preventiva o aquel organismo que tenga conocimiento de los detalles pormenorizados de la investigación, en concordancia a lo establecido por la autoridad judicial.

Teniendo en consideración lo señalado hasta aquí, es pertinente conocer y comprender la importancia del tratamiento minucioso y detallado de la evidencia digital. La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y la Dirección General de Cooperación Regional e Internacional (DIGCRI), indican que la información que se almacenan en los dispositivos de los proveedores de servicios puede ser eliminada. Ahora bien, esto puede ocurrir por dos razones, concretamente:

> Por acción del usuario, que puede borrar información puntual (por ejemplo, fotos, publicaciones, mensajes) o eliminar definitivamente la cuenta, o por el transcurso del tiempo, en tanto razones económicas o de otra naturaleza pueden llevar a que los proveedores decidan almacenar los datos por un periodo limitado (por ejemplo, los logs de acceso a las cuentas). (UFECI y DIGCRI, 2020, p. 12)

Por estos motivos, si se tiene en cuenta la inestabilidad y la variabilidad de la evidencia digital, es conveniente que se requiera de una sólida preservación de los datos tan pronto como se notifique que pueden ser datos de interés para la investigación que se está llevando a cabo. Es importante resaltar, que ciertos datos pueden desaparecer rápidamente sin dejar registros visibles. De esta manera, es sustancial preservar la evidencia a la mayor brevedad posible. La preservación de la evidencia digital "permite mantener a disposición de la autoridad judicial los registros de la cuenta en el momento de materializar la operación, de forma tal que estén disponibles frente a un eventual pedido que se canalice antes del vencimiento de la medida" (UFECI y DIGCRI, 2020, p. 12).

Como se puede advertir, es fundamental la instancia en la que se solicite preservar y proteger la información básica del suscriptor, un procedimiento que suele ser relativamente simple y breve. Es conveniente aclarar que, en el ámbito de la información digital, un suscriptor es una persona que paga una tarifa periódica o una suscripción para acceder a contenido digital, tales como noticias, revistas, servicios de transmisión de música o video, entre otros. Esta suscripción puede proporcionar un acceso ilimitado a ciertos contenidos o servicios durante un período de tiempo determinado.

Se debe indicar que la mayor parte de los prestadores de servicios importantes, disponen de un portal para las fuerzas de seguridad o de un correo electrónico al que se puede contactar para concertar esta clase de acciones. Para los organismos citados, es sustancial que se revisen los términos y condiciones de las compañías a las que se les solicitará la información. Sobre todo, es crucial que se les exija la entrega de "los aspectos de privacidad (donde indican qué información guardan, por cuánto tiempo y cómo la comparten) y las directrices para las fuerzas de la ley (en las que suele detallarse el procedimiento para cursar los requerimientos)" (UFECI y DIGCRI, 2020, p. 14).

La realización de este tipo de acciones puede ser llevada a cabo por cualquier fiscal a cargo. La UFECI se encuentra a disposición para concretar este tipo de medidas y, también, para responder consultas con respecto "a las firmas con las que se suele trabajar frecuentemente (Facebook, Instagram, WhatsApp, Twitter, Zoom, Netflix, etc.) o a fin de contactar a empresas (en particular, en el extranjero) para establecer cómo realizar una preservación" (UFECI y DIGCRI, 2020, p. 14). No obstante, según el proveedor y la autoridad competente en la que se encuentre localizado, es plausible que no se sienta inclinado a cumplir con las exigencias cursadas, de manera inmediata, por las autoridades judiciales radicadas en el exterior.

Sobre esta cuestión, UFECI y DIGCRIE publicaron la *Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero*. Este procedimiento propone una serie de pautas para especificar las buenas prácticas que deben desempeñar los especialistas a la hora de obtener información electrónica almacenada en el extranjero. En este apartado se ha observado cómo se puede analizar y almacenar posteriormente los datos relevados como evidencia. Pero ¿qué sucede cuándo esa evidencia se encuentra en el extranjero? En principio, es importante resaltar que la mayor parte de las empresas a las que se le solicita información en función de las investigaciones "se encuentran radicadas en los EE. UU. o en la Unión Europea, por lo que hace especial foco en las regulaciones que permiten solicitar información a compañías radicadas dichas jurisdicciones" (UFECI y DIGCRI, 2020, p. 7). Resulta sustancioso indicar que tanto Argentina como los EE. UU. forman parte del Convenio sobre Ciberdelito del Consejo de Europa (ETS N° 185), también conocida como Convención de Budapest, firmado en 2001. Este convenio ayuda a los expertos a la hora de reclamar cierto tipo de información para la investigación que realizan.

Capítulo 6 – Beneficios del Convenio de Budapest en el Contexto del Ciberpatrullaje

La ciberdelincuencia se ha convertido en una amenaza global que exige respuestas coordinadas y efectivas a nivel internacional. En este escenario, el Convenio de Budapest se destaca como el primer y más significativo tratado internacional que aborda de manera integral los delitos informáticos. Este capítulo examina los beneficios específicos que el Convenio de Budapest aporta al ciberpatrullaje, subrayando cómo facilita la implementación de prácticas de monitoreo y vigilancia en línea de manera efectiva, al mismo tiempo que respeta los derechos humanos.

6.1. El Convenio de Budapest: Un Marco Legal Integral

6.1.1. Objetivos y Alcance

Adoptado en 2001, el Convenio de Budapest tiene como objetivo principal armonizar las legislaciones nacionales, mejorar las técnicas de investigación y promover la cooperación internacional en la lucha contra la ciberdelincuencia (Consejo de Europa, 2001). Entre sus disposiciones más importantes se encuentran la criminalización del acceso ilegal a sistemas informáticos (Artículo 2), la interferencia en datos (Artículo 4) y sistemas (Artículo 5), así como la producción y distribución de pornografía infantil (Artículo 9). Además, el Convenio aboga por la actualización constante de sus disposiciones para enfrentar nuevas formas de ciberdelincuencia, asegurando así su relevancia en un entorno digital en constante evolución (Consejo de Europa, 2021).

6.1.2. Medidas Procedimentales

El Convenio introduce medidas procedimentales fundamentales que se aplican directamente al ciberpatrullaje, tales como:

- Búsqueda e Incautación de Datos Informáticos: de acuerdo con el Artículo 19 del Convenio de Budapest, las autoridades tienen la facultad de acceder a sistemas

informáticos y confiscar datos relevantes, estableciendo un marco legal estandarizado para estas acciones entre los países miembros. Este artículo especifica que la búsqueda y la incautación de datos informáticos deben llevarse a cabo de acuerdo con la legislación nacional correspondiente, asegurando así una implementación consistente y legal en todas las jurisdicciones.

- Intercepción de Comunicaciones: el Artículo 21 del Convenio de Budapest permite la interceptación de datos en tiempo real, lo cual es esencial para el monitoreo de actividades sospechosas en línea. Este artículo establece que la interceptación debe ser autorizada conforme a la legislación nacional y debe incluir las salvaguardias adecuadas para proteger los derechos humanos y la privacidad de los individuos.
- Conservación Rápida de Datos: los Artículos 16 y 17 del Convenio de Budapest autorizan la conservación inmediata de datos informáticos potencialmente relevantes para investigaciones criminales. El Artículo 16 focaliza en la preservación de datos de tráfico específicos, permitiendo a las autoridades ordenar a los proveedores de servicios que mantengan estos datos por un período limitado. Por otro lado, el Artículo 17 aborda la conservación de datos ya almacenados, asegurando que se mantengan disponibles para futuras investigaciones.

Ampliación de las Medidas Procedimentales

Se debe indicar, que el convenio determina una serie de medidas para ejecutar los procedimientos, a saber:

- Búsqueda y Acceso Remoto: el Artículo 19 autoriza la búsqueda y el acceso remoto a datos almacenados en sistemas informáticos situados en otras jurisdicciones, bajo ciertas condiciones. Esto facilita la cooperación internacional en investigaciones transnacionales.
- Recopilación en Tiempo Real de Datos de Tráfico: el Artículo 20 permite la recopilación en tiempo real de datos de tráfico, lo cual es fundamental para rastrear la actividad en línea y prevenir delitos cibernéticos antes de que se materialicen.

- Producción de Datos por Terceros: el Artículo 18 faculta a las autoridades para exigir a terceros, como los proveedores de servicios, la entrega de datos específicos necesarios para la investigación, simplificando así la obtención de pruebas esenciales.

El Segundo Protocolo Adicional al Convenio de Budapest, adoptado en 2021, fortalece estas medidas al establecer disposiciones específicas para la cooperación internacional en la obtención de pruebas electrónicas y la asistencia mutua en el acceso directo a datos transfronterizos. Este protocolo agiliza el intercambio de información y fomenta la colaboración entre autoridades de distintos países, mejorando así la capacidad para abordar delitos cibernéticos complejos y transnacionales (Consejo de Europa, 2022). Además, introduce mecanismos como la solicitud de conservación de datos transfronterizos y la cooperación directa entre autoridades y proveedores de servicios, reduciendo la burocracia y acelerando los procesos de investigación.

6.1.3. Provisión para la Flexibilidad y Adaptación

El Convenio de Budapest reconoce la importancia de adaptarse a la rápida evolución tanto en tecnología como en criminalidad. Por ello, contempla disposiciones para la enmienda y actualización periódica de sus términos, garantizando que permanezca pertinente y eficaz frente a nuevas amenazas y métodos delictivos (Consejo de Europa, 2021).

6. 2. Beneficios del Convenio de Budapest para el Ciberpatrullaje

6.2.1. Marco Legal y Estándares Uniformes

Uno de los principales beneficios del Convenio de Budapest es la creación de un marco legal uniforme que simplifica la implementación del ciberpatrullaje. Al armonizar las definiciones de delitos y los procedimientos legales entre los Estados Parte, el Convenio asegura que las prácticas de ciberpatrullaje se realicen bajo un marco legal claro y coherente, reduciendo así las ambigüedades legales y los posibles abusos (Consejo de Europa, 2001; Consejo de Europa, 2021).

Esta armonización es fundamental para garantizar que las acciones de vigilancia y monitoreo se ajusten a normas aceptadas internacionalmente, estableciendo una base sólida para la cooperación internacional en la lucha contra la ciberdelincuencia.

Ampliación del Marco Legal

- Tipificación de Nuevos Delitos: el Convenio de Budapest impone la obligación de legislar sobre delitos emergentes relacionados con las tecnologías de la información, como el fraude informático (Artículo 8) y las infracciones asociadas al contenido, como la pornografía infantil (Artículo 9). Esta exigencia garantiza que las legislaciones nacionales permanezcan actualizadas y pertinentes frente a las nuevas amenazas cibernéticas.
- Protección de Infraestructuras Críticas: los artículos del Convenio también se ocupan de la protección de infraestructuras críticas al tipificar delitos que afectan la integridad, disponibilidad y confidencialidad de los sistemas informáticos. Esto asegura la seguridad de las infraestructuras esenciales para el funcionamiento de la sociedad.

6.2.2. Mejora de la Cooperación Internacional

El Convenio de Budapest, junto con su Segundo Protocolo Adicional, fomenta la cooperación internacional, un elemento clave para el éxito del ciberpatrullaje. Gracias al Convenio, los países pueden intercambiar información y coordinar operaciones conjuntas de manera más eficiente, lo que resulta fundamental para enfrentar la naturaleza transnacional de muchos delitos cibernéticos. Esto permite respuestas rápidas y efectivas a incidentes que afectan a múltiples jurisdicciones (Consejo de Europa, 2001; Consejo de Europa, 2021). La cooperación internacional potencia la capacidad de los países para investigar y prevenir delitos cibernéticos al facilitar el intercambio de información y la colaboración en investigaciones transnacionales, lo que es crucial para desmantelar redes de ciberdelincuencia complejas y bien organizadas.

El Segundo Protocolo Adicional del Convenio de Budapest fortalece esta cooperación al introducir mecanismos para la asistencia mutua y el acceso directo a datos transfronterizos. Por

ejemplo, permite a las autoridades de un país solicitar directamente a un proveedor de servicios en otro país la conservación y entrega de datos electrónicos, lo que agiliza de manera significativa el proceso de obtención de pruebas.

Ampliación de la Cooperación Internacional

- Asistencia Jurídica Mutua: el Convenio y el Segundo Protocolo Adicional facilitan la asistencia jurídica mutua en investigaciones cibernéticas, permitiendo la ejecución de órdenes judiciales y la colaboración en tiempo real entre las autoridades de distintos países.
- Centros de Coordinación: la implementación de puntos de contacto disponibles las 24 horas del día, como estipula el Artículo 35 del Convenio, asegura una comunicación ágil y efectiva entre las autoridades de los Estados Parte, optimizando así la capacidad de respuesta inmediata a incidentes cibernéticos.

6.2.3. Simplificación en la Obtención de Pruebas Electrónicas

El Convenio establece procedimientos detallados para la obtención de pruebas electrónicas, esenciales para el ciberpatrullaje. La capacidad de conservar y acceder de manera ágil a datos electrónicos relevantes facilita la identificación y persecución de delitos cibernéticos. Estas disposiciones permiten a las autoridades recopilar pruebas de forma eficiente y legal, fortaleciendo así las investigaciones criminales (Consejo de Europa, 2001; 2021). Además, el Segundo Protocolo Adicional introduce medidas para la conservación rápida de datos y el intercambio directo de información entre proveedores de servicios y autoridades, simplificando los procesos y aumentando la eficiencia en la obtención de pruebas electrónicas (Consejo de Europa, 2022).

El Segundo Protocolo Adicional también incorpora disposiciones para la cooperación directa entre autoridades de aplicación de la ley y proveedores de servicios, lo que permite un acceso rápido a datos cruciales para las investigaciones.

Estas directrices establecen mecanismos de asistencia mutua y procedimientos simplificados para la transferencia de datos, disminuyendo los obstáculos burocráticos y legales en las investigaciones transnacionales.

Ampliación en la Obtención de Pruebas Electrónicas

- Datos Transfronterizos: el Segundo Protocolo Adicional facilita el acceso a datos transfronterizos mediante acuerdos de cooperación directa entre autoridades y proveedores de servicios, lo cual resulta fundamental para las investigaciones que abarcan múltiples jurisdicciones.
- Intercambio de Información en Tiempo Real: la capacidad de intercambiar información en tiempo real entre autoridades de distintos países optimiza la prevención y la respuesta a incidentes cibernéticos, permitiendo una gestión más efectiva y oportuna de las situaciones.

6.3. Desafíos y Consideraciones Éticas

6.3.1. Protección de los Derechos Humanos

A pesar de sus ventajas, el ciberpatrullaje presenta desafíos importantes en términos de privacidad y protección de datos. El Convenio de Budapest incluye salvaguardas para garantizar que las medidas de vigilancia sean proporcionales y respeten los derechos humanos (Consejo de Europa, 2001; 2021). Es fundamental que las actividades de ciberpatrullaje se lleven a cabo con transparencia y una supervisión adecuada para prevenir abusos y proteger la privacidad de los individuos.

Las autoridades deben equilibrar la necesidad de seguridad con la protección de los derechos fundamentales, asegurándose de que las medidas de vigilancia no se utilicen para abusos o controles indebidos. Entre las salvaguardas se encuentran la supervisión judicial y la evaluación continua de la proporcionalidad de las medidas adoptadas, conforme al Artículo 15 del Convenio.

Salvaguardas y Supervisión Judicial

- Supervisión Judicial Independiente: las medidas de vigilancia deben estar sometidas a una supervisión judicial independiente, garantizando que cualquier invasión en la privacidad de los individuos se lleve a cabo únicamente con la autorización de un juez y de acuerdo con procedimientos legales establecidos.
- Evaluación de Proporcionalidad: la proporcionalidad de las medidas de vigilancia debe ser evaluada de manera continua para asegurar que no se sobrepasen los límites necesarios para la seguridad pública, preservando así los derechos fundamentales.

6.3.2. Transparencia y Rendición de Cuentas

Las autoridades deben garantizar la transparencia en sus actividades de ciberpatrullaje y rendir cuentas sobre el uso de los datos recopilados. Esto implica la implementación de mecanismos de supervisión independientes que puedan evaluar la legalidad y proporcionalidad de las operaciones de vigilancia (Consejo de Europa, 2001; Schulkin, 2018).

La transparencia y la rendición de cuentas son cruciales para mantener la confianza pública y asegurar que las prácticas de ciberpatrullaje se lleven a cabo de manera ética y legal. La presencia de órganos de supervisión independientes y la disponibilidad de mecanismos de queja son fundamentales para proteger los derechos de los ciudadanos y garantizar la legitimidad y efectividad del ciberpatrullaje en un contexto democrático. Estos mecanismos incluyen auditorías regulares de las prácticas de ciberpatrullaje y la publicación de informes de transparencia.

Ampliación en la Transparencia y Rendición de Cuentas

- Supervisión Judicial: la implementación de una supervisión judicial sólida asegura que todas las medidas de ciberpatrullaje se realicen de acuerdo con la ley y respeten los derechos humanos. Las autoridades deben obtener las autorizaciones judiciales necesarias antes de llevar a cabo determinadas operaciones de vigilancia, garantizando así un control independiente.

- Evaluaciones de Impacto: realizar evaluaciones de impacto en la protección de datos y la privacidad antes de implementar nuevas tecnologías de ciberpatrullaje garantiza que los riesgos potenciales se identifiquen y se mitiguen de manera efectiva.

6.4. La Adhesión de Argentina al Convenio de Budapest

En 2018, Argentina se unió a la Convención de Budapest sobre delitos informáticos, marcando un avance significativo en su compromiso de combatir la ciberdelincuencia. La adhesión al Convenio implica la adopción de sus estándares y procedimientos, fortaleciendo así el marco legal y operativo del país para enfrentar los delitos cibernéticos (Schulkin, 2018). Esta integración facilita la cooperación internacional, permitiendo a Argentina beneficiarse del intercambio de información y la asistencia judicial con otros Estados Parte del Convenio, lo que mejora su capacidad para investigar y perseguir delitos informáticos de manera más efectiva y coordinada.

Argentina formalizó su adhesión a través de la Ley 27.411, promulgada en 2017, que incorpora las disposiciones del Convenio en el marco legal nacional. La implementación de esta ley también ha permitido a Argentina acceder a recursos y conocimientos internacionales, fortaleciendo su capacidad para responder a amenazas cibernéticas de manera más eficiente y eficaz.

En 2022, Argentina se unió al Segundo Protocolo Adicional del Convenio de Budapest, subrayando su compromiso con la cooperación internacional y la optimización de su capacidad para obtener pruebas electrónicas transfronterizas. Esta adhesión conlleva la implementación de nuevas medidas para la rápida conservación de datos y el intercambio directo de información entre proveedores de servicios y autoridades, lo que mejora tanto la eficiencia como la efectividad en las investigaciones cibernéticas (Consejo de Europa, 2022).

La Ley 27.411 establece las bases para la cooperación internacional en la lucha contra la ciberdelincuencia y garantiza que las autoridades argentinas puedan emplear herramientas modernas y eficientes para investigar y procesar delitos cibernéticos. Esta ley también fomenta la formación continua de profesionales en ciberseguridad, asegurando que las fuerzas del orden

y los fiscales estén debidamente capacitados para enfrentar los desafíos de la ciberdelincuencia actual. Además, la Ley 27.411 incluye disposiciones específicas para la protección de los derechos humanos, garantizando que las actividades de ciberpatrullaje se lleven a cabo de manera transparente y respetuosa con la privacidad de los individuos.

El impulsor de la incorporación de Argentina en l Convención de Budapest es Marcos Salt, coordinador académico del Programa Nacional Contra la Criminalidad Informática del Ministerio de Justicia. Para este abogado, Argentina empezó a indagar acerca de la Convención de Budapest, con varios altibajos, pero manteniendo siempre una actitud positiva. De este modo, en los últimos tiempos se ha reavivado la intención de adherir a la Convención, y la postura ha sido constante, y, en este sentido, esto es fundamental para el país.

La Convención de Budapest es el único convenio internacional sobre delitos informáticos y obtención de evidencia digital que presenta una cooperación internacional específica en este sentido. Asimismo, es probable que en cinco años, la evidencia digital superará a la evidencia física. La Convención es "dinámica" y ofrece numerosas oportunidades al integrarse en el tratado, como la posibilidad de participar en foros especializados sobre ciertos temas y de debatir continuamente sobre las últimas novedades tecnológicas (Salt, 2018, como se citó en Schulkin, 2018). Con respecto a las obligaciones que surgirán con la adhesión de cada país al convenio, cada miembro contará con un contacto disponible las 24 horas del día, los 7 días de la semana, para facilitar la comunicación entre los países del Convenio.

Ampliación de la Adhesión de Argentina

- Formación y Capacitación: la adhesión al Convenio de Budapest y al Segundo Protocolo Adicional ha posibilitado a Argentina participar en programas internacionales de formación y capacitación, elevando así las competencias de sus profesionales en la lucha contra la ciberdelincuencia.
- Cooperación Técnica: Argentina ha reforzado su infraestructura técnica y operativa en la lucha contra la ciberdelincuencia mediante la colaboración con otros países y organismos internacionales, aprovechando las mejores prácticas y tecnologías de vanguardia.

Consideraciones Finales sobre el Convenio

El Convenio de Budapest se ha establecido como una herramienta clave en la lucha global contra la ciberdelincuencia. Su marco legal uniforme ofrece una base sólida para la implementación de prácticas de ciberpatrullaje, alinear las definiciones de delitos y los procedimientos legales entre los Estados Parte. Esto minimiza las ambigüedades legales y los riesgos de abusos, garantizando que las acciones de vigilancia y monitoreo se realicen conforme a normas internacionales ampliamente aceptadas.

Beneficios Específicos

1. Cooperación Internacional Mejorada: el Convenio facilita la cooperación internacional al permitir un intercambio eficiente de información y la coordinación de operaciones conjuntas. Esto resulta esencial para enfrentar la naturaleza transnacional de numerosos delitos cibernéticos, ya que posibilita respuestas rápidas y efectivas a incidentes que afectan a múltiples jurisdicciones.
2. Obtención Eficiente de Pruebas Electrónicas: las disposiciones del Convenio, fortalecidas por el Segundo Protocolo Adicional, optimizan significativamente la capacidad de las autoridades para obtener pruebas electrónicas de forma eficiente y legal. Estas medidas abarcan la rápida conservación de datos y el intercambio directo de información entre proveedores de servicios y autoridades, simplificando los procesos y aumentando la eficacia en la obtención de pruebas.
3. Protección de los Derechos Humanos: pese a sus ventajas operativas, el Convenio asegura que las medidas de vigilancia sean proporcionales y respeten los derechos humanos. Esto se logra mediante salvaguardas como la supervisión judicial y la evaluación continua de la proporcionalidad de las medidas adoptadas, garantizando que las actividades de ciberpatrullaje se lleven a cabo con transparencia y una supervisión adecuada, previniendo abusos y protegiendo la privacidad de los individuos.

Desafíos y Consideraciones Éticas

El Convenio también aborda los desafíos éticos y legales vinculados al ciberpatrullaje. Proteger los derechos humanos y asegurar la transparencia y rendición de cuentas son esenciales para mantener la confianza pública y garantizar que las prácticas de vigilancia se lleven a cabo de manera ética y legal. Esto implica la implementación de mecanismos de supervisión independientes, la realización de auditorías regulares de las prácticas de ciberpatrullaje y la publicación de informes de transparencia.

Impacto en Argentina

La adhesión de Argentina al Convenio de Budapest y al Segundo Protocolo Adicional ha reforzado considerablemente su marco legal y operativo para combatir delitos cibernéticos. La adopción de estas disposiciones ha permitido a Argentina acceder a recursos y conocimientos internacionales, mejorar la cooperación con otros países y fortalecer su capacidad para enfrentar amenazas cibernéticas de manera más eficaz y eficiente. Además, la formación continua de profesionales en ciberseguridad y la implementación de medidas específicas para proteger los derechos humanos garantizan que las actividades de ciberpatrullaje se realicen con transparencia y respeto por la privacidad de los individuos.

Perspectivas Futuras

El Convenio de Budapest, con sus actualizaciones continuas y la inclusión del Segundo Protocolo Adicional, continúa evolucionando para abordar nuevas amenazas en el entorno digital. Su capacidad para adaptarse rápidamente a innovaciones tecnológicas y a las cambiantes tácticas de los ciberdelincuentes asegura que este tratado se mantenga a la vanguardia en la lucha contra la ciberdelincuencia. Los países que aún no se han unido al Convenio podrían experimentar beneficios significativos mediante su adopción, tanto en el fortalecimiento de sus marcos legales nacionales como en la mejora de su capacidad para cooperar a nivel internacional.

En resumen, el Convenio de Budapest proporciona un marco legal y operativo sólido para el ciberpatrullaje, facilitando la cooperación internacional y la recolección de pruebas

electrónicas, al mismo tiempo que protege los derechos humanos y asegura la transparencia y la rendición de cuentas. Su adopción y aplicación efectiva son cruciales para abordar los desafíos de la ciberdelincuencia en el entorno digital de forma ética y legal.

Capítulo 7 - El Progreso del Ciberpatrullaje y la Integración de la IA

La IA desempeña un papel cada vez más importante en el campo de la ciberseguridad, ofreciendo herramientas y técnicas innovadoras para defenderse contra amenazas cada vez más sofisticadas. Algunas formas en las que la IA contribuye con la ciberseguridad son: (a) la detección de amenazas; (b) el análisis de comportamiento; (c) la predicción de amenazas; (d) la automatización de respuestas; (d) la generación de inteligencia de amenazas; (e) la mejora de la autenticación y la identificación. En definitiva, la IA está transformando, de manera abrupta, la forma en que se afronta y soluciona la ciberseguridad, al fomentar capacidades avanzadas de detección, análisis y respuesta que propician las condiciones necesarias para proteger a las organizaciones contra las crecientes amenazas y delitos informáticos.

El ciberpatrullaje asistido por IA surge como una herramienta estratégica y fundamental en lo que respecta a la detección y la prevención de actividades delictivas en el ciberespacio. La integración de la IA en las estrategias de ciberseguridad posibilita un análisis profundo y exacto del ciberespacio, perfeccionando la capacidad de las autoridades para lograr la identificación de las amenazas potenciales y, de esa forma, responder de manera eficiente a los desafíos emergentes del ciberdelito y del ciberterrorismo (Pons Gamón, 2017) .

En el contexto actual, donde el ciberdelito representa una de las amenazas más significativas relativas a la seguridad global, la INTERPOL (*International Criminal Police Organization*) ha adoptado, de manera progresiva, tecnologías de IA para mejorar sus operaciones de ciberpatrullaje. Este enfoque, no sólo busca corregir y mejorar la eficiencia y la competencia en lo que respecta a la detección y la respuesta a incidentes cibernéticos sino que, también, pretende favorecer y fomentar una cooperación internacional más efectiva. La IA otorga las herramientas necesarias para efectuar un análisis avanzado de grandes volúmenes de datos facilitando, de esa manera, la identificación de patrones delictivos y, al mismo tiempo, la anticipación ante potenciales amenazas que pueden sobrevenir.

La adopción de IA por parte de INTERPOL incluye la creación de centros de fusión cibernética que funcionan como *hubs* de inteligencia, donde se integran y analizan datos de múltiples fuentes. Un *hub* de IA tiene como su principal objetivo el de contribuir a las políticas

públicas y a la utilización de estas tecnologías desde una perspectiva ética y un enfoque social. Estos centros han sido fundamentales en lo concerniente a la emisión y difusión de alertas tempranas y a la coordinación de respuestas internacionales contra una variedad de amenazas cibernéticas, desde *malware* hasta fraudes a gran escala. A través de estas iniciativas, INTERPOL no sólo ha incrementado la capacidad de respuesta individual de los países miembros sino que, también, ha reforzado la infraestructura global de lucha contra el ciberdelito.

No obstante, la integración de tecnologías de IA en la seguridad pública también presenta desafíos particulares, a saber: la necesidad de mantener la privacidad y proteger los derechos civiles mientras se manejan enormes conjuntos de datos. Por otra parte, se requiere una constante actualización tecnológica y una permanente formación especializada del personal para manejar estas herramientas avanzadas de modo eficaz y competente.

Mientras que la IA proporciona herramientas poderosas para el ciberpatrullaje, su implementación efectiva requiere una consideración cuidadosa en relación con los aspectos éticos, legales y operativos. La continua evolución de la IA ofrece y asegura una transformación sólida de las operaciones de INTERPOL, brindando nuevas oportunidades para combatir el ciberdelito de manera proactiva y eficiente.

7.1. Aplicación de la IA en la Ciberseguridad

Es fundamental establecer las conexiones entre la IA y la ciberseguridad, para poder dejar en claro cómo pueden vincularse y combatir los delitos informáticos. La ciberseguridad y la IA están cada vez más interconectadas, puesto que la IA desempeña un papel significativo en el progreso de las medidas de ciberseguridad. De este modo, “esta integración no es nueva, pero ha evolucionado con el tiempo a medida que avanza la tecnología y las amenazas cibernéticas se vuelven más sofisticadas” (Nigro, 2024).

Si se tiene en cuenta la línea cronológica, se puede advertir que hacia finales de la década de 1990 y principios de la de 2000, la IA comenzó a desempeñar un papel importante en los sistemas de detección de intrusiones (IDS, del inglés *Intrusion Detection System*). Esta función se generó a partir de técnicas que se dedicaban al análisis de patrones de tráfico de red y servían

para identificar anomalías que podrían indicar una violación de la seguridad. Asimismo, "en la década de 2000 también se produjo un mayor uso de técnicas de aprendizaje automático en ciberseguridad, aplicando algoritmos para analizar patrones de datos e identificar amenazas potenciales" (Nigro 2024). Este proceso se desarrolló, sobre todo, a través de una de las formas de la IA, el análisis del comportamiento. Esto cobró gran relevancia en la detección de *malware* y otras amenazas cibernéticas, puesto que se podía entender el comportamiento normal e identificar desviaciones de la norma.

A partir del progreso de la IA y de su relación con la ciberseguridad, se generan las condiciones para que se establezca una interacción y una reciprocidad, dado que los ciberdelincuentes utilizan la IA para llevar a cabo una variedad de ataques sofisticados, desde envenenamiento de datos hasta *deepfakes*. De esta manera, las organizaciones de ciberseguridad dependen cada vez más de la IA para poder detectar datos sospechosos e identificar o malograr ataques (Morgan Stanley, 2023).

Es fundamental advertir las relaciones entre la ciberseguridad y la IA, sobre todo para poder analizar posibles ataques, es decir, tratar de identificar y prever cómo operan los delincuentes informáticos. La ciberseguridad presenta algunos desafíos únicos: (a) una vasta superficie de ataque; (b) decenas o cientos de miles de dispositivos por organización; (c) cientos de vectores de ataque; (d) grandes deficiencias en el número de profesionales de seguridad cualificados; (e) masas de datos que han ido más allá de un problema de escala humana (Balbix (2023).

Como se puede anticipar, el uso de la IA no es propiedad excluyente de los profesionales de la ciberseguridad, sino que sus adversarios también utilizan esta herramienta. Los profesionales de la seguridad informática pueden utilizar la IA para aplicar buenas prácticas de ciberseguridad y, de ese modo, disminuir la posibilidad de ataque en lugar de perseguir las actividades maliciosas. No obstante, la IA es empleada por las bandas cibernéticas criminales, los piratas informáticos ideológicos y por los atacantes patrocinados por ciertos Estados, que pueden utilizar las mismas técnicas para vencer las defensas y evitar su detección.

Estas agrupaciones pueden ser desarrolladas para comprender, de manera minuciosa, cómo se conforman y cómo operan. En el caso de las bandas cibernéticas criminales, se puede

indicar que son grupos de individuos que colaboran para llevar a cabo actividades delictivas en el ambiente informático. Estas actividades pueden incluir el robo de información confidencial, el fraude financiero, el robo de identidad, el sabotaje de sistemas informáticos, el espionaje cibernético y la distribución de *malware*, entre otros.

En el caso de los piratas informáticos ideológicos, también conocidos como hacktivistas, son individuos o agrupaciones que realizan actividades de *hacking* con el objetivo de promover una causa política social o ideológica. Habitualmente, utilizan sus capacidades técnicas para realizar acciones como el vandalismo digital, el robo de datos, la interrupción de servicios en línea o la difusión de mensajes políticos. Estos activistas informáticos pueden pertenecer a una diversidad de grupos o movimientos y sus motivaciones pueden abarcar desde la defensa de la libertad de expresión, la lucha contra la censura, la protección del medio ambiente, la denuncia de injusticias sociales o la oposición a ciertas políticas gubernamentales o corporativas.

Por último, los atacantes patrocinados por ciertos Estados son grupos de *hackers* respaldados, financiados o dirigidos por gobiernos o agencias gubernamentales con la finalidad de realizar actividades informáticas maliciosas para el provecho y conveniencia de un Estado en particular, que respalda a la agrupación. Estos grupos pueden tener una vasta variedad de objetivos, que van desde la recolección de información sensible hasta el sabotaje de infraestructuras críticas o la manipulación de sistemas informáticos con fines políticos, económicos o militares.

Es importante resaltar que los Estados que apoyan y financian a estos grupos pueden utilizar a los atacantes informáticos con el objetivo de llevar a cabo operaciones encubiertas, obtener ventajas estratégicas, espiar a otros Estados, desestabilizar gobiernos extranjeros o proteger sus propios intereses. Por su parte, los atacantes suelen tener acceso a recursos significativos, tales como un gran financiamiento, tecnología avanzada y personal altamente especializado. En el ámbito de la ciberseguridad, los ataques producidos por estos grupos encarnan una amenaza grave y compleja, dado que pueden ser altamente constantes y difíciles de atribuir a un actor específico y, por ende, es difícil determinar quién lo ha ejecutado.

A pesar de estas cuestiones complejas que se desarrollan en paralelo al uso de IA por parte de los Estados en materia de seguridad, la IA evoluciona y contribuye para mejorar la

ciberseguridad y, de esa manera, las empresas deberán prepararse contra la posible superioridad de esta nueva y apasionante tecnología. Este progreso deberá tener en consideración ciertos ejes a futuro:

- La IA puede ayudar a derrotar los ciberataques, pero los delincuentes informáticos pueden frustrar los algoritmos de seguridad centrándose en los datos con los que entrenan y las señales de advertencia que buscan.
- Los delincuentes informáticos pueden utilizar la IA para romper las defensas y desarrollar *malware* que varíe su estructura y así eludir la detección.
- Sin volúmenes masivos de datos y eventos, los sistemas de IA generarán resultados inexactos y falsos positivos.
- Si la manipulación de datos no se detecta, las organizaciones tendrán dificultades para recuperar los datos correctos que alimentan sus sistemas de inteligencia artificial, con graves consecuencias. (Balbix, 2023)

7.2. Implementación Eficiente de la IA en Ciberseguridad

Antes de establecer ciertas apreciaciones sobre este tema es fundamental distinguir la ciberseguridad de la IA. La protección de la ciberseguridad con IA nunca reemplazará por completo a los profesionales de la seguridad, ya que siempre habrá una necesidad de resolución creativa de problemas y desafíos más complejos en el lugar de trabajo. La IA puede proteger y beneficiar a los profesionales de la seguridad informática al analizar grandes cantidades de datos, así como también, al reconocer patrones y crear conocimientos basados en grandes volúmenes de datos de seguridad. Los procesos de seguridad tradicionales podrían acarrear grandes cantidades de tiempo, algo vital si se tiene en cuenta la velocidad con la que realizan sus ataques los delincuentes informáticos. Con anterioridad a la aparición de la IA, los profesionales de la seguridad empleaban sistemas e instrumentos de detección basados en firmas, con el objetivo de identificar posibles amenazas cibernéticas (Nyíri, 2023).

Estos instrumentos de seguridad equiparaban el tráfico de red entrante con una base de datos de amenazas o firmas de códigos maliciosos. De esta manera, tras la detección, el sistema

activa una alerta y sugiere al profesional de seguridad que debe tomar una acción para bloquear o poner en cuarentena la amenaza. Este enfoque de seguridad basado en firmas fue eficaz frente a amenazas conocidas, pero el enfoque de detección basado en firmas ha demostrado ser inadecuado contra amenazas nuevas. De manera frecuente, "estos instrumentos resultaron en una mayor frecuencia de falsos positivos, lo que envió a los profesionales de seguridad a una *búsqueda inútil*" (Nyíri, 2023).

Ahora bien, la IA es extremadamente importante en materia de ciberseguridad por un motivo notorio: los grupos de delincuentes cibernéticos han empezado a utilizar tecnologías de aprendizaje automático, automatización e IA para perpetrar ataques cibernéticos masivos contra empresas. El número de riesgos y la posibilidad de que el *ransomware* cause estragos en las redes sigue en aumento. La IA y el aprendizaje automático están permitiendo a los analistas de seguridad igualar las condiciones, al manejar grandes volúmenes de información, ofrecer análisis rápido y deshacerse del exceso de alertas y falsos positivos. Esto ha incrementado significativamente la eficacia y el rendimiento de sus equipos, otorgándoles una ventaja frente a potenciales delincuentes cibernéticos.

Un interrogante significativo que debe plantearse sobre esta cuestión es cómo se aplica la IA a la ciberseguridad. La IA puede monitorear, analizar, detectar y responder a las ciber amenazas en tiempo real. ¿Cómo se lleva a cabo esto? Se ejecuta tan pronto como "los algoritmos de IA analizan cantidades masivas de datos para detectar patrones que son indicativos de una amenaza cibernética, también pueden escanear toda la red en busca de debilidades para prevenir tipos comunes de ataques cibernéticos" (Nyíri, 2023). Generalmente, la IA monitorea y analiza patrones de comportamiento y, al utilizar estos patrones para crear una línea de base, detecta comportamientos inusuales y restringe el acceso no autorizado a los sistemas. Asimismo, la IA ayuda a distinguir los riesgos y, de esa manera, puede identificar, de modo instantáneo, la posibilidad de aparición de un *malware* o de ciertas intrusiones previamente a su aparición. Cuando la IA es implementada, sirve como motor para automatizar la seguridad. Esta situación libera recursos y tiempo de los empleados al posibilitar la automatización de tareas repetitivas.

Por los motivos mencionados hasta aquí, es esencial preguntarse acerca de los beneficios de la IA en la ciberseguridad. En este sentido, actualmente la IA está preparada para identificar potenciales riesgos cibernéticos, descubrir nuevas formas de ataque y proteger la información confidencial de cualquier empresa. Las tres principales ventajas que estriba emplear herramientas de ciberseguridad impulsadas por IA abarcan:

- Analizar rápidamente grandes cantidades de datos;
- Detectar anomalías y vulnerabilidades;
- Automatizar procesos repetitivos. (Nyíri, 2023)

El potencial de utilizar IA en la ciberseguridad es casi ilimitado, puesto que la velocidad y precisión de la detección y respuesta a amenazas es lo más cercana posible al tiempo real. La IA puede contribuir a reducir el impacto de un ataque de *ransomware* al alertar a su equipo de seguridad sobre comportamientos inusuales tan pronto como sea posible. Además, la IA mejora la eficiencia de las operaciones de ciberseguridad mediante la automatización, lo que permite liberar tiempo y recursos efectivos de su equipo de seguridad para dedicarlos a otras tareas prioritarias.

Por otro lado, cabe preguntarse si hay riesgos a la hora de utilizar IA en la ciberseguridad. En este aspecto, es imprescindible resaltar que la IA como tecnología se encuentra en sus inicios. La IA aún requiere la necesidad de la intervención humana para su funcionamiento, no sólo para entrenar sus motores, sino también para intervenir si un motor comete un error. Los sistemas de seguridad impulsados por IA utilizan algoritmos de aprendizaje automático que se nutren de datos históricos. Esta dinámica puede ocasionar falsos positivos al encontrarse con amenazas nuevas, desconocidas, que no se ajustan a los patrones previamente establecidos. Además, existe una creciente preocupación sobre cómo los *hackers* pueden utilizar la IA de manera maliciosa, como la generación de correos electrónicos de *phishing* convincentes o incluso la creación de *malware* (Nyíri, 2023).

7.3. Posibles Contribuciones de la IA en la Ciberseguridad

El avance de las TIC ha generado un cambio fundamental en la forma en que abordamos la seguridad cibernética. Este cambio requiere la implementación de métodos especializados para contrarrestar y gestionar las amenazas en línea. El ciberpatrullaje no sólo se centra en la prevención de ataques, sino que también implica una respuesta activa para garantizar la protección de la seguridad digital. Cada Estado desarrolla su propio enfoque de ciberseguridad, que, a su vez, se encuentra influenciado por la propia percepción en lo que respecta a la defensa y a la seguridad nacional.

Los centros de investigación en seguridad informática Trend Micro Research, UNICRI y Europol han elaborado un informe en el que se señalaba que la IA le asegura a los individuos una sólida automatización y autonomía. Para estos organismos, las personas están preocupadas por el uso indebido de la IA y, por ese motivo, es imperioso garantizar la transparencia con respecto a las amenazas pero, al mismo tiempo, examinar los posibles beneficios de la tecnología de la IA. En este sentido, si bien la IA le está generando altos niveles de recaudación a las empresas que se dedican a IA y las que utilizan esta tecnología, también están creciendo los niveles de uso indebido y de abuso (Trend Micro Research, UNICRI y Europol, 2020) .

Dentro de los potenciales peligros detrás de la popularidad de este tipo de tecnología están los *deepfakes*, es decir, los "contenidos audiovisuales en los que se cambia el sonido y/o la imagen original de una grabación" (Gaimari, 2021, p. 55). La IA se ha desarrollado enormemente en los últimos tiempos con logras destacables pero, también, se ha empleado con el objetivo de desinformar para acarrear problemas tanto políticos como empresariales.

El informe de Trend Micro Research, UNICRI y Europol contribuye en lo que respecta a mejorar esta tecnología y a aclarar ciertas cuestiones oscuras, puesto que sugiere que los ciberdelincuentes emplean (y emplearán) la IA como método y como objetivo de sus ataques. A pesar de que las *deepfakes* son actualmente la implementación más reconocida de la IA como método de ataque, simultáneamente se advierte que en un futuro cercano se requerirán nuevas herramientas de detección para reducir el riesgo de campañas de desinformación, extorsión, fraudes y amenazas dirigidas a conjuntos de datos de IA.

Con el propósito de solucionar estos inconvenientes, se detalla, a continuación, una serie de requerimientos que plantean diferentes modalidades de uso de la IA, a saber:

- Convencer a los ataques de ingeniería social a gran escala;
- *Malware* de rastreo de documentos para hacer que los ataques sean más eficientes;
- Evasión del reconocimiento de imágenes y biometría de voz;
- Ataques de *ransomware*, mediante la evasión y la focalización inteligente;
- Contaminación de datos, mediante la identificación de puntos ciegos en las reglas de detección. (Gaimari, 2021, p. 56)

Asimismo, existe una serie de recomendaciones, basadas en el informe que se mencionó, con el objetivo de buscar soluciones en el futuro para esta problemática:

- Aprovechar el potencial de la tecnología de IA como herramienta de lucha contra el crimen para preparar la industria y la policía de la ciberseguridad en el futuro;
- Continuar la investigación para estimular el desarrollo de tecnología defensiva;
- Promover y desarrollar marcos de diseño de IA seguros;
- Reducir la retórica políticamente cargada sobre el uso de IA con fines de ciberseguridad;
- Aprovechar las asociaciones público-privadas y establecer grupos de expertos multidisciplinar. (Gaimari, 2021, p. 56)

Ahora bien, es fundamental comprender que "el derecho nunca va por delante de la tecnología, por lo cual es necesario que el mismo, se adapte a las nuevas realidades que las TIC plantean" (Pastorini, 2019, p. 3). Por este motivo, es necesario focalizar sobre la IA y profundizar sobre sus caracteres positivos y negativos, dado que los sistemas basados en IA, al cambiar el concepto de la investigación de los delitos, pueden hallar conexiones que los seres humanos habitualmente ignoran. De esta manera, la inteligencia criminal podría llegar a anticiparse a la delincuencia y prevenir ataques, apoyando la investigación de casos individuales y logrando, de este modo, resultados positivos en las investigaciones criminales.

Por las razones presentadas hasta aquí, se puede indicar que la IA es una herramienta efectiva para afrontar y combatir el cibercrimen. No obstante, su efectividad requiere que esté respaldada por el cumplimiento de las leyes y los derechos fundamentales de cada Nación.

7.4. Importancia de la Declaración de Bletchley

La Declaración de Bletchley, presentada en la Cumbre de Seguridad en IA celebrada en Bletchley Park, Reino Unido, los días 1 y 2 de noviembre de 2023, es un acuerdo internacional fundamental diseñado para sentar las bases del desarrollo y la implementación segura de tecnologías avanzadas de IA. Esta declaración, respaldada por 28 países, incluyendo Estados Unidos, China, Reino Unido, Alemania, Francia, Japón, India, Canadá y la Unión Europea, demuestra un consenso global sobre la urgencia de abordar los riesgos y desafíos asociados con la IA de vanguardia. La declaración establece una comprensión compartida de las oportunidades y los riesgos que plantea la IA, así como también la necesidad de que los gobiernos trabajen juntos para enfrentar los desafíos más importantes (Gov.UK, 2023a).

Entre los aspectos más relevantes de la declaración se destacan:

1. Reconocimiento de los Riesgos Existenciales y Sistémicos de la IA: los países firmantes admiten que los modelos de IA avanzada, especialmente aquellos con capacidades autónomas y generales, podrían representar amenazas significativas para la seguridad global. En consecuencia, subrayan la necesidad de una cooperación internacional robusta para su adecuada gestión.
2. Compromiso con el Desarrollo Ético y Responsable: los signatarios se comprometen a fomentar la investigación y el desarrollo de IA que respete los derechos humanos, los principios democráticos y el estado de derecho. Esto implica priorizar aspectos clave como la seguridad, la equidad y la transparencia en el avance tecnológico.
3. Fomento de la Gobernanza Internacional y la Transparencia: se enfatiza la necesidad de establecer estándares globales y promover la colaboración entre el sector público y el privado para reducir los riesgos emergentes de la IA, al tiempo que se optimizan sus beneficios sociales. Esto abarca la creación e implementación de marcos regulatorios y de supervisión conjuntos.

4. Cooperación Transnacional: la declaración exhorta a los gobiernos, organizaciones internacionales y actores del sector privado a trabajar conjuntamente para identificar, gestionar y mitigar los riesgos asociados con las tecnologías de IA de alto impacto, con el fin de fomentar una gobernanza global eficaz. (Laje, 2023)

Como se puede advertir, la Declaración de Bletchley establece un marco preliminar para la gobernanza global de la IA, subrayando la importancia de coordinar los esfuerzos en la supervisión de tecnologías avanzadas de inteligencia artificial. Además, este acuerdo multilateral resalta la necesidad de fortalecer las capacidades internacionales para evaluar, gestionar y mitigar los riesgos asociados con sistemas de IA complejos.

Es fundamental mencionar, que todos los actores en el mundo, poseen un papel esencial que desempeñar para garantizar la seguridad de la IA, concretamente, las naciones, los foros internacionales, las empresas, la sociedad civil y el mundo académico deberán trabajar juntos. Cada actor debe tomar nota de la importancia de la IA inclusiva y de la reducción de la brecha digital, reafirmando que la colaboración internacional debe procurar la implicancia en una amplia gama de socios según corresponda (Gov.UK, 2023b). Asimismo, cada Estado debería ampararse de manera firme a los enfoques y políticas orientados al desarrollo que podrían ayudar a los países en desarrollo para, de ese modo, fortalecer la creación de capacidad en materia de IA y aprovechar el papel facilitador de la IA con la finalidad de apoyar el crecimiento sostenible y abordar la brecha de desarrollo.

7.4.1. Puntos Positivos y Negativos de la Declaración

Iain Standen, el CEO de Bletchley Park Trust, el sitio donde se organiza la convención, fue categórico al señalar que se sienten contentos por la posibilidad de que su organización albergue a la primera Cumbre de seguridad de IA del mundo. Asimismo, aseguró que “como sitio que ha sido testigo del poder de la inteligencia humana, la tecnología emergente y la colaboración, reconocemos la importancia de garantizar que la tecnología de IA se desarrolle e implemente de manera segura y ética” (Standen, 2023, como se citó en Wisner Glusko, 2023).

De esta manera, se puede advertir que se está produciendo un enfoque internacional más coherente en la regulación de la inteligencia artificial, el cual combina características del enfoque europeo con elementos de políticas más liberales dirigidas al emprendimiento, la innovación tecnológica y la economía. Este enfoque pretende establecer un equilibrio que contemple y armonice las diversas perspectivas y bloques regionales involucrados. En este sentido, es positivo que las naciones estén progresando en lo que respecta a reflexionar sobre ciertos temas tecnológicos fundamentales. ¿Por qué esto es primordial? Sin duda, los modelos de gobernanza de la IA son fundamentales para determinar si los sistemas adoptarán enfoques que garantizan en mayor o menor medida la protección de los derechos humanos. La competencia entre los tres grandes bloques (China, Estados Unidos y la UE) "no deja de ser una competencia de valores donde la centralidad del ser humano es la clave que marca la diferencia (Wisner-Glusko, 2022, pp. 543-544).

Se debe mencionar, que hay voces críticas que han señalado falencias y deficiencias con respecto a la declaración. Por ejemplo, ciertos especialistas, provenientes del propio ámbito tecnológico, han indicado el riesgo de una captura regulatoria. Estos críticos argumentan que se está exagerando el peligro que representan los sistemas de IA en la actualidad con el fin de imponer una regulación que, en la práctica, establezca barreras desproporcionadas y solo accesibles para las grandes empresas tecnológicas. Esta regulación podría, en consecuencia, dificultar la entrada de nuevos actores en el mercado. Además, dicho sector puede llegar a "prohibir el desarrollo de sistemas que no sean seguros o cuya seguridad no pueda garantizarse" (Velasco Rico, 2024)). Asimismo, el mencionado sector propugna que la creación de sistemas de IA se alinee con el conocimiento social de la tecnología y con los objetivos de desarrollo sostenible.

Por otra parte, la finalidad de la declaración puede ser resumida en dos puntos centrales: (a) de crear un panel que examine de manera regular los avances y, especialmente, los desafíos en el ámbito de la IA, con el objetivo de lograr un desarrollo de sistemas de inteligencia artificial que sea tanto humanista como seguro; (b) exigir que todos los actores involucrados en el campo de la IA mantengan altos estándares de transparencia, confiabilidad y rendición de cuentas, para evaluar y supervisar tanto las capacidades potencialmente peligrosas como los efectos

derivados de su implementación. No obstante, a pesar de esto, "el documento no tuvo la capacidad de definir puntos concretos ni claros, se utilizará de base para la celebración de distintas cumbres globales sobre la seguridad de la IA que se realizarán cada seis meses" (Flores, 2023).

En definitiva, es sustancial resaltar que la Declaración de Bletchley no es vinculante, por ende, no obliga a ningún tipo de acción por parte de las naciones. De todos modos, pueden resaltarse algunos puntos positivos, a saber: la reunión marcó el comienzo de una colaboración internacional más comprometida, en la que los participantes abordaron con mayor seriedad el tema de la IA y los posibles efectos perjudiciales asociados a su desarrollo.

7.5. Ciberpatrullaje con IA en la Dark Web

7.5.1. IA y Dark Web

El ciberpatrullaje se ha consolidado como una herramienta esencial en la lucha contra el cibercrimen, especialmente dentro de la dark web, un entorno digital conocido por su alto nivel de anonimato y sofisticadas técnicas de encriptado. La incorporación de la IA ha transformado estas operaciones, incrementando la eficacia de las fuerzas de seguridad en la identificación y desactivación de actividades delictivas en este entorno complejo. No obstante, aunque la IA ofrece ventajas técnicas considerables, su uso en la dark web plantea importantes desafíos legales que demandan una atención cuidadosa y específica.

7.5.2. Características de la Dark Web

La dark web es una parte especializada de la deep web, accesible únicamente mediante navegadores como Tor, que ofrecen anonimato utilizando técnicas avanzadas de encriptación y enrutamiento del tráfico. Si bien este entorno asegura la privacidad de usuarios legítimos, también es aprovechado por delincuentes para llevar a cabo actividades ilícitas, como la venta de drogas, el tráfico de armas y el comercio de datos robados (Europol, 2024). La complejidad técnica inherente a la dark web representa un desafío considerable para las fuerzas de seguridad,

ya que las actividades en este espacio son extremadamente difíciles de rastrear y documentar (Kaspersky, 2024).

7.5.3. Ventajas Técnicas del Ciberpatrullaje con IA en la Dark Web

Procesamiento y Análisis Avanzado de Big Data: la capacidad de la IA para procesar grandes cantidades de datos no estructurados es crucial en la dark web, donde la información suele estar dispersa y presentarse en formatos complejos (Ganesh, 2023). Herramientas como DarkBERT, un modelo de lenguaje diseñado específicamente para combatir el cibercrimen, emplean técnicas de procesamiento de lenguaje natural (NLP) y aprendizaje profundo para analizar textos y detectar patrones anómalos con alta precisión. Esto no solo mejora la capacidad de respuesta en tiempo real, sino que también permite una correlación de datos de diversas fuentes para identificar redes criminales ocultas (Kaspersky, 2024).

Para comprender en profundidad esta cuestión es importante desarrollar una serie de puntos sobre las ventajas técnicas que se generan al implementar IA a partir de la dark web:

Automatización y Eficiencia Operacional: la integración de la IA para automatizar tareas rutinarias, como la vigilancia constante de foros y mercados clandestinos, mejora significativamente la eficiencia operativa. Los algoritmos avanzados de detección de anomalías, alimentados con extensos conjuntos de datos históricos, tienen la capacidad de identificar comportamientos sospechosos con mayor precisión y rapidez que los métodos convencionales. Esta capacidad permite a las fuerzas de seguridad concentrar sus recursos en alertas prioritarias y en investigaciones de mayor impacto, al mismo tiempo que minimiza la necesidad de intervención humana en actividades repetitivas (Carter, 2022).

Adaptabilidad y Mejora Continua: los sistemas de IA tienen la habilidad de aprender y adaptarse de forma continua, una característica esencial en la dark web, donde las tácticas de los ciberdelincuentes cambian rápidamente. Los algoritmos de aprendizaje automático pueden actualizarse periódicamente con datos nuevos, lo que les permite refinar sus modelos predictivos y mantenerse al tanto de las amenazas emergentes. Esta capacidad de adaptación es crucial para garantizar la eficacia en la detección y neutralización de actividades ilícitas en un entorno tan dinámico (Interpol, 2024).

Reducción de Falsos Positivos: la elevada precisión de la IA en el análisis contextual contribuye a disminuir los falsos positivos, un desafío frecuente en la detección de amenazas en la dark web. Los sistemas de IA, al emplear redes neuronales profundas y técnicas avanzadas de minería de datos, son capaces de distinguir con mayor precisión entre actividades legítimas y delictivas. Esto permite a los analistas enfocar sus esfuerzos en amenazas reales, optimizando así la eficiencia operativa y reduciendo el desgaste de recursos en investigaciones sin fundamento (Flare, 2023).

7.5.4. Desafíos Legales del Ciberpatrullaje con IA en la Dark Web

Cumplimiento de Normativas Internacionales: la implementación de IA en el ciberpatrullaje debe adherirse rigurosamente a las normativas internacionales que regulan la vigilancia digital. La transparencia y la auditabilidad, que incluyen el registro exhaustivo de todas las conexiones entrantes y salientes, son esenciales para asegurar que las operaciones se realicen dentro de un marco legal bien definido y respeten los derechos humanos y la privacidad (Bhattacharya, 2021). Las agencias de seguridad deben garantizar que las tecnologías utilizadas cumplan con regulaciones como el Reglamento General de Protección de Datos (GDPR) en Europa, el cual establece estrictos estándares para la protección de datos personales (National Institute of Justice, 2020).

Es sustancial tener en cuenta los parámetros legales para la implementación de esta tecnología, a saber:

- Admisibilidad y Validez de la Evidencia Digital: la evidencia obtenida mediante IA debe ser gestionada cuidadosamente para preservar su integridad y asegurar su admisibilidad en procedimientos judiciales. Esto implica mantener una cadena de custodia continua y aplicar técnicas de preservación de datos que cumplan con los estándares forenses internacionales. La validez de la evidencia digital es fundamental, ya que cualquier discrepancia en su recolección o manejo podría resultar en la exclusión de pruebas esenciales en procesos judiciales penales (Interpol, 2024).
- Transparencia, Supervisión Ética y Privacidad: el uso de IA en el ciberpatrullaje plantea importantes dilemas éticos, particularmente en lo que respecta a la privacidad y la

libertad de expresión. Es esencial que las actividades de vigilancia realizadas con IA sean supervisadas de manera ética para prevenir abusos de poder. Los algoritmos deben ser diseñados y revisados para minimizar sesgos y asegurar que las decisiones tomadas por la IA se adhieran a los principios legales y éticos. La falta de transparencia en estas prácticas puede socavar la confianza pública y generar riesgos significativos para los derechos civiles (National Institute of Justice, 2020).

- Sostenibilidad Financiera y Recursos: el desarrollo, implementación y mantenimiento de sistemas avanzados de IA, como DarkBERT, exigen inversiones significativas en infraestructura tecnológica, personal especializado y recursos financieros. Además, la constante necesidad de actualizar estos sistemas para abordar nuevas amenazas representa un costo continuo que las organizaciones de seguridad deben asumir. Por ello, una planificación financiera estratégica es esencial para garantizar la viabilidad y efectividad de estos programas a largo plazo (Flare, 2023).

7.5.5. Consideraciones Finales

El ciberpatrullaje con IA en la dark web ofrece importantes ventajas técnicas, como el procesamiento avanzado de datos y la automatización de operaciones, que son esenciales para combatir el cibercrimen en este entorno complejo. Sin embargo, estas capacidades deben ser equilibradas con los desafíos legales y éticos que plantea su implementación. El cumplimiento normativo, la transparencia, la supervisión ética, y la sostenibilidad financiera son pilares fundamentales para garantizar que estas tecnologías sean utilizadas de manera efectiva y responsable en la lucha contra el cibercrimen.

En definitiva, El cumplimiento normativo es crucial para garantizar que el uso de la IA se ajuste a las leyes y regulaciones vigentes, protegiendo los derechos y la privacidad de los individuos. La transparencia en el funcionamiento de los sistemas de IA permite que las acciones y decisiones tomadas por estos sistemas sean auditables y comprensibles, lo cual es fundamental para mantener la confianza pública. Además, la supervisión ética asegura que la tecnología se utilice de manera responsable, evitando abusos de poder y garantizando que las prácticas de vigilancia respeten los principios fundamentales de justicia y equidad.

Por otro lado, la sostenibilidad financiera también juega un papel clave, ya que el desarrollo, mantenimiento y actualización de sistemas avanzados de IA requieren una inversión continua en infraestructura, personal especializado y recursos. Es esencial que las organizaciones encargadas de la seguridad planifiquen estratégicamente sus recursos para asegurar que estos programas no solo sean efectivos en el corto plazo, sino también sostenibles a lo largo del tiempo. De este modo, mientras que la IA proporciona herramientas poderosas para el ciberpatrullaje, es fundamental que su implementación esté equilibrada con una sólida base de principios legales, éticos y financieros para asegurar que estas tecnologías sean utilizadas de manera efectiva, responsable y equitativa en la lucha contra el cibercrimen.

Capítulo 8 - Cifrado y Seguridad como un Nuevo Desafío del Ciberpatrullaje

Los hechos de delincuencia informática implicaron la necesidad de utilizar herramientas de cifrado o encriptación de las comunicaciones en el marco de las tecnologías informáticas, que permiten agregar una capa de inviolabilidad técnica no normativa a los actos comunicativos intermediados por tecnologías. El cifrado de las comunicaciones implica "la utilización de un algoritmo matemático que envuelve un mensaje de manera que solo el receptor legítimo pueda abrirlo y hacerse de su contenido, mediante la utilización de una llave o clave única que desenvuelve el mensaje" (Álvarez Valenzuela, 2019, p. 243). En definitiva, el objetivo del cifrado es volver ininteligible un mensaje ante un tercero ajeno a esa comunicación.

Es importante atender la cuestión de la trascendencia de advertir la importancia del cifrado de los activos digitales, dado que es uno de los métodos más eficaces con respecto a la protección de los activos. Es importante aclarar que, un activo digital (recurso digital), es cualquier recurso que existe de modo digitalizado y que alguien puede poseer y utilizar, así también, representa contenido que alguien puede detentar y, de esta manera, tienen asociado un derecho para su uso. Por lo tanto, como son abordados como una propiedad, esta puede ser vendida, comprada o licenciada. Concretamente, el cifrado convierte los datos en códigos que no pueden ser descifrados, puesto que solamente pueden ser leídos por los que disponen de las llaves de descifrado adecuadas. De esta manera, "las soluciones de cifrado actuales son robustas y utilizadas en varias formas de contenido digital, desde correos electrónicos hasta monedas digitales" (Chapellin, 2023).

En este contexto, persuadir y desalentar las filtraciones de información en activos digitales es fundamental en lo que respecta a la seguridad de los sistemas de administración. De este modo, hay acciones significativas que se deben implementar, como por ejemplo el monitoreo ininterrumpido de los flujos de datos, como así también la localización e identificación de potenciales filtración de información confidencial. En este sentido, el ciberpatrullaje es una práctica imprescindible y necesaria en estos aspectos, dado que involucra

actos tales como el monitoreo activo de las actividades en línea con la finalidad de determinar posibles actividades sospechosas o intentos concretos de robo de datos.

Es primordial que los profesionales de la tecnología de la información implementen procedimiento de autenticación sólidos, como contraseñas seguras, autenticación de dos factores (MFA) y sistemas de gestión de identidad y acceso (IAM), para garantizar que solo las personas autorizadas puedan acceder a los activos digitales. La autenticación de múltiples factores (AMF), habitualmente denominada como MFA (*multi factor authentication*), es un método de control de acceso informático en el cual a un determinado usuario se le otorga acceso al sistema después de que proporcione dos o más pruebas diferentes de que es quien dice ser. Estas pruebas pueden ser diversas, por ejemplo: (a) una contraseña; (b) poseer una clave secundaria rotativa; (c) detentar un certificado digital instalado en el equipo; (d) a partir de una biometría, entre otros testimonios de identidad (Chapellin, 2023).

Por su parte, con respecto a la gestión de identidades y accesos (IAM, del inglés *identity and access managemen*), se debe mencionar que es la especialidad de seguridad que posibilita que las entidades correctas (ya sean personas o cosas), utilicen los recursos apropiados, es decir, aplicaciones o datos, cuando sea necesario, sin la aparición de interferencias, y empleando los dispositivos que desean usar.

Como se pudo advertir, en informática, sobre todo en el ámbito de la criptografía (práctica que consiste en proteger información mediante el uso de algoritmos codificados, *hashes* y firmas), el cifrado implica la transformación de la información, conocida como texto plano, en una forma alternativa llamada texto cifrado. Esta técnica asegura que sólo los usuarios autorizados puedan convertir el texto cifrado nuevamente a su forma original y acceder, de ese modo, a la información. A pesar de que el cifrado no elimina la posibilidad de interferencias, sí puede evitar que un tercero pueda comprender el contenido de manera inteligible.

En el ámbito de la seguridad informática, existen diferentes clases de cifrado que se utilizan para proteger la información. Algunos de los más comunes son los siguientes:

- Cifrado simétrico: utiliza una sola clave para cifrar y descifrar datos; algunos algoritmos de cifrado simétrico populares son AES (*advanced encryption standard*) y DES (*data encryption standard*).

- Cifrado asimétrico: utiliza un par de claves, una pública y una privada, para cifrar y descifrar datos; algunos ejemplos incluyen RSA (por sus creadores: Rivest, Shamir y Adleman) y ECC (*elliptic curve cryptography*).
- Cifrado de flujo: cifra datos a medida que se transmiten, generalmente uno a uno, utilizando una clave de cifrado. Un ejemplo común es el cifrado RC4 (*Rivest Cipher 4*).
- Cifrado de bloque: divide los datos en bloques fijos antes de cifrarlos, lo que hace que el cifrado sea más seguro. AES es un ejemplo destacado de cifrado de bloque.
- Cifrado homomórfico: permite realizar operaciones matemáticas en datos cifrados sin necesidad de descifrarlos primero. Esto es útil en aplicaciones donde la privacidad es fundamental, como en el procesamiento de datos en la nube.
- Cifrado de extremo a extremo: garantiza que la comunicación cifrada solo pueda ser entendida por las partes que la están intercambiando, sin que nadie más pueda acceder a ella, ni siquiera el proveedor del servicio de comunicación. Se utiliza, habitualmente, en aplicaciones de mensajería segura como *Signal* o *WhatsApp*.

Estos son sólo algunos ejemplos de los tipos de cifrado utilizados en seguridad informática. Cada tipo tiene sus propias características y aplicaciones específicas, y la elección del cifrado adecuado depende de los requisitos de seguridad y las restricciones del sistema en particular. En este trabajo se resaltará la importancia del último tipo de cifrado expuesto.

El cifrado de extremo a extremo (E2EE, del inglés *end-to-end encryption*) asegura que sólo los participantes en la comunicación puedan acceder a los mensajes, impidiendo que terceros, como proveedores de servicios de internet o de comunicación, puedan interceptar o descifrar los datos. Este sistema garantiza que sólo el emisor y el receptor puedan leer los mensajes, protegiendo la privacidad y la confidencialidad de la conversación. Por ejemplo, con respecto a las empresas que emplean este tipo de cifrado, se genera la imposibilidad de proporcionar a las autoridades acceso a los mensajes de texto de los usuarios. Ahora bien, en los últimos años se han abiertos ciertos debates en torno a este tipo de cifrado, así como también, disputas en torno a sus implicancias en las prácticas de ciberpatrullaje. Esta situación, supone una tensión inherente entre la seguridad pública y la privacidad individual. La Agencia de la

Unión Europea para la Cooperación Policial (Europol), es la entidad responsable de diseñar, coordinar y llevar a cabo acciones contra grupos delictivos y dirigir la lucha contra el terrorismo en la Unión Europea, trabajando en conjunto con las autoridades de los países miembros. Esta agencia, ha planteado preocupaciones significativas respecto al E2EE, sugiriendo que este tipo de cifrado dificulta severamente la capacidad de las fuerzas del orden para acceder a las comunicaciones críticas durante las investigaciones de crímenes graves, como es el caso del abuso infantil, el fraude financiero y el tráfico de drogas.

Europol, trata decididamente el tema de los delitos informáticos. Entre sus actividades se encuentra el Sistema de Informática de Europol (TECS), que establece la implementación de un sistema computarizado que facilite la entrada, acceso y análisis de datos. Este sistema consta de tres elementos principales: un sistema de análisis y un sistema de índices (ambos en funcionamiento en la actualidad), y un sistema de información, del cual una versión preliminar está en funcionamiento desde enero de 2002. Una autoridad de control común, integrada por expertos en protección de datos de cada estado, supervisa el contenido y el uso de todos los datos personales disponibles para esta agencia (Europol, 2024).

Es imperativo que los gigantes tecnológicos y los gobiernos contemplen y planteen serios ajustes en la implementación del E2EE, para permitir un acceso legal y regulado en situaciones específicamente justificadas. El argumento principal es que un acceso controlado es esencial para permitir a las autoridades combatir eficazmente el crimen sin comprometer la seguridad general del público (Mak, 2024).

Por el contrario, esta posición ha generado una fuerte oposición por parte de activistas de derechos civiles y defensores de la privacidad, quienes argumentan que los esfuerzos para limitar el E2EE podrían derivar en una vigilancia masiva, un hecho que podría debilitar y perjudicar, de manera significativa, la privacidad individual. Estos críticos sostienen que es crucial que se encuentre un equilibrio que no tienda a socavar los derechos fundamentales al intentar proteger la seguridad pública (Mak, 2024).

El dilema del E2EE en el contexto del ciberpatrullaje acentúa la necesidad de un enfoque imparcial y equilibrado que respete la seguridad y los derechos a la privacidad. Asimismo, expertos en políticas públicas y en ciberseguridad sugieren que la solución podría residir en el

desarrollo de tecnologías de cifrado innovadoras, que posibiliten que las autoridades realicen su labor sin comprometer la integridad de las comunicaciones privadas de los usuarios (Mak, 2024).

En lo que respecta a las investigaciones específicas, se debe indicar que en el caso de indagaciones acerca de los datos en un dispositivo móvil, el cifrado debe llevarse a cabo a través de un proceso instalado en el dispositivo móvil. En este sentido, el mensaje cifrado obtenido mediante el algoritmo RSA y la clave privada del servidor, viajan por el hilo de comunicación hasta el servidor local (Solís et al., 2017, p. 161). De ese modo, una vez que llega al servidor, es descifrado a partir de una llave privada, y es cifrado una vez más con la llave pública del usuario de destino. Posteriormente, cuando llega al usuario receptor, el descifrado se lleva a cabo a partir del método RSA inversa. A partir de este método, durante el proceso de cifrado y descifrado es necesario acceder a los datos reservados para el método, y a continuación mostrar el mensaje descifrado. Se debe aclarar, que el RSA es un método de encriptación desigual, aplicado en numerosos sectores de la transferencia de información en la web debido a su carácter práctico. Está compuesto por dos claves: una pública, empleada en el proceso de encriptación, y otra privada, utilizada para la decodificación de datos (Solís et al., 2017, p. 161).

8.1. Regulación del Cifrado

Teniendo en consideración, se debe señala que la regulación del cifrado en materia informática es un tema de creciente importancia en la era digital. El cifrado, como se pudo advertir, es una técnica fundamental para proteger la privacidad y la seguridad de la información, y por estos motivos, se encuentra en el centro de debates legales y políticos a nivel mundial.

En relación con este asunto, un paso importante pero complejo surgió a partir del surgimiento de las tecnologías de cifrado civiles, es decir, los sistemas y métodos de cifrado utilizados por personas, empresas u organizaciones no pertenecientes al ámbito militar o gubernamental. Estas prácticas provocaron las denominadas criptoguerras que enfrentaron a las autoridades políticas y del sistema de inteligencia de EE. UU. con la comunidad científica y tecnológica vinculadas al desarrollo de sistemas de cifrado (Álvarez Valenzuela, 2019, p. 244).

Se debe aclarar, que en países como en los EE. UU., no existe una norma que prohíba en el marco del derecho el desarrollo o uso de herramientas de encriptación, la exportación de estas, así como también de aplicaciones que utilicen alguna forma o tipo de tecnología de cifrado, está sujeta a las normas federales de la *Export Administration Regulations* (EAR), es decir, las regulaciones de administración de las exportaciones, administradas por la Oficina de Industria y Seguridad.

De esta manera, se debe resaltar que ciertas normas, como las ya mencionadas en este trabajo (como es el caso de la *USA Patriot Act*), no establecen reglas específicas sobre el cifrado, lo que ha permitido en la práctica que, si una agencia de investigación en el ejercicio de sus atribuciones se enfrenta a este tipo de tecnologías al momento de llevar a cabo una interceptación, se encontraría facultada para descifrarlas, usando los medios técnicos y humanos de que disponga (Álvarez Valenzuela, 2019, p. 245).

La norma constitucional fija las reglas necesarias para que una corte determine, en el caso concreto, qué bien será objeto de protección especial en el caso de la tensión entre privacidad y seguridad nacional, identificando, al menos, cuatro criterios distintos que permitirían descartar que el cifrado esté protegido por dicha garantía constitucional: (a) autorizaciones judiciales expedidas conforme a la ley; (b) daños inherentes que ocasionaría el cifrado; (c) el interés público en casos especialmente graves; y (d) obstrucción a la justicia (Etzioni, 2015, como se citó en Álvarez Valenzuela, 2019, p. 246). En definitiva, es clave que se establezca una norma constitucional que acuerde las pautas esenciales para que, en una situación específica, un tribunal decida le bien que merece un resguardo particular cuando acontezca un conflicto determinado entre y la seguridad del Estado y la privacidad de cualquier ciudadano.

Capítulo 9 - Evaluación de la Resolución 428/2024 sobre Ciberpatrullaje

La Resolución 428/2024, promulgada por el Ministerio de Seguridad de Argentina, brinda una estructura normativa integral destinada a supervisar y regular el despliegue del ciberpatrullaje por parte de las fuerzas de seguridad federales. Su propósito fundamental radica en la regulación y control de la vigilancia en el ámbito digital, con la finalidad de prevenir y contrarrestar la comisión de delitos cibernéticos. Este documento busca asegurar que estas acciones se lleven a cabo dentro de los límites legales y éticos, velando por el respeto absoluto a los derechos humanos y la salvaguarda de la privacidad de todos los ciudadanos.

En este apartado se procederá a examinar los detalles de esta resolución, así como sus fundamentos legales, es decir, cómo la base jurídica de la resolución se apoya en diversas normativas tanto nacionales como internacionales. Asimismo, se abordarán los aspectos técnicos del ciberpatrullaje, la amplia gama de delitos prioritarios que deben ser destacados en las operaciones de ciberpatrullaje, así como la supervisión y la rendición de cuentas, con el fin de garantizar la transparencia en relación con las acciones llevadas a cabo por las fuerzas durante el ciberpatrullaje.

9.1. Fundamentos Legales

La base legal de la Resolución 428/2024 se sustenta en un conjunto de normativas nacionales e internacionales, lo que respalda su fundamentación jurídica y su alcance en términos de regulación y aplicación. Se pueden mencionar las siguientes:

- Constitución Nacional: la resolución se adecúa con los principios y derechos establecidos en la Constitución Nacional de Argentina, garantizando que las prácticas de ciberpatrullaje no violen derechos fundamentales como la libertad de expresión y el derecho a la privacidad (Resolución 428/2024; Gargarella, 2021). La Constitución protege estos derechos en los artículos 14 y 19, y cualquier forma de monitoreo digital debe cumplir con las garantías constitucionales correspondientes.

- Ley de Protección de Datos Personales N° 25.326: este marco legal regula el tratamiento de datos personales, estableciendo que cualquier recolección, almacenamiento y procesamiento de datos debe hacerse con el consentimiento del titular de los datos o bajo orden judicial. En este sentido, la resolución especifica que los datos sensibles no pueden ser tratados sin la debida autorización judicial y cualquier información recopilada debe ser destruida si no se judicializa (Resolución 428/2024). Esta ley protege los datos personales y garantiza que el procesamiento de datos sea transparente y sea llevado a cabo con responsabilidad (Resolución 428/2024; Onocko, 2024).
- Pactos Internacionales de Derechos Humanos: Argentina es signataria de diversos pactos internacionales que protegen los derechos humanos, incluyendo el Pacto Internacional de Derechos Civiles y Políticos. La resolución garantiza que las prácticas de ciberpatrullaje cumplan con estos compromisos a nivel internacional (ACNUDH, 2021). Estos acuerdos obligan al Estado a proteger derechos fundamentales como la privacidad y la libertad de expresión, incluso en el contexto digital (ACNUDH, 2021).
- Decreto N° 954/17 y Decreto Ley N° 13.473/57: ambos decretos establecen el marco legal para la estructura y operatividad de las fuerzas de seguridad, así como para la integración de tecnologías avanzadas en sus operaciones (Resolución 428/2024). Estos decretos capacitan a las fuerzas de seguridad para adoptar y aprovechar nuevas tecnologías con el fin de mejorar la efectividad de sus labores de vigilancia y seguridad (Resolución 428/2024).

9.2. Aspectos Técnicos del Ciberpatrullaje

Desde un punto de vista técnico, la Resolución 428/2024 permite el uso de una variedad de tecnologías avanzadas para llevar a cabo tareas de ciberpatrullaje, a saber:

- Inteligencia Artificial: la IA se utiliza para analizar grandes volúmenes de datos de forma eficaz, permitiendo la identificación de patrones y comportamientos sospechosos que puedan indicar actividades delictivas (Russell & Norvig, 2021). Los algoritmos de

IA pueden detectar anomalías en el comportamiento en línea que podrían sugerir la realización de actividades ilícitas (Onocko, 2024).

- Aprendizaje Automático (*machine learning*): Esta tecnología capacita a los sistemas para aprender y perfeccionarse utilizando información previa, lo que aumenta la precisión y adaptabilidad en la detección de delitos (Goodfellow et al., 2016). Los modelos de aprendizaje automático pueden adaptarse y perfeccionarse con el tiempo, lo que incrementa su efectividad en la identificación de actividades sospechosas (Resolución 428/2024).
- Redes Neuronales y Sistemas Expertos: estas tecnologías de vanguardia imitan el funcionamiento del cerebro humano para llevar a cabo tareas complejas como el reconocimiento de imágenes y la predicción de comportamientos, lo que potencia considerablemente la habilidad de las fuerzas de seguridad para detectar actividades delictivas (Goldblum et al., 2023). Las redes neuronales profundas (*deep learning*) son especialmente eficaces en el análisis de grandes conjuntos de datos sin una estructura definida, como imágenes y texto proveniente de plataformas de redes sociales (Resolución 428/2024). Los sistemas expertos proporcionan una base de conocimiento especializada que puede ser aplicada en tiempo real para evaluar situaciones específicas con precisión y eficiencia. La combinación de estas herramientas permite una detección más precisa y rápida de actividades sospechosas (Goodfellow et al., 2016; Goldblum et al., 2023).
- Fuentes Digitales Abiertas: el ciberpatrullaje se lleva a cabo exclusivamente en fuentes digitales abiertas y sitios web de acceso público, garantizando que no se viole la privacidad de comunicaciones privadas sin una autorización judicial (Resolución 428/2024; MEITy, 2023). Esto incluye redes sociales, foros, blogs y otros sitios web de acceso público, asegurando que la vigilancia respete la privacidad individual (Resolución 428/2024).

9.3. Delitos Prioritarios

La resolución detalla una extensa variedad de delitos que deben recibir prioridad en las operaciones de ciberpatrullaje. Estos delitos son enumerados a continuación:

- venta de drogas y armas
- amenazas y extorsión
- ciberdelitos y fraudes
- violencia de género y acoso sexual
- distribución de pornografía infantil
- trata de personas y lavado de dinero
- terrorismo

Este enfoque exhaustivo ha sido concebido para hacer frente a las múltiples manifestaciones de delincuencia presentes en el entorno digital, con el propósito de resguardar a la sociedad de amenazas de considerable magnitud (Resolución 428/2024).

9.4. Supervisión y Rendición de Cuentas

Para garantizar la transparencia y la responsabilidad, la Resolución 428/2024 establece la obligación de que las fuerzas de seguridad presenten informes detallados mensuales sobre sus actividades de ciberpatrullaje. Estos informes son supervisados por el Ministerio de Seguridad, que utiliza estadísticas y denuncias ciudadanas para ofrecer directrices estratégicas, asegurando que las prácticas se adhieran a los estándares legales y éticos establecidos (Resolución 428/2024). Esta supervisión abarca auditorías periódicas y la revisión de los procedimientos para garantizar el respeto de los derechos fundamentales (Onocko, 2024).

Capítulo 10 - Creación de la Unidad de Inteligencia Artificial Aplicada a la Seguridad

10.1. Establecimiento del Organismo

Este documento académico explora la creación de la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS) según la Resolución 710 del Ministerio de Seguridad, sancionada en 2024. La UIAAS, dependiente de la Dirección de Ciberdelito y Asuntos Cibernéticos, surge como una respuesta estratégica a la creciente amenaza de delitos cibernéticos y busca mejorar la eficacia de las fuerzas de seguridad mediante la aplicación de tecnologías avanzadas de inteligencia artificial. El análisis considera el contexto normativo, las funciones específicas de la UIAAS, y su importancia en el marco de la seguridad nacional e internacional.

El avance de la tecnología, especialmente en el ámbito de la inteligencia artificial (IA), ha transformado significativamente la forma en que se manejan los asuntos de seguridad a nivel mundial. Países como Estados Unidos, China, Reino Unido, Israel, Francia, Singapur e India han liderado la integración de IA en sus operaciones gubernamentales y de seguridad. La Resolución 710 del Ministerio de Seguridad de se enmarca en esta tendencia global, estableciendo la UIAAS con el objetivo de fortalecer las capacidades de prevención, detección, investigación y persecución del delito.

10.2. Contexto Normativo y Legal

La creación de la UIAAS está respaldada por una serie de normativas y resoluciones previas. La Ley de Ministerios (texto ordenado por Decreto N° 438 de 1992 y sus modificatorias) y el Decreto N° 50 del 19 de diciembre de 2019, junto con la Decisión Administrativa Nº 340 del 16 de mayo de 2024 y la Resolución del Ministerio de Seguridad Nº 428 del 27 de mayo de 2024, proporcionan el marco legal necesario para su establecimiento. Estos documentos subrayan la competencia del Ministerio de Seguridad en la protección de la seguridad interior y la preservación de los derechos y garantías de los ciudadanos.

10.3. Funciones y Objetivos de la UIAAS

La UIAAS está diseñada para abordar una variedad de amenazas cibernéticas mediante el uso de IA. Sus principales funciones incluyen:

- Patrullaje de redes sociales y la "Internet profunda": identificación de delitos e investigación de situaciones de riesgo;
- Reconocimiento de imágenes: comparación e identificación de imágenes en soporte físico o virtual;
- Análisis en tiempo real de cámaras de seguridad: detección de actividades sospechosas y personas buscadas;
- Predicción de delitos: utilización de algoritmos de aprendizaje automático para analizar datos históricos y prever futuros crímenes;
- Detección de amenazas cibernéticas: identificación de malware, phishing y otras formas de ciberataque;
- Procesamiento de grandes volúmenes de datos: creación de perfiles de sospechosos y vinculación de casos;
- Vigilancia mediante drones: supervisión de áreas extensas y respuesta a emergencias;
- Desactivación de explosivos mediante robots: realización de tareas peligrosas;
- Mejora de la comunicación y coordinación: asegurar la compartición eficiente de información crítica entre fuerzas de seguridad;
- Análisis de actividades en redes sociales: detección de amenazas y movimientos de grupos delictivos;
- Detección de transacciones financieras sospechosas: identificación de actividades ilegales.

10.4. Importancia Estratégica de la UIAAS

La UIAAS representa un paso crucial hacia la modernización de las capacidades de seguridad del Ministerio de Seguridad. La adopción de tecnologías de IA no solo mejoría la eficiencia y la precisión en la respuesta a amenazas, sino que también posiciona al país a la

vanguardia de la seguridad cibernética global. Al integrar estas tecnologías, la UIAAS puede abordar de manera más efectiva las complejidades y dinámicas de los delitos modernos, proporcionando un entorno más seguro para los ciudadanos.

En definitiva, la creación de la UIAAS mediante la Resolución 710 refleja un enfoque proactivo y adaptativo hacia los desafíos de la seguridad en la era digital. Con un marco legal sólido y funciones bien definidas, la UIAAS está bien posicionada para enfrentar las amenazas cibernéticas contemporáneas. Su establecimiento no solo fortalece la capacidad de respuesta del Ministerio de Seguridad, sino que también asegura una integración efectiva de tecnologías avanzadas en la lucha contra el delito. De todos modos, es imprescindible que se tomen las precauciones pertinentes y se analicen los alcances de la tecnología que se empleará y para qué fines.

10.5. Consideraciones Puntuales

La resolución permite indicar que la creación de la UIAAS es fundamental para la Argentina y múltiples aspectos relevantes en estos tiempos, como una respuesta estratégica para enfrentar las crecientes amenazas cibernéticas, mejorando la eficacia de las fuerzas de seguridad mediante el uso de tecnologías avanzadas de IA. En este sentido, la UIAAS utiliza IA para monitorear redes sociales abiertas y la "internet profunda" (dark web) en busca de actividades delictivas. La identificación de delitos y la investigación de situaciones de riesgo son fundamentales para prevenir amenazas graves a la seguridad pública. Este patrullaje proactivo permite la detección temprana de posibles crímenes, ayudando a las fuerzas de seguridad a actuar con mayor rapidez y precisión. La UIAAS emplea tecnología avanzada de reconocimiento de imágenes para comparar e identificar imágenes en soporte físico o virtual. Esto es crucial en investigaciones criminales, donde la identificación precisa de personas y objetos puede proporcionar pruebas fundamentales. El reconocimiento facial y de objetos en tiempo real permite la rápida identificación de sospechosos y la vinculación de pruebas visuales con incidentes delictivos.

El análisis de imágenes de cámaras de seguridad en tiempo real es una de las capacidades más innovadoras de la UIAAS. Utilizando algoritmos de reconocimiento facial y

de comportamiento, la unidad puede detectar actividades sospechosas e identificar personas buscadas de manera inmediata. Esta capacidad mejora significativamente la respuesta a incidentes y la vigilancia continua en áreas críticas. Mediante el uso de algoritmos de aprendizaje automático, la UIAAS analiza datos históricos de crímenes para predecir futuros delitos. Esta función permite a las fuerzas de seguridad anticipar posibles amenazas y planificar estrategias preventivas efectivas. La predicción basada en datos históricos optimiza la asignación de recursos y la implementación de medidas de seguridad proactivas.

La identificación de amenazas cibernéticas antes de que se produzcan ataques es esencial para la protección de infraestructuras críticas. La UIAAS detecta *malware*, *phishing* y otras formas de ciberataque mediante el análisis continuo de patrones inusuales en las redes informáticas. Esta vigilancia constante permite una respuesta inmediata a amenazas emergentes y reduce el riesgo de daños significativos. La capacidad de procesar grandes volúmenes de datos de diversas fuentes es una ventaja clave de la UIAAS. Mediante el análisis de datos masivos, la unidad puede extraer información útil, crear perfiles de sospechosos e identificar vínculos entre diferentes casos. Este enfoque basado en datos mejora la precisión de las investigaciones y la identificación de patrones delictivos complejos.

Por su parte, el uso de drones permite a la UIAAS realizar vigilancia aérea en áreas extensas y de difícil acceso. Los drones proporcionan imágenes en tiempo real y pueden responder rápidamente a emergencias, aumentando la cobertura y eficacia de las operaciones de seguridad. Esta tecnología es especialmente útil en situaciones de búsqueda y rescate, así como en la vigilancia de eventos multitudinarios. La UIAAS emplea robots para realizar tareas peligrosas, como la desactivación de explosivos. Esta capacidad reduce el riesgo para los oficiales de seguridad y permite una intervención segura en situaciones de alta peligrosidad. Los robots equipados con IA pueden realizar operaciones precisas y controlar explosivos de manera efectiva, protegiendo tanto a los ciudadanos como a las fuerzas de seguridad.

La UIAAS mejora la comunicación y coordinación entre diferentes fuerzas policiales y de seguridad federales; así también, se debe mencionar que lograr que la información crítica se comparta de manera rápida y eficiente es esencial para una respuesta unificada y coherente a las amenazas. La IA facilita la integración de datos y la comunicación en tiempo real, optimizando

las operaciones conjuntas y la toma de decisiones. El análisis de actividades en redes sociales es crucial para detectar amenazas potenciales y prever movimientos de grupos delictivos. La UIAAS utiliza IA para identificar patrones y comportamientos sospechosos en las redes sociales, permitiendo una intervención preventiva. Esta capacidad ayuda a las fuerzas de seguridad a monitorear y neutralizar actividades delictivas antes de que se conviertan en amenazas reales.

La detección de transacciones financieras sospechosas es una función clave de la UIAAS. Mediante el análisis de comportamientos anómalos en transacciones financieras, la unidad puede identificar actividades ilegales como el lavado de dinero y la financiación del terrorismo. La IA permite una vigilancia continua y precisa de las transacciones, protegiendo la integridad del sistema financiero. La creación de la UIAAS conforme a la Resolución 710 refleja un enfoque proactivo y adaptativo hacia los desafíos de la seguridad en la era digital.

La implementación de la UIAAS traerá numerosos beneficios futuros a Argentina. Al mejorar la capacidad de respuesta a delitos cibernéticos, se protegerá mejor a los ciudadanos y se garantizará la seguridad de infraestructuras críticas. La eficiencia y precisión en la identificación y prevención de delitos aumentarán, lo que reducirá significativamente el riesgo de crímenes y amenazas. Además, la adopción de tecnologías avanzadas posicionará a Argentina como un líder en la seguridad cibernética a nivel global, promoviendo la confianza en las instituciones y atrayendo inversiones en tecnología y seguridad. Con funciones específicas y el respaldo de tecnologías avanzadas de inteligencia artificial, la UIAAS está preparada para enfrentar los desafíos contemporáneos de la seguridad. Su implementación no solo fortalece las capacidades de las fuerzas de seguridad, sino que también posiciona a Argentina como un líder en la adopción de IA para la protección y seguridad ciudadana.

De todos modos, como se mencionó anteriormente, es fundamental conocer en profundidad los alcances que tendrá este organismo y para qué será utilizada la tecnología. Es esencial que el organismo haga públicas sus acciones e iniciativas de manera transparente.

10.6. Opiniones Iniciales sobre la Resolución

10.6.1. Avances Tecnológicos y Seguridad

A pesar de que la resolución fue emitida este año, expertos en tecnología y derecho han examinado su contenido y destacado tanto los riesgos como los beneficios potenciales que podría conllevar esta normativa.

La mayoría de los países están evaluando cómo ajustar sus marcos normativos para asegurar un uso ético, seguro y transparente de la inteligencia artificial. La Unión Europea ha tomado la delantera con la reciente aprobación del Reglamento sobre Inteligencia Artificial (RIA). La tecnología en sí misma no es intrínsecamente buena o mala; su efecto dependerá del modo en que se utilice. El principal reto regulatorio consiste en diseñar un sistema normativo que proteja de manera efectiva los derechos fundamentales, sin imponer restricciones excesivas que puedan frenar el progreso tecnológico. La implementación de la UIAAS conlleva ciertos inconvenientes importantes que requieren una aclaración y un análisis minucioso. Una de las posturas más controvertidas "es la facultad otorgada a la UIAAS de procesar grandes volúmenes de datos de diversas fuentes para crear perfiles de sospechosos o identificar vínculos entre diferentes casos" (Laje, 2024). Esto implica evaluar a las personas no en función de sus acciones actuales, sino en base a predicciones sobre comportamientos futuros, generadas a partir de perfiles construidos con criterios que las fuerzas de seguridad determinan de manera discrecional.

Asimismo, el Ministerio de Seguridad de la Nación destaca que el desarrollo "de la tecnología y la inteligencia artificial representa un cambio de relevancia para la población, y por ende se necesita utilizar estos avances en las Fuerzas Policiales y Seguridad Federales para responder más rápido y con mayor precisión las amenazas" (Ciampa Dolárd, 2024). Por lo tanto, es esencial utilizar la IA para prevenir, identificar, investigar y perseguir tanto los delitos como sus posibles vínculos.

10.6.2. Cumplimiento de la Ley, Protección de Datos y Alcance de la UIAAS

Es importante comprender que "la Resolución del Ministerio de Seguridad N°428/24, durante las labores preventivas el personal policial debe cumplir con la Ley de Protección de Datos Personales N° 25.326" (Beccar Varela et al., 2024). Asimismo, la resolución omite que (a) está prohibido de manera estricta manejar datos sensibles sin la debida autorización judicial, así como utilizar publicaciones que involucren a menores sin el permiso correspondiente, y (b) que si se identifica que una actividad preventiva involucra a un menor, esta deberá suspenderse de inmediato y notificar a las autoridades competentes, salvo que exista un riesgo vital para el menor.

Con respecto al uso de herramientas tecnológicas para la prevención de conductas delictivas, el alcance y las restricciones de las funciones de la nueva UIAAS tendrán que ser analizadas de manera profunda, "teniendo en consideración los potenciales problemas en cuanto al derecho a la privacidad y la validez o legalidad de la actuación de las fuerzas de seguridad" (Beccar Varela et al., 2024).

El enfoque que adquiere este organismo, parece vulnerar el principio de presunción de inocencia establecido en la Constitución Nacional. En respuesta, el RIA prohíbe de manera explícita el uso de IA para la creación de perfiles sospechosos con el propósito de anticipar delitos futuros, a menos que estos perfiles se basen en hechos objetivos y verificables directamente vinculados a actividades delictivas. En este sentido, "la resolución nacional también autoriza al UIAAS a utilizar IA para analizar datos históricos de crímenes y, de ese modo, predecir delitos futuros" (Rueda Laje, 2024). Aunque esta práctica es innovadora y podría aumentar la eficacia en la prevención del crimen, es crucial establecer criterios precisos para evitar sesgos y discriminaciones. Por lo tanto, además de los criterios especificados en el Artículo 4, inciso (a) de la resolución 484/2024, es fundamental incorporar otras categorías relevantes, como la nacionalidad, la condición socioeconómica y la identidad de género, en la lista de criterios prohibidos.

10.6.3. Identificación de Amenazas Cibernéticas

Un aspecto crucial es la capacidad de identificar patrones atípicos en las redes informáticas y detectar amenazas cibernéticas antes de que se materialicen en ataques. Esto abarca la identificación de *malware*, *phishing* y otras modalidades de ciberataques. Asimismo, el organismo tendrá que facultad de "analizar imágenes de cámaras de seguridad en tiempo real a fin de detectar actividades sospechosas o identificar personas buscadas utilizando reconocimiento facial" (Peirano, 2024).

Esta cuestión es importante, dado que arroja luz sobre puntos concretos y sensibles, por ejemplo, con respecto a que la nueva normativa posee la capacidad de identificar patrones atípicos en las redes informáticas y detectar amenazas cibernéticas antes de que se concreten en ataques efectivos. Esta habilidad es fundamental para prevenir daños potenciales y mitigar riesgos asociados a la ciberseguridad. Esta capacidad incluye la detección de modalidades de ciberataques que podrían comprometer la integridad de los sistemas informáticos y, asimismo, la seguridad de la información.

Además, la normativa otorga al organismo la facultad de analizar imágenes de cámaras de seguridad en tiempo real. Esta capacidad permite la supervisión constante de espacios públicos y privados para identificar actividades sospechosas. El uso de tecnologías avanzadas, como el reconocimiento facial, se integra en esta función, permitiendo la identificación de personas buscadas o involucradas en actividades delictivas. Esta integración tecnológica facilita la vigilancia proactiva y la intervención temprana, contribuyendo a una respuesta más rápida y eficiente ante potenciales amenazas.

Es importante señalar, que el enfoque en la vigilancia en tiempo real también destaca la importancia de la capacidad de procesar y analizar grandes volúmenes de datos visuales. Esto incluye la revisión de imágenes capturadas por múltiples cámaras ubicadas en áreas estratégicas, lo que puede proporcionar información valiosa para la prevención del delito y la seguridad pública. La implementación de estas tecnologías promete mejorar significativamente la capacidad del organismo para prevenir incidentes y garantizar una mayor seguridad en los entornos vigilados. En conjunto, la capacidad para identificar patrones atípicos y analizar imágenes en tiempo real representa un avance significativo en la estrategia de seguridad, con el

potencial de transformar la forma en que se gestionan y responden las amenazas cibernéticas y delictivas.

El uso del reconocimiento facial en espacios públicos para identificar personas buscadas y detectar actividades sospechosas en tiempo real es un aspecto, que como se puede advertir, es crucial. Aunque esta tecnología puede ser eficaz en algunos contextos, su aplicación de esta manera conlleva una invasión generalizada a la privacidad, ya que posibilita una vigilancia continua y omnipresente de la ciudadanía.

Se debe mencionar, que en la Unión Europea, "el RIA se posiciona bajo la premisa de que el uso indiscriminado de esta tecnología puede socavar los derechos fundamentales de los ciudadanos y crear una sociedad de vigilancia" (Rueda Laje, 2024). Por este motivo, se prohíbe de manera explícita el uso de sistemas de reconocimiento facial en tiempo real en espacios públicos, excepto en casos excepcionales y siempre que se cuente con salvaguardias adecuadas.

Por estos motivos, es esencial establecer mecanismos para evaluar y mitigar los riesgos asociados con los sistemas de inteligencia artificial, como los sesgos algorítmicos y los errores, mediante auditorías y una supervisión humana continua. También es fundamental ofrecer información clara y accesible sobre las características y riesgos del sistema, asegurando así transparencia y una comprensión adecuada por parte de los usuarios. La falta de transparencia puede incrementar el riesgo de malentendidos y desconfianza pública, además de poner en peligro el derecho a la privacidad de las personas.

10.6.4. Controversias sobre la Implementación y Control

La nueva unidad estatal no se encargará de investigar las redes sociales de los ciudadanos. El ciberpatrullaje, en esencia, es comparable al patrullaje físico realizado por un oficial en la calle. Esta unidad no accederá a perfiles individuales ni buscará información específica sobre personas en particular. En lugar de realizar inteligencia sobre individuos, su labor se centrará en la investigación general de actividades delictivas en el ámbito digital. En definitiva, lo que se busca es el delito, no la persona; concretamente, si se identifica "un comentario en un grupo sobre la venta de drogas, el enfoque será judicializar ese hecho específico. Posteriormente, la Justicia podrá solicitar información adicional relacionada con el

caso. No se recopilarán datos sobre individuos sin contar con una orden judicial" (Bellengeri, 2024, como se citó en Davidovsky, 2024). Para los especialistas, aún no está definido el software que se utilizará ni tampoco los analistas que conformarán el equipo. Actualmente, el país se encuentra en las etapas iniciales de exploración de alternativas y soluciones, y en el proceso de desarrollar protocolos. La puesta en marcha de estas iniciativas se encuentra todavía en una etapa preliminar. De todos modos, este especialista resalta que no se perseguirá a individuos específicos, y si alguien deja de publicar contenido por temor, eso iría más allá de los objetivos previstos. Aunque algunos ciudadanos puedan pensar de esa manera, en realidad no es el propósito de la iniciativa, su enfoque está claramente dirigido a la prevención de delitos específicos, como la trata de personas y el narcotráfico, y no a la vigilancia general de la población.

El ciberpatrullaje, generalmente, es percibido como una violación a las leyes de inteligencia nacional, seguridad interior y los códigos procesales penales. De este modo, "la inteligencia (vigilancia específica de conductas y personas) debe hacerse bajo control judicial y sobre sospechas de delitos concretos" (Pallero, 2024, como se citó en Davidovsky, 2024). Recolectar información de manera general para luego determinar si existen delitos potenciales es incompatible con la Constitución y con las leyes vigentes. De esta manera, se debería implementar un método de vigilancia preventiva que no se transforme en inteligencia criminal. Esto se lograría mediante leyes apropiadas, controles judiciales continuos y la aplicación rigurosa de protocolos que restrinjan la observación a aspectos o términos muy generales. En el momento en que se identifique información que justifique un análisis más detallado de las publicaciones de ciertas personas, la actividad deberá considerarse como inteligencia criminal y someterse a las regulaciones procesales correspondientes.

10.6.5. Deficiencias en la Resolución y Riesgos para las Libertades Civiles

Con respecto a deficiencias específicas en cuanto al derecho, la Resolución 710/2024, que establece la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS), no solo está llena de deficiencias jurídicas, sino que también prevé llevar a cabo actividades para las cuales la utilización de inteligencia artificial no debería estar contemplada. La normativa establece un

marco para el uso de sistemas de IA en la predicción de delitos, la elaboración de perfiles de personas, el análisis de casos y la detección de fraudes, entre otras aplicaciones. Pero, al mismo tiempo, “no hay en la resolución ningún reaseguro de legalidad y debido proceso en la aplicación de estas tecnologías, se desconoce el tipo de herramientas a utilizar, los proveedores y los mecanismos de contralor para las mismas” (Busaniche, 2024).

En resumen, la resolución representa una manera rudimentaria de encubrir un avance desproporcionado e inaceptable sobre las libertades civiles, disfrazado bajo la promesa de una tecnología sin fundamento. Desde el punto de vista legal, las propuestas de la Ministra de Seguridad están en conflicto con los principios establecidos en la ley de inteligencia (Busaniche, 2024). Aunque la UIAAS no se presenta formalmente como una entidad de inteligencia, sus funciones efectivamente se ajustan a esa categoría y, por ende, están sujetas a la prohibición explícita de ciertas cuestiones, como por ejemplo: acceder a información, producir inteligencia o almacenar datos sobre personas, únicamente por su raza, religión, vida privada, opiniones políticas, afiliación a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, o por la actividad lícita que desarrollen en cualquier ámbito. Estas consideraciones están estipuladas expresamente por el artículo 4 de la Ley de Inteligencia Nacional, ley 25.520 del año 2001.

En definitiva, más allá de la mención a la constitución y la legislación vigente, “la resolución no integra ningún elemento que permita imaginar siquiera un mínimo control sobre la utilización por parte de las fuerzas de seguridad federales de estas tecnologías” (Busaniche, 2024). Al mismo tiempo, no se contempla ninguna auditoría, análisis de impacto ni políticas de supervisión y control para estas medidas. Esta situación deja un vacío significativo en cuanto a la vigilancia y regulación de las herramientas tecnológicas, poniendo en riesgo el cumplimiento de estándares legales y éticos fundamentales.

10.7. Consideraciones Técnicas y Jurídicas sobre la UIAAS

En este apartado se examinará cómo una entidad como la UIAAS, a pesar de sus buenas intenciones, puede comprometer las libertades de los ciudadanos. Es un tema complejo, ya que,

aunque un organismo estatal busque proteger la seguridad de la población, puede, al mismo tiempo, provocar infracciones a esas mismas libertades.

Es evidente, que la democracia en Argentina ha evolucionado desde finales de 1983, no solo por las reformas jurídicas e institucionales que se han implementado a lo largo del tiempo, sino también por los cambios fundamentales en las interacciones humanas impulsados por las nuevas tecnologías de comunicación. Estas innovaciones han transformado la forma en que los ciudadanos se relacionan y participan en el proceso democrático, añadiendo una dimensión adicional a su evolución. Por lo tanto, para comprender adecuadamente la sociedad argentina, es crucial considerar los avances tecnológicos que la han impactado profundamente. No se puede analizar la realidad social sin tener en cuenta cómo estas innovaciones han moldeado y transformado las dinámicas y las interacciones dentro del país.

Desde el Ministerio de Seguridad de la Nación se han implementado dos resoluciones de gran importancia. Sin embargo, estas decisiones parecen haber sido ignoradas en términos de debate público y no han generado el impacto esperado a pesar de su relevancia. Ambas podrían influir considerablemente en la calidad de vida de los ciudadanos debido a su potencial para afectar ciertos derechos fundamentales inherentes a ellos. Entre los derechos más evidentes que podrían verse afectados se encuentran la intimidad, la dignidad humana y la libertad de expresión, aunque el impacto no se limita a estos aspectos. Esto se refiere a las Resoluciones Nros. 428/2024 y 710/2024, publicadas en mayo y julio pasados, respectivamente.

Si se comparan las resoluciones 428 y 710, al examinar los propósitos y competencias establecidos en ambas resoluciones, se observa que en varios casos se autoriza la realización de actividades que, en tiempos recientes, han sido prohibidas o estrictamente limitadas en sociedades similares a la nuestra, que se citan como ejemplos a seguir. En particular, se advierte que las resoluciones incluyen actividades sin detallar quién será el encargado del desarrollo o suministro tecnológico, ni las especificaciones de los sistemas de inteligencia artificial que se utilizarán (Riquert, 2024).

Estas actividades están restringidas en la Unión Europea, donde el Parlamento Europeo aprobó en marzo de 2024 la propuesta de Reglamento de Inteligencia Artificial (RIA), que establece regulaciones claras al respecto. El RIA constituye una auténtica Ley de Inteligencia

Artificial (LIA), pionera a nivel global, y que aborda de manera fundamental las prácticas de inteligencia artificial prohibidas (Riquert, 2024).

En relación con el uso de la IA para labores de inteligencia, es fundamental debatir y definir claramente qué se va a investigar, con qué propósito y para qué fines específicos se utilizará dicha inteligencia. En este caso particular, el tema se acentúa debido a que se trata de "la conceptualización de la inteligencia de fuentes abiertas (OSINT) imprecisa y no atrapa su concepto en toda su extensión, y eso dificulta la posibilidad de analizar las tensiones que podría generar la utilización de estas herramientas por parte de agentes estatales" (Riquert, 2024, p. 9). En este caso específico, el Ministerio de Seguridad asume un rol central, ya que, de acuerdo con el artículo 6 de la resolución en cuestión, será el encargado de definir los lineamientos y prioridades estratégicas para las tareas preventivas. El Ministerio se basa en indicadores de su propia creación, como las estadísticas de los informes enviados a la Dirección de Ciberdelito y Asuntos Cibernéticos (a la que estará subordinada la UIAAS), y añade un vago término de "otras fuentes" sin especificar detalles adicionales. Esto implica que podría recurrir a cualquier criterio que considere apropiado el responsable.

Se podría esgrimir una objeción genérica, aduciendo que al pasar al tratamiento de la Res. 710/2024, en su artículo 3° se precisa que la misión de la UIAAS es "la prevención, detección, investigación y persecución del delito y sus conexiones mediante la utilización de la inteligencia artificial" (Riquert, 2024, p. 9) . Asimismo, El artículo 4º establece las funciones asignadas para cumplir con esta misión. Las examinaremos y comentaremos de manera individual. Sin embargo, antes de entrar en detalle, es importante señalar que una revisión superficial de la estructura y las funciones propuestas plantea una objeción general esencial: ¿quién supervisará al organismo encargado y cómo se garantizará que no haya desvíos en la información sensible recopilada? En última instancia, la UIAAS funcionará en la Dirección de Ciberdelito y Asuntos Cibernéticos, que depende de la Unidad de Gabinete de Asesores del propio Ministerio (art. 1º), y estará regida "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)" (Riquert, 2024, p. 11).

En otras palabras, se le otorga a la UIAAS una función de ciberpatrullaje con un alcance extremadamente amplio e impreciso: no solo investigar delitos e identificar a sus autores, sino también llevar a cabo tareas "preventivas", como la detección de situaciones de riesgo grave para la seguridad. Aunque la Constitución debería ser el límite, lo que se está permitiendo es que esta nueva estructura realice tareas de inteligencia de manera continua y sin restricciones claras (¿qué actividades constituyen un riesgo grave para la seguridad?), sin una hipótesis delictiva concreta ni supervisión judicial (o de otro tipo). Este primer inciso, vago y general, sugiere que el Ministerio está habilitando a un organismo con un poder intrusivo desmedido sobre los asuntos sociales. Se debe resaltar, que esta situación acontece en un momento de la sociedad "en que gran parte de la vida comunitaria transita justamente por las redes sociales u otras instancias tecnológicas (como podría ser el metaverso)" (Riquert, 2024, p. 12).

Asimismo, es crucial atender a los sistemas que la UIAAS planea utilizar, como los sistemas de reconocimiento facial. La preocupación radica en que, actualmente, no existe una normativa que regule estos sistemas adecuadamente, o bien la normativa existente es insuficiente (como la falta de control y supervisión sobre los operadores). Además, esta normativa se ha establecido sin un debate adecuado sobre los derechos que pueden verse comprometidos con el uso de la tecnología de reconocimiento facial, tales como la libertad personal, la libertad de expresión, la libertad de asociación (considerando su posible uso para la represión de opositores políticos), así como la intimidad, la privacidad y la autodeterminación informativa. Este caso ilustra la clásica tensión entre eficacia y garantías. A pesar de que los problemas actuales de errores de identificación, que pueden llevar a la privación de la libertad ambulatoria, se resolverán eventualmente con los avances tecnológicos, la verdadera cuestión es cómo lograr una mayor eficacia en la persecución del delito sin sacrificar los derechos fundamentales en el proceso.

Para ilustrar esta problemática, se puede recordar un incidente significativo que ocurrió poco después de la implementación del sistema en la CABA, conocido como el caso "Ibarrola" el cual tuvo una amplia repercusión mediática. Debido a una identificación incorrecta, una persona fue arrestada durante seis días tras ser erróneamente acusada de un robo agravado cometido en 2016 en Bahía Blanca. Este error se originó por una carga errónea en el sistema, lo

que llevó a la detención del ciudadano exclusivamente basada en el reconocimiento facial, a pesar de que no existía ninguna orden de restricción en su contra.

Además, se debería reparar en el inciso (d.), que habla acerca de la utilización de algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos. Con respecto a esto, es importante destacar que "se trata de otra actividad que tiene un largo historial de cuestionamientos en el ámbito internacional, tanto sea en su versión de vigilancia predictiva, como en la de apoyo de decisiones judiciales con valoración de riesgos" (Riquert, 2024, p. 15).

En definitiva, esta herramienta podría profundizar la selectividad tradicional en la criminalidad patrimonial al amplificar el sesgo inherente en las bases de datos que alimentan el algoritmo. Los sistemas de inteligencia artificial no son completamente confiables ni neutrales; pueden producir errores debido a la mala calidad de los datos utilizados o a defectos en la programación del algoritmo. Estos sistemas, al estar influenciados por las limitaciones humanas, pueden generar resultados que reflejan prejuicios xenófobos, racistas o misóginos. Así, las respuestas obtenidas podrían estar sesgadas por el discurso dominante que se considera "correcto", lo que pone en riesgo la diversidad y la equidad.

También, el mencionado autor, hace una especial mención al inciso (f.) que habla acerca de 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 que se autoriza mediante este inciso es una extensa tarea de perfilamiento (profiling) que se aplicará a toda la población, clasificando a las personas en "sospechosos" y "no sospechosos" a partir del análisis de "grandes volúmenes de datos de diversas fuentes" (¿cuáles son esas fuentes? ¿cómo se obtuvieron? ¿por qué se eligieron estas en lugar de otras?). Este enfoque es claramente inaceptable, sobre todo "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»" (Rickert, 2024, p. 18). Esto implica que podríamos ser categorizados como "sospechosos" y enfrentar medidas de seguimiento intrusivo basadas en criterios que son imposibles de revisar o cuestionar, ya que están enmascarados dentro de los parámetros de entrenamiento y autoaprendizaje del algoritmo.

El Ministerio de Seguridad avanza bajo el pretexto de una necesidad urgente en materia de seguridad, buscando mejorar la eficacia en la prevención, investigación y persecución del delito. En muchos casos, los objetivos que se proponen alcanzar no parecen, a primera vista, inadecuados. Sin embargo, como se ha demostrado, lo que prevalece es la autorización de numerosas actividades que tienen un claro potencial para afectar derechos fundamentales. Estas actividades carecen de la precisión y las limitaciones necesarias basadas en principios de razonabilidad y proporcionalidad. Un ejemplo claro de esto es la autorización del ciberpatrullaje para cualquier tipo de delito, sin restricciones específicas.

En resumen, la Resolución 710 no detalla aspectos cruciales como la tecnología utilizada, los proveedores, los métodos de acceso y protección, ni la trazabilidad y transparencia del sistema. Este conocimiento es esencial, ya que, contrariamente a la idea errónea de que la tecnología es neutra, los algoritmos están diseñados con sesgos ideológicos que influyen en los resultados que generan. Además, no existen controles externos independientes a la autoridad ministerial, lo que crea vacíos que pueden facilitar la represión de la protesta social y el acceso no autorizado a información confidencial de organismos de inteligencia. En muchos casos, se permite la implementación de tecnologías que en países citados como ejemplos ya han sido prohibidas (como el perfilamiento masivo para categorizar a la población) o severamente restringidas (especialmente en lo relativo al reconocimiento facial). La reciente regulación europea sobre IA, considerada pionera a nivel mundial, ofrece ejemplos de enfoques más rigurosos en este ámbito.

10.8. Proyecto de Ley Anulación de la Resolución 710

Se debe indicar, que diez días después de que la Resolución 710/2024 fuera sancionada, un grupo de diputados nacionales pertenecientes al Frente de Izquierda y de los Trabajadores, presentó un proyecto de ley para anular dicha resolución sancionada por el Gobierno.

El Artículo 1° del proyecto de ley es contundente y propone:

> Se anula la Resolución 710/2024 del Ministerio de Seguridad de la Nación, publicada en el Boletín Oficial con fecha del 29/07/2024 (RESOL-2024-710-APN-MSG), por medio de la cual se crea 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.

Según este proyecto, es claro que se está avanzando en la legalización del espionaje masivo sobre las personas, incluso aquellas que no han cometido ni han sido acusadas de ningún delito. Este tipo de monitoreo indiscriminado socava la presunción de inocencia, ya que convierte a todos los usuarios en sospechosos potenciales, sometiéndolos a una vigilancia encubierta. Además, no se han ofrecido detalles sobre cómo se utilizará la Inteligencia Artificial en estos procesos, qué mecanismos de control se implementarán, cuáles serán las medidas preventivas, y si las situaciones a monitorear están relacionadas con investigaciones judiciales. La falta de una orden judicial para estas acciones por parte de las fuerzas de seguridad infringe garantías constitucionales fundamentales y principios básicos de las libertades democráticas.

Además, este grupo de diputados menciona que es importante señalar que las prácticas de monitoreo que implican observar indiscriminadamente lo que las personas publican, sin una definición clara de los objetivos y los individuos a ser observados, se conocen como "excursiones de pesca". Estas prácticas están estrictamente prohibidas por leyes tanto locales como internacionales, ya que no cumplen con las salvaguardias fundamentales de derechos humanos, como los principios de legalidad, necesidad y proporcionalidad.

Asimismo, el proyecto asevera que la creación de la UIAAS busca otorgar amplios poderes a las fuerzas policiales y a las agencias de represión federales, como la Policía Federal, la Gendarmería, la Policía Aeroportuaria y el Servicio Penitenciario General, para realizar espionaje cibernético. Esto se llevará a cabo mediante una unidad de ciberpatrullaje equipada con inteligencia artificial para supervisar las redes sociales. Con esta nueva herramienta de vigilancia y persecución, el gobierno pretende intensificar la represión de la libertad de expresión y podría instaurar un clima de miedo ideológico.

Con la creación de la UIAAS, el gobierno tiene la capacidad de monitorear las opiniones, declaraciones y actividades de millones de personas. Como resultado de esta vigilancia, muchos usuarios de redes sociales podrían optar por abstenerse de comentar sobre temas políticos o ideológicos por temor a represalias. Mientras el gobierno establece esta nueva agencia de ciberpatrullaje, el proyecto presentado por la oposición plantea que esta herramienta

permitirá que "los trolls libertarios que amenacen de muerte a los opositores en internet actúen sin consecuencias". De este modo, el proyecto de ley presentado por este grupo de diputados, resalta que "es evidente que estamos ante una política totalitarista, que sólo tiene por objeto robustecer todos los medios del Estado para perseguir, espiar y conspirar contra los trabajadores y los que se oponen a su política". Sobre todo, se resalta que la UIAAS pretende vigilar a aquellos que, particularmente, se manifiestan y organizan contra las políticas de ajuste y la ofensiva contra los derechos de los trabajadores promovida por el gobierno.

En el contexto de una intensificación de la represión del gobierno contra los trabajadores y la oposición política, el proyecto de ley destaca que permitir que una unidad de vigilancia bajo su control pueda identificar, por ejemplo, la afiliación política de una persona crítica del oficialismo y tomar medidas al respecto representa un precedente extremadamente peligroso para las libertades democráticas. Este refuerzo de los poderes represivos del gobierno facilita la imposición de los ataques de la clase capitalista contra los trabajadores, consolidando aún más su control autoritario.

Capítulo 11 - Identificar y Mitigar los Riesgos de la IA en el Ciberpatrullaje Financiero

El uso de la IA en el sector financiero está transformando radicalmente las prácticas de ciberseguridad y la detección de fraudes. El informe del Departamento del Tesoro de los Estados Unidos (2024), denominado *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector*, ofrece una evaluación exhaustiva de los riesgos asociados con la IA y, al mismo tiempo, presenta estrategias de mitigación de los peligros que presenta la seguridad. En este apartado se examinarán los riesgos y las estrategias en el contexto del ciberpatrullaje financiero, con el objetivo de proporcionar una visión integral de los desafíos y oportunidades que presenta la implementación de IA en este sector.

11.1. Identificación de Riesgos Específicos de la IA

11.1.1. Manipulación de Datos

La manipulación de datos, también conocida como *data poisoning*, sucede cuando los atacantes introducen datos falsos o corruptos en los conjuntos de datos empleados para entrenar los modelos de IA. Este tipo de ataque puede distorsionar los patrones aprendidos por los modelos, afectando su capacidad para detectar fraudes y amenazas cibernéticas de manera precisa (Departamento del Tesoro de EE. UU., 2024). Asimismo, estos ataques pueden ser sutiles y discretos, dificultando la capacidad de los profesionales de poder detectarlos. Por estos motivos, propicia que el modelo aprenda y desarrolle patrones incorrectos y tome decisiones erróneas (Instituto Nacional de Estándares y Tecnología, NIST, 2024).

En lo que respecta a las implicaciones, se debe indicar que la manipulación de datos puede resultar en la detección incorrecta de actividades legítimas como fraudulentas o en la omisión de actividades fraudulentas, comprometiendo la fiabilidad y efectividad de los sistemas de ciberpatrullaje basados en IA. Este riesgo es particularmente grave en el sector financiero, puesto que la precisión en la detección de fraudes en lo que concierne a la protección de los activos y mantener la confianza de los clientes (Departamento del Tesoro de EE. UU., 2024). Además, la manipulación de datos puede afectar, de manera vital, la integridad de los modelos

de IA, provocando que las decisiones automatizadas sean menos fiables y potencialmente perjudiciales. Este tipo de ataque subraya la importancia de implementar técnicas robustas de validación y monitoreo de datos con la finalidad de propiciar la identificación y reducción de posibles manipulaciones antes de que impacten negativamente en los modelos de IA.

11.2. Ataques de Evasión

En los ataques de evasión, denominados también como *evasion attacks*, los agresores diseñan entradas específicas que los modelos de IA interpretan de manera incorrecta, lo que permite que las actividades maliciosas pasen desapercibidas (GAO, 2024). Estos ataques explotan las vulnerabilidades en los algoritmos de IA dado que presentan datos diseñados para engañar al modelo y evadir su detección. En este sentido, pequeñas perturbaciones en los datos de entrada pueden llevar a que un modelo de IA clasifique de manera errónea, permitiendo a los atacantes evadir la detección (Goodfellow et al., 2014).

Con respecto a sus implicancias, se debe decir que este tipo de ataques pueden hacer que los sistemas de detección de fraudes no identifiquen actividades sospechosas, permitiendo que los fraudes se ejecuten sin ser detectados. Esta circunstancia representa un desafío significativo para el ciberpatrullaje, puesto que compromete la capacidad que poseen los sistemas de IA para prevenir delitos financieros (NIST, 2024). A su vez, los ataques de evasión pueden debilitar y perjudicar la confianza en los sistemas de detección automatizada, lo que provocaría una dependencia excesiva de la intervención humana, reduciendo la eficiencia del sistema. Para lograr reducir este riesgo, es fundamental desarrollar modelos de IA que sean robustos a perturbaciones adversas y que puedan detectar intentos de evasión mediante técnicas avanzadas de aprendizaje automático y monitoreo continuo.

11.3. Exfiltración de Datos

La exfiltración de datos ocurre cuando los atacantes roban datos sensibles procesados por los modelos de IA, explotando vulnerabilidades en el sistema (NIST, 2024). La exfiltración es un concepto utilizado, sobre todo, en el ámbito militar, y describe el proceso de salir de un área específica, típicamente un territorio enemigo, en contraposición a la infiltración, que

implica entrar en dicha área. Este tipo de ataque puede implicar el seguimiento de datos durante su transmisión, la explotación de vulnerabilidades en las bases de datos o la utilización de accesos no autorizados.

En lo que respecta a sus intervenciones, se debe mencionar que la exfiltración de datos compromete la información valiosa y sensible, lo que puede ocasionar graves y considerables consecuencias para la seguridad y privacidad de las instituciones financieras y sus clientes. La protección de datos es esencial para mantener la confianza del público y la integridad de los sistemas financieros. Además, la pérdida de datos puede resultar en la imposición de sanciones regulatorias, daños en la reputación y pérdidas financieras significativas (NIST, 2024). La implementación de técnicas de cifrado de extremo a extremo, controles de acceso estrictos y auditorías de seguridad regulares son cruciales y valiosos en lo concerniente a la protección de los datos contra exfiltraciones.

11.4. Estrategias de Mitigación

11.4.1. Fortalecimiento de la Seguridad de los Datos

La implementación de medidas robustas para asegurar la integridad de los datos utilizados por los modelos de IA es determinante. Esto incluye la validación y verificación continua de los datos de entrenamiento y operación (Departamento del Tesoro de EE.UU., 2024). En este sentido, las técnicas de seguridad y garantía de datos pueden incluir la detección de anomalías, la auditoría de datos y la implementación de controles de acceso estrictos (NIST, 2024).

En lo que respecta a su aplicación en el ciberpatrullaje, dicha medida es esencial para garantizar la calidad y la integridad de los datos, a fin de mantener la precisión y fiabilidad de los sistemas de ciberpatrullaje. Por estos motivos, se deben implementar filtros y mecanismos de control para detectar y eliminar datos anómalos o manipulados. Esto asegura que los modelos de IA funcionen con datos precisos y fiables, mejorando su efectividad en la detección de fraudes. También, la implementación de técnicas de cifrado y anonimización de datos puede proteger la información sensible durante su procesamiento y almacenamiento. Se puede agregar, que la

anonimización de datos consiste en un proceso que implica la eliminación de información de identificación personal de conjuntos de datos, de modo que las personas que describen los datos permanecen en el anonimato. Las técnicas de *hash* (convierte uno o varios elementos de entrada a una función en otro elemento) y *checksum* (herramienta de redundancia diseñada para identificar modificaciones no intencionales en una serie de datos, con el fin de salvaguardar su integridad), pueden ser utilizadas para verificar la integridad de los datos, asegurando que no hayan sido alterados de manera maliciosa (NIST, 2024).

11.5. Detección y Respuesta Rápida

Es sumamente importante, establecer sistemas avanzados de monitoreo que utilicen IA para detectar anomalías en tiempo real y responder rápidamente a cualquier indicio de compromiso (Gov.UK, 2024). Estos sistemas deben ser capaces de analizar grandes volúmenes de datos en tiempo real, identificando patrones sospechosos y alertando a los operadores humanos cuando se detecten amenazas potenciales.

En relación con la aplicación en el ciberpatrullaje, la capacidad de detectar y reaccionar a las amenazas de manera oportuna es fundamental para el éxito del ciberpatrullaje. EN consecuencia, se deben implementar sistemas de alerta temprana y protocolos de respuesta automatizados para mitigar las amenazas antes de que causen daños significativos. Esto permite a las instituciones financieras reaccionar rápidamente a los incidentes, minimizando el impacto de los fraudes.

Además, los sistemas de respuesta rápida deben incluir capacidades de aprendizaje automático que mejoren continuamente su precisión y efectividad a medida que se enfrentan a nuevas amenazas. Se debe destacar, que la implementación de sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) basados en IA pueden aumentar significativamente la capacidad de una organización para responder a amenazas en tiempo real (Gov.UK, 2024).

11.6. Colaboración y Difusión de Información

Es imprescindible que se genere y aliente una activa promoción de la colaboración entre instituciones financieras y la difusión de información sobre ciber amenazas (National Institute of Standards and Technology, 2024). La colaboración interinstitucional puede incluir el intercambio de inteligencia sobre amenazas, la coordinación de respuestas a incidentes y la participación en ejercicios de ciberseguridad conjuntos.

En cuanto a la aplicación en el ciberpatrullaje, la colaboración impulsa y profundiza sustancialmente la detección de fraudes al posibilitar una visión más amplia y detallada de las amenazas, facilitando, de esa manera, respuestas coordinadas y efectivas. Asimismo, las alianzas estratégicas entre agencias gubernamentales y privadas pueden fortalecer las defensas cibernéticas al compartir inteligencia y recursos.

Se debe resaltar, que la información compartida puede incluir detalles sobre nuevas tácticas de ataque, vulnerabilidades identificadas y estrategias de mitigación efectivas. Además, la creación de plataformas de información compartida puede ayudar a las instituciones más pequeñas a beneficiarse de las experiencias y conocimientos de organizaciones más grandes y mejor equipadas (NIST, 2024). La colaboración también puede incluir el uso de plataformas seguras para el intercambio de información, garantizando que los datos sensibles se compartan de manera segura y eficiente.

11.7. Beneficios y Consideraciones de Conductas Propicias

Es fundamental alcanzar la eficiencia y la precisión, dado que la implementación de IA en la detección de fraudes permite procesar grandes volúmenes de datos en tiempo real, mejorando la capacidad de respuesta y la exactitud en la identificación de amenazas. Esto es crucial para la prevención de fraudes en el sector financiero, donde la rapidez y la precisión son esenciales para proteger los activos de los clientes y la integridad del sistema financiero (NIST, 2024). La automatización de la detección de fraudes no solo reduce el tiempo de respuesta, sino que también libera recursos humanos para tareas considerablemente estratégicas (Departamento del Tesoro de EE. UU., 2024). Se debe indicar, que la capacidad de analizar patrones complejos

de datos en tiempo real permite a las instituciones financieras detectar actividades sospechosas con anterioridad a que se conviertan en problemas más profundos.

Con respecto a las consideraciones éticas de esta cuestión, se debe mencionar, que es fundamental abordar los posibles sesgos en los modelos de IA con el objetivo de garantizar la transparencia y privacidad en el uso de los datos. Las políticas deben asegurar que los derechos de los clientes sean protegidos y que la tecnología se utilice de manera ética (Departamento del Tesoro de EE. UU., 2024). Esto incluye la implementación de auditorías regulares y la adopción de marcos de gobernanza para la IA que promuevan el uso responsable y ético de la tecnología.

Además, se deben considerar los impactos sociales y económicos de la IA, garantizando que su implementación no perpetúe desigualdades ni discrimine a grupos vulnerables. De esta manera, la transparencia en los algoritmos y la capacidad de un modelo para ser entendido y explicado de manera clara y comprensible son esenciales para asegurar que las decisiones automatizadas sean comprensibles y justificables (NIST, 2024).

11.8. Ejemplos de Aplicaciones Específicas en Ciberpatrullaje

11.8.1. Detección de Fraude en Transacciones

Es fundamental atender a la cuestión del empleo de algoritmos de aprendizaje automático para analizar patrones de comportamiento y datos de transacciones, identificando actividades sospechosas (Departamento del Tesoro de EE. UU., 2024). Estos algoritmos pueden aprender de datos históricos con la finalidad de identificar transacciones que se desvían de los patrones normales y señalar posibles fraudes.

Con respecto a su aplicación, se debe indicar que las instituciones pueden detectar y bloquear transacciones fraudulentas en tiempo real, mejorando la seguridad y reduciendo las pérdidas financieras. Esto se logra mediante el análisis continuo de las transacciones con la intención de buscar patrones anómalos que puedan indicar actividad fraudulenta. Por otra parte, los sistemas de detección pueden ser entrenados para adaptarse a nuevos tipos de fraude, mejorando, de manera constante, su capacidad para identificar actividades sospechosas (NIST, 2024). Las técnicas de aprendizaje profundo y redes neuronales pueden ser particularmente efectivas para detectar patrones complejos y no lineales en los datos transaccionales.

11.9. Análisis de Redes de Transacciones

Se debe garantizar un efectivo mapeo de las transacciones entre múltiples cuentas utilizando IA para propiciar la identificación de esquemas complejos de lavado de dinero (GAO, 2024). Este enfoque implica el análisis de grandes volúmenes de datos transaccionales para localizar patrones de comportamiento que sugieren una actividad ilícita.

En cuanto a la aplicación, la IA puede detectar transferencias repetitivas entre cuentas que sugieren actividades ilícitas, permitiendo a las autoridades intervenir antes de que se completen las operaciones fraudulentas. Este análisis avanzado de redes de transacciones permite una identificación más certera de actividades sospechosas, facilitando la intervención temprana. Asimismo, el uso de técnicas de visualización de datos puede ayudar a los analistas humanos a comprender mejor las relaciones complejas entre diferentes transacciones y cuentas (NIST, 2024). Se debe indicar, que las herramientas de análisis de las redes pueden utilizar algoritmos de detección de comunidades y análisis de grafos para identificar estructuras y patrones ocultos en las transacciones.

11.10. Detección de Anomalías y Comportamiento

La implementación de perfiles de comportamiento normal para usuarios y transacciones, y utilizar técnicas de detección de anomalías para identificar desviaciones sustanciales es una cuestión que debe tenerse en consideración de manera significativa (NIST, 2024). Debe indicarse, que los sistemas de detección de anomalías pueden utilizar el aprendizaje no supervisado para identificar comportamientos atípicos que podrían indicar fraude.

Con respecto a su aplicación, es fundamental señalar que la identificación de cambios abruptos en el tamaño y en la frecuencia de las transacciones, representa aquello que puede activar alertas de fraude y permitir una respuesta rápida. La detección de anomalías es una herramienta poderosa para generar las condiciones necesarias para poder identificar actividades inusuales que pueden indicar intentos de fraude o actividades ilícitas. Además, estos sistemas pueden ser ajustados para reducir los falsos positivos, mejorando así su eficacia y reduciendo las

interrupciones innecesarias en las operaciones legítimas (NIST, 2024). Se debe mencionar, que las técnicas de *clustering* (técnica de aprendizaje no supervisado en la que se agrupan datos similares entre sí en conjuntos distintos) y análisis de series temporales pueden ser utilizadas para identificar patrones inusuales en los datos transaccionales.

Como se pudo advertir, este apartado proporciona un fundamento sólido para la integración de tecnologías de IA en las estrategias de ciberpatrullaje, distinguiendo tanto las oportunidades como los desafíos que conlleva su implementación y desarrollo. De este modo, la identificación y mitigación de riesgos específicos de la IA son esenciales para fortalecer la ciberseguridad y proteger el sector financiero contra fraudes y otras amenazas cibernéticas.

Capítulo 12 - Ética de la IA en la Aplicación de la Ley

El informe desarrollado conjuntamente por el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (United Nation Interregional Crime and Justice Research Institute, UNICRI) e INTERPOL en el año 2020, prioriza y enfatiza la importancia crítica que supone la implementación y uso de la IA de manera ética y responsable dentro de las operaciones de aplicación de la ley. Las conclusiones del informe acentúan la necesidad de desarrollar una serie de marcos legales y directrices éticas que aseguren el respeto por los derechos humanos y los principios fundamentales de legalidad, transparencia y justicia en la adopción de tecnologías de IA.

El documento advierta acerca de la importancia de comprender que mientras la IA tenga el potencial de mejorar, de manera significativa, la eficiencia y la efectividad de las operaciones policiales, es fundamental que su implementación sea gestionada, de manera minuciosa, para prevenir riesgos asociados con violaciones de privacidad y posibles abusos de poder. Es imperioso recomendar la creación de un foro global para el intercambio de experiencias y mejores prácticas en el uso de la IA, que, simultáneamente, fomente la colaboración interinstitucional y multidisciplinaria, algo esencial para abordar los desafíos emergentes y garantizar, de este modo, una implementación tecnológica que refuerce la confianza pública en las autoridades que apliquen y supervisen la ley (UNICRI & INTERPOL, 2020).

El empleo intensivo de la IA y el *big data* en el ámbito de la administración de justicia y de las actividades de ciberpatrullaje, aporta beneficios significativos, pero, también, plantea complejidades con respecto a los derechos fundamentales de la sociedad. La implementación de estas tecnologías en el proceso penal y en la seguridad pública exige un delicado equilibrio entre la eficacia y la ética. Para asegurar este hecho, es crucial garantizar la transparencia y la adecuada regulación legal para mitigar los riesgos de abusos y violaciones de los derechos (Martín Ríos, 2022).

La práctica del ciberpatrullaje, concretamente a través del análisis de fuentes abiertas (OSINT) y de medios sociales (SOCMINT), es efectiva para identificar actividades delictivas en línea, pero puede conducir a excesos si no se controla de manera adecuada y oportuna. En

este sentido, resulta indispensable establecer límites y procedimientos manifiestos y evidentes con respecto a la utilización de estas técnicas, asegurando el respeto de los principios de proporcionalidad y necesidad.

Además, la automatización en la toma de decisiones, una característica particular de la IA puede conducir a una "tiranía del algoritmo", en la cual decisiones cruciales que afectan a los derechos individuales se encuentran basadas y sustentadas en fórmulas matemáticas desligadas de la necesaria y conveniente supervisión humana. Para Martín Ríos (2022), esta cuestión recalca la necesidad de un marco normativo robusto que incluya protecciones y garantías que contribuyan para prevenir la discriminación y garantizar que las decisiones automatizadas sean justas, precisas y verificables.

En definitiva, la práctica de técnicas de inteligencia implica que los Estados se muestran renuentes a proporcionar información acerca del empleo de este tipo de tecnologías de vigilancia. En este sentido, los casos de espionaje estatal ilegal se han multiplicado en la región, e involucran generalmente a disidentes políticos, defensores de derechos humanos, manifestantes, así como miembros de organizaciones sindicales y periodistas. De todos modos, estas técnicas de inteligencia, como OSINT, utilicen, por definición, fuentes "abiertas", no significa que su práctica no pueda ser una práctica ilícita del derecho a la privacidad (Schatzky y Zara, 2023, p. 3).

La práctica de técnicas de inteligencia, como es el caso de OSINT, por parte del Estado y sin una sujeción a reglamentaciones específicas o ceñidas a una normalización general, "tiene implicancias negativas en derechos humanos, principalmente en lo que respecta a privacidad y libertad de expresión" (Schatzky y Zara, 2023, p. 32). De esta manera, la actividad de OSINT por parte del Estado debe ser reglamentada legalmente, de acuerdo con criterios respetuosos de los derechos humanos.

Se debe señalar, que existe cierta opacidad en la manera en la que la administración pública lleva a cabo la inteligencia de fuentes abiertas sobre su población. Esta situación, impide el correcto de la actividad en varios aspectos. Por un lado, la naturaleza de la actividad y sus potenciales afectaciones en derechos humanos requerirían la puesta en funcionamiento de un sistema de rendición de cuentas mediante el cual el Estado reporte periódicamente la actividad

OSINT que lleva adelante (Schatzky y Zara, 2023, p. 32). Por otro lado, admitir que el Estado participa en actividades de este carácter facilitaría la imposición de una serie de obligaciones que podrían propiciar la transparencia en relación al compromiso con terceros de funciones emparentadas con dicha actividad. De esta manera, la práctica de este tipo de inteligencia, si se mantiene fuera de las normativas, implica que se lleven a cabo desde la informalidad, sin profesionales especializados en el tema.

En resumen, la integración de la IA y el *big data* en el ciberpatrullaje y la administración de justicia, debe proceder con cautela. Esta inclusión debe priorizar de manera constante la protección de los derechos fundamentales y la integridad de los procesos judiciales y policiales. Para solucionar estos inconvenientes, es imprescindible "predecir comportamientos en un área establecida, en unas condiciones ambientales dadas, con una mayor o menor visibilidad o afluencia de personas" (Martín Ríos, 2022, p. 5). La utilidad de técnicas de este tipo, es decir, predictivas, se transformará de acuerdo con el delito que se analice, sin embargo, alcanza con tener los datos necesarios para que el respectivo algoritmo genere la información acerca de la probabilidad de que una conducta determinada se lleve a cabo, como un simple reflejo estadístico. De este modo, resulta indispensable que tanto las autoridades policiales como las judiciales "puedan siempre separarse de esa interpretación, evitando las consecuencias potencialmente graves que derivan de la tiranía del algoritmo" (Martín Ríos, 2022, p. 5).

Teniendo en cuenta lo desarrollado hasta aquí, es importante focalizar sobre el perfeccionamiento y el aprovechamiento de la IA en lo que respecta a su capacidad de adaptación y resistencia de la seguridad. Las soluciones a los crecientes ataques son aplicaciones de IA enfocadas y dirigidas con una finalidad específica. Los organismos estatales y las empresas especializadas deben actuar con rapidez, pero también con prudencia (Steele, 2024). El objetivo de esto es llevar a cabo políticas y, de esa manera, aplicar soluciones y metodologías impulsadas por IA para robustecer la eficacia de sus equipos de seguridad para hacer frente a los posibles ataques. Las últimas investigaciones han arrojado datos certeros y preocupantes: el 35 % informó que ya están experimentando con IA para la ciberdefensa, incluido el análisis de *malware*, la automatización del flujo de trabajo y la puntuación de riesgos (Steele, 2024).

La IA transformará la manera y los procedimientos en que las organizaciones más grandes y complejas del mundo amparan y protegen sus sistemas digitales seguros y confiables. En los próximos años, a partir del acelerado avance de la tecnología, la IA aportará un enorme valor al detectar anomalías de forma automática, empleando los modelos predictivos para, de ese modo, suministrar modos superiores para que las herramientas utilizadas en seguridad obtengan datos, hallen patrones y distingan las amenazas posibles.

Ahora bien, es esencial profundizar sobre la responsabilidad ética en esta materia. Existe una gran cantidad de oportunidades para que las industrias y los gobiernos de todo el mundo integren la IA en sus sistemas y servicios para mejorar los resultados e impulsar el progreso. Los líderes en esta materia deben pensar racionalmente si existe una abundancia equivalente de estrategia y responsabilidad, dado que el uso responsable y ético de la IA es primordial y eso comienza con la transparencia estatal y también empresarial. Una posible solución es la utilización de programas como *Splunk*, un software para buscar, monitorizar y analizar macrodatos generados por máquinas de aplicaciones, sistemas e infraestructura de la tecnología de la información a través de una interfaz web. El empleo de software como estos, "implicaría que los sistemas de IA y el uso de datos deben ser explicables, transparentes y comprensibles para nuestros clientes y partes interesadas" (Steele, 2024). Asimismo, los sistemas de IA, por diseño, deben ser imparciales y respetuosos de los datos personales y organizacionales.

Debe indicarse que, al mismo tiempo, la utilización de estos programas tiene que ser adecuada y responsable para resolver un conjunto de problemas específicos, a saber: distinguir el empleo del aprendizaje automático para mejorar la capacidad de detectar problemas potenciales y, de esa manera, brindar la adecuada asistencia para solucionarlos. En definitiva, esta sería una utilidad rápida y valiosa de la tecnología. Para lograr que la IA tenga un efecto realmente significativo y positivo, es crucial ser claros, objetivos y, sobre todo, responsables acerca de dónde puede ser aplicada esta tecnología para impulsar un mundo digital más resistente y moralmente transparente.

12.1. Reglamentación de la IA en el Mundo

En el contexto del progreso irrefrenable de la IA a nivel mundial, la UE ha realizado el proyecto de la Ley de Inteligencia Artificial (*Artificial Intelligence Act*, *AI Act*), que fue propuesto por la Comisión Europea en 2021. Es un reglamento para el uso correcto de la IA, que actualmente se encuentra en proceso de aprobación, es decir, aún no ha entrado en vigor. Su propósito es establecer un marco normativo unificado para regular los sistemas de IA en la Unión Europea. Esta iniciativa representa la primera ley de su tipo a escala internacional y pretende abordar los riesgos potenciales para la seguridad y los derechos fundamentales de los ciudadanos de la UE.

La *AI Act* de la UE establece un marco regulador para el uso responsable de la IA, especialmente en lo que respecta a aplicaciones de alto riesgo como es el caso del ciberpatrullaje. Asimismo, la ley impone estrictos requisitos de transparencia, supervisión humana y protección de datos personales y, al mismo tiempo, prohíbe el uso de sistemas de identificación biométrica remota en tiempo real en espacios públicos, con el objetivo de eludir la vigilancia masiva y proteger los derechos fundamentales de los ciudadanos. Se debe destacar, que están exceptas de excepción si se realizan a partir de una autorización judicial.

La *AI Act* requiere que los proveedores y los encargados de ejecutar el despliegue de los sistemas de IA, cumplan con ciertas obligaciones, específicamente, la documentación técnica y la conservación de registros, para asegurar la trazabilidad y responsabilidad de estos sistemas. Estas medidas son esenciales para garantizar que los sistemas de ciberpatrullaje operen de manera ética y legal, minimizando los riesgos de discriminación y violaciones de privacidad.

Por otra parte, la ley promueve el desarrollo y la instauración de la innovación y el desarrollo responsable de tecnologías de IA, respaldando y contribuyendo a la expansión de las pequeñas y medianas empresas (pymes) y *startups* (empresa emergente, normalmente fundada por un emprendedor, sobre una base tecnológica e innovadora). Este enfoque equilibrado intenta fomentar el avance tecnológico paralelamente a la salvaguarda de los derechos fundamentales y asegurar la seguridad pública.

Se cree sustancial, teniendo en consideración todo lo expresado hasta aquí, relevar y analizar el tema de la IA en Argentina, sus orígenes, su presente y los marcos normativos que se

han pensado y establecido para poder regular esta tecnología que se desarrolla con una celeridad notable.

12.2. Orígenes y Normativas de la IA en Argentina

Una de las primeras iniciativas sobre IA en Argentina fue elaborada entre los años 2018-2019, denominada como "Plan Nacional de Inteligencia Artificial". A pesar del título del proyecto, se trató de un informe sobre IA, una descripción general, pero que carecía de los matices que tendría que poseer una política pública sobre IA en el país. El informe se focalizó, entre otras cosas, "en la necesidad de formar Recursos Humanos (a los que denomina talentos), la importancia del uso de los datos (públicos más que privados), la infraestructura computacional y la ética y las regulaciones" (Vercelli, 2024, p. 111). Con respecto a esto último, se debe decir que el informe distingue que las regulaciones públicas sobre las IA y su desconocimiento podrían funcionar como una barrera para llegar a una innovación eficiente. A finales de 2019, con la llegada de un nuevo gobierno, el informe fue rápidamente descartado.

A partir de 2020, a través de la Secretaría de Innovación Pública dependiente de la Jefatura de Gabinete de Ministros (JGM) se creó el servicio de *chatbot* del Estado, "basado en un programa de IA, que pueda automatizar tareas simulando conversaciones con los usuarios en lenguaje natural y a través de sitios web, aplicaciones móviles o por teléfono móvil" Vercelli, 2024, p. 115). Este instrumento, por sus peculiaridades conversacionales, se encuentra dirigido a propiciar y beneficiar las comunicaciones con los ciudadanos las 24 h del día, y, además, a pretender crear una experiencia personalizada a partir de la aplicación "Mi Argentina", una herramienta de asistencia virtual en la que el ciudadano podía gestionar trámites, sacar turnos, acceder a sus credenciales y recibir información personalizada. De acuerdo con el artículo 1 de la Resolución 14/2022, se renombró al *chatbot* como TINA, el "Chatbot del Estado Nacional". Al mismo tiempo, TINA se acopló al Perfil Digital del Ciudadano "Mi Argentina". Para su correcta operatividad, se determinó un número oficial y verificado en la aplicación *WhatsApp* (1139101010). Asimismo, la resolución mencionada asegura que el *chatbot* está disponible en los portales web del Estado, y exhorta a provincias y municipios a incorporarse al servicio.

Es importante destacar, también, que en la Ciudad Autónoma de Buenos Aires, a partir de 2017, se implementó sistema de asistencia virtual para la redacción de documentos judiciales. Dentro del contexto de las investigaciones sobre tecnologías disruptivas que están revolucionando organizaciones globalmente, surgió PROMETEA, una IA desarrollada en Argentina en el ámbito del Ministerio Público Fiscal de CABA. Inicialmente, el sistema fue diseñado para mejorar el servicio de justicia y acelerar significativamente los procesos judiciales. Sin embargo, se descubrió que los beneficios que ofrecía podrían ser utilizados por cualquier organización pública. El desarrollo de esta IA "tuvo sus inicios en agosto de 2017, y a partir de esa fecha, ha sido presentada en numerosas instituciones nacionales e internacionales" (Ministerio Público Fiscal de CABA, 2021).

Además, PROMETEA ha sido destacada en la publicación N° 31 de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Gobernanza Pública. También ha recibido reconocimiento de dos destacados líderes de organismos internacionales: Vincenzo Aquaro, Director de Gobierno Digital de la Organización de las Naciones Unidas (ONU), y Ekkehard Ernst, Jefe de Investigación de Políticas Macroeconómicas y Unidades de Trabajo de la Organización Internacional del Trabajo (OIT).

Actualmente, PROMETEA está operativa en varias instituciones, tanto en la Ciudad de Buenos Aires como en otras provincias del país, como Mendoza, Chaco, Corrientes y Santa Fe. Tras seis años de trabajo continuo, podemos afirmar que PROMETEA se ha establecido como una política pública federal en la gestión e integración de tecnología y derecho.

Se debe indicar, que PROMETEA se caracteriza por tres grandes aspectos:

> I) Posee una interfaz intuitiva y amigable que permite "hablarle" al sistema o chatear a partir de un reconocedor de lenguaje natural; II) Opera como sistema experto con multiplicidad de funciones, que permite automatizar datos y documentos y realizar asistencia inteligente; III) Utiliza técnicas de *machine learning* supervisado y de *clustering*, a partir de etiquetado manual y de máquina con *dataset* de entrenamiento, a efectos de realizar predicciones y/o detecciones en grandes volúmenes de documentación.

Según las evaluaciones realizadas en casos reales, PROMETEA ha demostrado que los tiempos de ejecución de las tareas pueden reducirse hasta un 90 %, además de disminuir, e incluso eliminar en algunos casos, el margen de error.

Con respecto a su eficiencia, se debe indicar que PROMETEA:

- Predice la solución a un caso judicial en menos de 20 segundos, con una tasa de acierto igual o superior del 90 %;
- Permite realizar un pliego de bases y condiciones particulares e incorpora una herramienta de control de precios públicos y privados sobre los bienes a adquirir, reduciendo los tiempos en la confección de un pliego de dos horas a tan solo un minuto;
- Contrasta datos entre documentos y base de datos sin intervención humana, y logra reducir tiempos de trece horas a cinco minutos;
- Segmenta informes en función de su contenido en investigaciones de abuso sexual infantil. Esta tarea que puede demandar 8 horas por día a una persona, PROMETEA logra hacerla en pocos segundos;
- Elabora un decreto de determinación de los hechos de manera automática, lo que reduce el tiempo de confección de veinticinco minutos a tan solo dos;
- Elabora una base de datos de manera automática a partir de la extracción de datos de la documentación;
- Elabora dictámenes y disposiciones por rectificatorias administrativa de partidas, y logra reducir los tiempos de confección hasta un 70 %;
- Redujo los tiempos de elaboración de despachos y sentencias hasta en un 80 %, en oficinas judiciales de las provincias de Corrientes y Chaco;
- Con relación a todas las implementaciones, se concluyó que PROMETEA reduce la cantidad de errores de tipeo en un 99 %; y permite hacer un control exhaustivo de aspectos formales de los documentos involucrados. (Ministerio Público Fiscal de CABA, 2021)

A su vez, entre otros proyectos que el Estado planificó para establecer directrices sobre el tema de la IA, se encuentra la creación en 2022 del Centro Argentino Multidisciplinario de

Inteligencia Artificial (CAMIA). Ese mismo año, y previamente al crédito otorgado por el Banco Interamericano de Desarrollo (BID), "se realizó un segundo evento llamado «Foro Internacional de Inteligencia Artificial: hacia un Centro Argentino Multidisciplinario de Inteligencia Artificial», con la intención de discutir algo más sobre la arquitectura institucional que tendría CAMIA" (Vercelli, 2024, p. 113). Específicamente, este diseño tiene la intención de: (a) promover una participación de los actores públicos y privados del ecosistema de IA; (b) generar mecanismos para la identificación y priorización de necesidades de formación, de investigación aplicada y de servicios a las empresas; (c) promover la transferencia tecnológica al sector productivo; y (d) garantizar la sustentabilidad financiera de mediano y largo plazo del centro. Se debe indicar que hasta la fecha la propuesta de CAMIA aún no ha publicado ningún tipo de informe sobre la IA en el país.

Se debe agregar que en 2023 la JGM, por medio de la Decisión Administrativa 750/2023, se crea la Mesa Interministerial sobre Inteligencia Artificial (MIIA). El propósito de este órgano es el de establecer un marco ético, del desarrollo sostenible y de la transformación digital en el Estado, con el objetivo de abordar los avances de la IA en los diversos sectores socioeconómicos y ayudar en el diseño de una estrategia integral sobre IA. De este modo, actualmente en Argentina, tanto las políticas públicas como las regulaciones sobre IA, "pueden caracterizarse como «inerciales» (imitan y acompañan las soluciones que otros países/regiones proponen), «fragmentadas» (tratan temas sueltos, dispersos o específicos) y de escasos resultados" (Vercelli, 2024, p. 128). Con excepción de algunos hechos puntuales, como es el caso de las políticas de defensa y ciberseguridad o, también, como la conformación de la mencionada MIIA, el esquema general exhibe una ausencia total de una estrategia nacional sobre la IA en el país. Esta ausencia podría generar la pérdida de recursos y a discusiones insignificantes o que aplacen el desarrollo eficiente de esta tecnología. En este sentido, es primordial que en Argentina se discutan políticos de implementación de un diseño estratégico sobre IA resguardando la soberanía tecnológica según los intereses particulares del país.

Teniendo en cuenta lo relevado hasta aquí, es importante mencionar que, ante la situación del país, si bien la IA está generando grandes avances y beneficios en materia laboral y tecnológica, también podrían llegar a profundizar y reactivar problemas precedentes como es el

caso de la desigualdad y el desempleo. El riesgo subyacente que podría acarrear la IA podría ser la generación de un cierto desorden social y una posterior crisis política debido al desempleo generalizado y a la enorme desigualdad que podría generar esta tecnología. El crecimiento del uso de la IA en la industria anticipa una claro incomodidad en la cultura tecnológica que emerge, como mínimo, de tres nociones: "el desconocimiento sobre qué cantidad, calidad y funciones tienen estos dispositivos a nivel mundial, su falta de transparencia (imposible arribar a una explicabilidad) y, finalmente, la complejidad creciente y una fuerte dependencia de las IA" (Vercelli, 2024, p. 109). En resumen, se debe atender esta problemática, dado que el incremento en el empleo de IA en el sector industrial podría provocar cierto malestar en la sociedad y este disgusto podría acarrear consecuencias graves en la sociedad y en la política.

12.3. Relevamiento de las Políticas de Estado y las Regulaciones con respecto a la IA

Es de amplio conocimiento que en los últimos años el Estado ha reconocido reconoce que, a nivel global, existe un auge en el desarrollo y en la implementación de proyectos que involucren IA. Por este motivo, se sancionó en 2023 la Disposición 2/2023 sobre "Recomendaciones para el uso de Inteligencia Artificial". En las "Consideraciones preliminares", la normativa reconoce que la irrupción de la IA, expresada en la creciente trascendencia de los datos y algoritmos en la vida de las personas, "empuja a los Estados a definir estrategias para encauzar el potencial transformador de esta tecnología en la resolución de problemas concretos y a favor del bien común".

En este sentido, según esta Disposición, se reconoce que las soluciones tecnológicas basadas en IA permiten mayores niveles de automatización, así como un gran salto hacia sistemas descentralizados y predictivos para la toma de decisiones, que podrían mejorar el diseño, implementación y evaluación de políticas. Por estos motivos, la normativa admite la necesidad de establecer reglas claras para asegurar que los progresos de los desarrollos tecnológicos puedan ser aprovechadas por todos los sectores de la sociedad y, al mismo tiempo, puedan fomentar e impulsar la coyuntura científico y tecnológico del país, para, de esa manera,

"fortalecer las capacidades de innovación, desarrollo y la producción de soluciones tecnológicas".

Si bien la Disposición no establece líneas rígidas y contundentes sobre políticas sobre IA, tiene la intención de proponer herramientas teóricas y prácticas a aquellos que formen parte del sector público, con la finalidad de liderar proyectos de innovación, desarrollar tecnologías, entre otras cuestiones.

Con respecto a la seguridad y protección, la Disposición indica que los sistemas que utilicen IA "deben ser robustos, seguros y protegidos a lo largo de todo su ciclo de vida para que, en condiciones de uso normal, uso previsible o uso indebido, u otras condiciones adversas, funcionen adecuadamente y no planteen riesgos de seguridad irrazonables". De este modo, aquellos que detenten esta tecnología deben asegurar la trazabilidad en relación con los conjuntos de datos, los procesos y las decisiones tomadas con el sistema de IA. Además, estos deben aplicar "un enfoque sistemático de gestión de riesgos a cada fase del ciclo de vida del sistema de IA de forma continua para abordar los riesgos relacionados, incluida la privacidad, la seguridad digital, la seguridad y la parcialidad".

En cuanto a cómo establecer un grado adecuado de seguridad de la información, la normativa indica que es fundamental que se realicen mejores prácticas concernientes a la seguridad de la información. Para este motivo, los responsables de la seguridad de la información deberán seguir ciertos lineamientos:

a) El relevamiento, conocimiento y comprensión del alcance de los estándares y normativas internacionales, y mejores prácticas en materia de seguridad de la información.
b) El relevamiento, conocimiento y comprensión de la normativa vigente en materia de seguridad de la información.
c) La utilización de aplicaciones accesorias encargadas de gestionar los registros (logueos, eventos, etc.) de los sistemas involucrados de manera tal de facilitar el tratamiento de eventuales incidentes de seguridad; automatizar la creación de informes de auditoría; y mejorar la transparencia a través del control de las personas que acceden a los sistemas, de las aplicaciones y de los equipos.

d) La realización de diferentes tests para hallar vulnerabilidades de seguridad que pudieran ocasionar eventuales incidentes no deseados.
e) La participación del área o de la autoridad con responsabilidad primaria en materia de seguridad de la información, que entiende en todos los aspectos relativos a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática. Esto es particularmente importante en el caso de que la institución adoptante del desarrollo basado en IA no disponga de un área específica de seguridad de la información. (Disposición 2/2023)

Ahora bien, la normativa indica que las tecnologías de IA son muy versátiles y, por ende, posibilitan una amplia gama de destinos de sus usos. De este modo, cada uno de esos destinos de uso implica diversos riesgos, que, a su vez, conlleva diferentes niveles de procesamiento de esos riesgos. La Disposición señala que "en algunas áreas esto resulta muy importante dado que ciertos destinos de uso, por ejemplo, en la ciberseguridad, pueden representar potenciales riesgos si su uso no es controlable, auditable y trazable". Estos riesgos pueden llegar a impactar de manera negativa y acarrear ciertos perjuicios manifiestos.

La Disposición plantea una serie de recomendaciones que se focalizan en la incorporación de fundamentos éticos transversales a toda la IA y, además, define, en cada etapa, los riesgos y responsabilidades que pueden suceder, "resaltando que la responsabilidad y supervisión deben recaer siempre en los seres humanos" (Martínez, 2023). Asimismo, pese a que las advertencias están orientadas al sector público, pueden ser tenidas en cuenta como instrucciones, no obligatorias, para el sector privado.

Asimismo, otra normativa que intenta profundizar sobre este tema: el "Programa Nacional de Transparencia y Protección de Datos Personales en el uso de la Inteligencia Artificial" sancionado en la Resolución 161/2023. Este Programa se ocupa de diferentes dimensiones estratégicas en lo referente a la implementación de proyectos de IA, a saber: "la sensibilización y la educación, la supervisión y la toma de decisiones humanas, y la responsabilidad y rendición de cuentas" (Martínez, 2023). Igualmente, se resalta la importancia

del respeto incondicional de los marcos jurídicos nacionales e internacionales vinculados con la privacidad y la protección de datos personales en el marco de la IA.

Esta Resolución tiene el objetivo de impulsar procesos que impliquen el análisis, la regulación y el fortalecimiento de las capacidades del Estado para asistir y complementar el desarrollo y uso de la IA en el sector público y en el privado. También, debe garantizar el ejercicio eficaz de los derechos de la población en lo que respecta a la transparencia y protección de los datos personales.

Se debe destacar, que esta normativa no plantea considerables contribuciones en referencia a la IA, sino que se centra en las cuestiones éticas, sobre todo apuntando a considerar a la ética en IA de una manera rígida. Para esta norma la ética en IA es:

> Una reflexión normativa sistemática, basada en un marco integral, global, multicultural y evolutivo de valores, principios y acciones interdependientes, que puede guiar a las sociedades a la hora de afrontar de manera responsable los efectos conocidos y desconocidos de las tecnologías de la IA en los seres humanos, las sociedades y el medio ambiente y los ecosistemas, ofreciendo una base para aceptar o rechazar las tecnologías de la IA. (Resolución 161/2023)

La mencionada normativa, manifiesta la necesidad de dotar de mayor seguridad y legitimidad a los sistemas de IA y, para ello, es imprescindible robustecer las capacidades institucionales del Estado, para propiciar las condiciones para incorporar la transparencia y la protección de datos personales como unas dimensiones significativas y transversales al diseño de proyectos de desarrollo tecnológico en materia de IA.

En definitiva, el objetivo de esta resolución es la creación del "Programa de transparencia y protección de datos personales en el uso de la Inteligencia Artificial", con la intención de promover y potenciar procesos de análisis, regulación y fortalecimiento de las capacidades del Estado para poder asistir y complementar el desarrollo y uso de la IA en el ámbito público y privado.

Para finalizar, es importante mencionar que la Agencia de Acceso a la Información Pública (AAIP), señala que un punto importante que tendrá este programa es la creación de un "Observatorio sobre inteligencia artificial", cuyas líneas de acción se ocuparán de: (a) el mapeo

de actores clave involucrados en la temática, tanto gubernamentales como no gubernamentales; (b) el seguimiento de avances regionales y globales en materia de regulación de los desarrollos tecnológicos basados en IA; (c) la elaboración de estadísticas e informes periódicos sobre la materia. Así también, el programa buscará fortalecer las capacidades en cuanto a la transparencia y protección de los datos personales en el uso de la IA, a partir de: (a) guías de buenas prácticas para entidades públicas y privadas en materia de transparencia y protección de datos personales en el uso de la IA; (b) capacitaciones y asistencia técnica en materia de transparencia y protección de datos personales en el uso de la IA; (c) campañas de sensibilización, alfabetización mediática e informacional; (e) documentación de los Sistemas de Decisiones Automatizados (SDA) y publicación de los criterios de transparencia en el Portal Nacional de Transparencia (AAIP, 2024).

Capítulo 13 - Consideraciones a Corto y Largo Plazo

Luego de analizar la normativa establecida en Argentina, es fundamental pensar cómo se sitúa el país en su realidad cotidiana, tanto social como económica, con respecto a la cuestión de la IA. De este modo, es imperioso plantear una serie de nuevas preguntas que tienen el propósito de convertirse en nuevas normativas relacionadas con la IA para prevenir el ciberdelito. Entre estas consideraciones a futuro se podrían mencionar:

- ¿Pueden las regulaciones de IA requerir que los algoritmos de ciberseguridad sean transparentes y comprensibles para los expertos y también para los usuarios cotidianos?
- ¿Deberían promulgarse normativas que exijan que las empresas utilicen sistemas de IA para detectar y prevenir ciberdelitos?
- ¿Deberían las empresas y organizaciones ser responsables legalmente por los fallos de los sistemas de IA en la prevención de los ciberdelitos?
- ¿Se deben establecer estándares mínimos de seguridad para los algoritmos de IA utilizados en la detección de amenazas informáticas?
- ¿Qué medidas de protección de datos deberían implementarse en los sistemas de IA utilizados para prevenir la ciberdelincuencia?
- ¿Deberían las normativas requerir que los desarrolladores de IA implementen protecciones para evitar la manipulación de los algoritmos por parte de los ciberdelincuentes?
- ¿Es necesario establecer una supervisión independiente por parte del Estado para garantizar la implementación de las normativas de IA en la prevención de los ciberdelitos?

En el contexto actual, es fundamental desarrollar estrategias y propuestas que permitan analizar los posibles riesgos asociados con la inteligencia artificial (IA) y establecer mecanismos para mitigar estos peligros. Dado el ritmo acelerado y los profundos cambios que la IA está imponiendo en diversos ámbitos, adoptar medidas preventivas se vuelve esencial para garantizar que el avance de esta tecnología sea ético y responsable.

Es crucial que los sistemas de IA sean diseñados con una transparencia que permita a los usuarios comprender el proceso mediante el cual se toman las decisiones. La "explicabilidad" de la IA debe ser una prioridad, de modo que el funcionamiento interno de estos sistemas y las razones detrás de sus conclusiones sean accesibles y comprensibles para los seres humanos, asegurando que la información proporcionada sea fiel a la realidad que intenta representar.

Además, es imperativo establecer normativas y marcos regulatorios basados en principios éticos sólidos. Estos marcos deben orientarse a evitar sesgos y discriminación, asegurando que la implementación de la IA respete los derechos humanos y promueva la equidad. La ética en el diseño y uso de la IA debe ser una guía constante para evitar que estos sistemas perpetúen desigualdades o injusticias.

Por su parte, la seguridad cibernética también juega un papel crucial en el desarrollo de la IA. Es necesario reforzar las medidas de protección para salvaguardar estos sistemas contra posibles ataques y garantizar la integridad, confidencialidad y disponibilidad de los datos. A medida que la IA se integra en más aspectos de la vida cotidiana, proteger la infraestructura subyacente de estos sistemas es esencial para evitar vulnerabilidades y preservar la confianza en la tecnología.

Por último, la protección de la privacidad y los datos personales debe ser una preocupación central. Implementar prácticas robustas para asegurar el consentimiento informado y el control por parte de los usuarios es esencial para proteger su privacidad. Los datos utilizados por los sistemas de IA deben ser gestionados con el máximo cuidado, respetando los derechos de los individuos y garantizando que la información personal esté protegida adecuadamente.

En resumen, para que el desarrollo de la inteligencia artificial sea ético y beneficioso, es fundamental abordar estos aspectos con seriedad y diligencia. Esto implica garantizar la transparencia y explicabilidad de los sistemas, establecer regulaciones éticas y equitativas, reforzar la seguridad cibernética, y proteger la privacidad de los datos. Al adoptar estas medidas, se puede facilitar un avance de la IA que sea seguro, justo y en alineación con los valores humanos fundamentales.

Particularmente en el caso de Argentina esta serie de prevenciones adquieren una relevancia específica, dada la creciente adopción de tecnologías de IA en diversos sectores. Argentina enfrenta desafíos en términos de regulación y aplicación de tecnologías emergentes, incluida la IA. Para abordar esta problemática el país podría considerar:

- Desarrollo de marcos regulatorios: Argentina debería trabajar e investigar acerca del desarrollo de marcos normativos específicos para la IA, con el objetivo de ocuparse de aspectos como la transparencia, la ética, la seguridad informática y la protección de datos.
- Capacitación y concientización: es sustancial la promoción de la capacitación y divulgación sobre los riesgos y los beneficios de la IA entre todos los actores, concretamente los desarrolladores, usuarios y reguladores, para fomentar un uso responsable de la IA.
- Colaboración internacional: el país debería buscar alianzas y trabajar en conjunto con otros países y organizaciones internacionales para compartir mejores prácticas y experiencias en la regulación y aplicación de la IA.
- Inversión en investigación: el Estado podría invertir en investigación y desarrollo de tecnologías de IA, generando la posibilidad de potenciar la investigación en seguridad, ética y equidad.

En resumen, en el contexto de Argentina, las medidas preventivas para la adopción de tecnologías de inteligencia artificial (IA) se vuelven especialmente cruciales debido al creciente uso de estas tecnologías en diversos sectores. La nación enfrenta retos significativos en la regulación y gestión de estas innovaciones emergentes, lo que hace imprescindible desarrollar estrategias específicas para abordar estas cuestiones de manera efectiva. Primero, Argentina necesita avanzar en la creación de marcos regulatorios específicos para la IA. Esto implica elaborar normativas que aborden temas fundamentales como la transparencia en el uso de la tecnología, la ética en su aplicación, la seguridad informática y la protección de los datos personales. Establecer estas directrices permitirá un uso más seguro y justo de la IA, alineado con los estándares internacionales y las mejores prácticas.

Además, es esencial promover la capacitación y la concientización sobre la IA entre todos los involucrados. Esto incluye a desarrolladores, usuarios y reguladores. Una educación adecuada en torno a los riesgos y beneficios de la IA fomentará un uso más consciente y responsable de la tecnología, minimizando potenciales problemas y maximizando sus beneficios. Por otra parte, la colaboración internacional es otro aspecto clave. Argentina debería buscar formar alianzas y trabajar en conjunto con otros países y organizaciones internacionales. El intercambio de experiencias y mejores prácticas en la regulación y aplicación de la IA permitirá al país adoptar enfoques más efectivos y mantenerse al día con los avances globales en esta área. Finalmente, el Estado argentino debería considerar la inversión en investigación y desarrollo de tecnologías de IA. Apoyar proyectos orientados a mejorar la seguridad, la ética y la equidad en el ámbito de la IA contribuirá a fortalecer la capacidad del país para enfrentar los desafíos futuros y aprovechar las oportunidades que ofrece esta tecnología.

En resumen, para enfrentar los retos asociados con la IA, Argentina debe enfocarse en desarrollar una regulación adecuada, promover la educación y la colaboración internacional, así como invertir en investigación y desarrollo. Estos esfuerzos contribuirán a una integración más segura y beneficiosa de la IA en la sociedad.

Como se pudo advertir en este trabajo, Argentina se enfrenta al desafío crucial de garantizar que el desarrollo de la inteligencia artificial (IA) sea ético y responsable. Para lograr esto, es fundamental implementar una serie de medidas preventivas que aborden de manera integral los aspectos éticos, legales y técnicos asociados con esta tecnología en constante evolución.

El desarrollo de la IA ofrece enormes oportunidades, pero también plantea riesgos significativos si no se gestiona adecuadamente. Es necesario que Argentina establezca un enfoque equilibrado que no solo impulse la innovación, sino que también asegure que este progreso se desarrolle de manera alineada con principios éticos sólidos y normativas legales rigurosas. Las medidas preventivas deben abarcar la creación de marcos regulatorios claros que promuevan la transparencia y la rendición de cuentas, así como la implementación de mecanismos que garanticen la protección de los derechos individuales y la privacidad.

Adicionalmente, es crucial fomentar una cultura de responsabilidad tanto entre los desarrolladores como entre los usuarios de la IA. Esto implica la promoción de una educación continua y la capacitación en torno a los desafíos éticos y técnicos que conlleva el uso de estas tecnologías. La inversión en investigación y la cooperación con organismos internacionales también jugarán un papel vital en el fortalecimiento de estas medidas, permitiendo a Argentina adoptar las mejores prácticas globales y adaptar las soluciones a sus necesidades específicas.

Por lo tanto, para que el país pueda aprovechar de manera óptima las oportunidades que la IA ofrece, mientras mitiga los posibles riesgos, debe adoptar una estrategia proactiva y multifacética. Esta estrategia debe combinar la regulación efectiva, la educación integral y la colaboración internacional, asegurando que el desarrollo de la IA sea tanto innovador como respetuoso de los valores fundamentales y las normativas legales.

Capítulo 14 - Conclusiones

Como se ha visto en el presente trabajo, el concepto de ciberpatrullaje implica el planteo de preocupaciones sobre la invasión de la privacidad y el potencial para el abuso de poder por parte de las autoridades encargadas de llevar a cabo estas prácticas. El ciberpatrullaje no sólo afecta la privacidad individual, sino que también socava la libertad de expresión y limita la diversidad de ideas en el ciberespacio. Asimismo, puede avizorarse que las actividades de vigilancia en línea pueden generar un efecto de autocensura entre los usuarios, quienes podrían abstenerse de expresar ciertas opiniones por temor a represalias o vigilancia.

Al ser una práctica que implica la vigilancia del ciberespacio, el tema de la privacidad es un tema que, como se vio reflejado en este trabajo, se encuentra entre paréntesis. La privacidad en el ciberespacio es un tema de creciente importancia en la era digital actual. A partir del acelerado desarrollo tecnológico y la omnipresencia de internet en la vida de los ciudadanos, las actividades en línea están cada vez más expuestas a la vigilancia y a la recopilación de datos por parte de diversas entidades, incluidas empresas, gobiernos y, también, por ciberdelincuentes. En este sentido, es fundamental atender el tema de la privacidad en el ciberespacio, que consiste en la capacidad que poseen los individuos para controlar qué información personal divulgan y quién tiene acceso a ella mientras navegan por internet, utilizan aplicaciones móviles, realizan transacciones en línea y participan en redes sociales, entre otras actividades en línea. Esto, además, incluye datos como nombres, direcciones, números de teléfono, correos electrónicos, historiales de navegación, compras en línea, ubicaciones geográficas y mensajes privados.

Para abordar estas preocupaciones y proteger la privacidad en el ciberespacio, es necesario adoptar un enfoque multidisciplinario que involucre a diferentes actores, incluidos los ciudadanos, las empresas, los gobiernos y las organizaciones internacionales. A nivel individual, es importante que las personas estén informadas sobre los riesgos para la privacidad en línea y tomen medidas para protegerse, como utilizar contraseñas seguras, habilitar la autenticación de dos factores, actualizar regularmente el software y las aplicaciones y ser selectivos sobre qué información comparten en línea.

En definitiva, la privacidad en el ciberespacio es un tema complejo y multidimensional que requiere la atención tanto de académicos como de legisladores. Es crucial encontrar un equilibrio entre la innovación tecnológica y la protección de los derechos individuales para garantizar un entorno en línea seguro y respetuoso de la privacidad. Esta última, en el contexto del ciberdelito, es un tema de gran relevancia en la actualidad, ya que la proliferación de tecnologías digitales ha aumentado la vulnerabilidad de los individuos y organizaciones ante posibles ataques cibernéticos.

Asimismo, el ciberpatrullaje en Argentina presenta tanto oportunidades como desafíos. Mientras que puede ser una herramienta valiosa para prevenir el crimen y proteger a la sociedad, también es imperativo que su implementación no vulnere las garantías procesales y los derechos humanos que son fundamentales en una sociedad democrática. La clave está en la creación de políticas que armonicen la seguridad con el respeto a la dignidad y la libertad de las personas. Por lo tanto, el ciberpatrullaje en Argentina requiere de una legislación cuidadosamente elaborada que equilibre la seguridad y la privacidad. Debe incorporar principios de necesidad y proporcionalidad, así como mecanismos de supervisión independientes que aseguren el cumplimiento de las garantías procesales y los derechos humanos. Sólo así se podrá confiar en que las tecnologías de vigilancia no socavarán las libertades fundamentales en nombre de la seguridad.

Por otra parte, se pudo advertir la importancia y la relevancia que está teniendo la IA en el mundo y también en Argentina. En primer lugar, se ha comprobado cómo se ha integrado la IA a la ciberseguridad y las potencialidades de esta tecnología al respecto. No obstante, se pudo advertir cómo la misma IA es utilizada por ciertas personas para cometer delitos y debilitar y sortear la seguridad informática. Por estos motivos, es imprescindible que los profesionales y expertos en IA puedan adelantarse a la ciberdelincuencia y aprovechar las ventajas que implica el uso de las herramientas de ciberseguridad impulsadas por IA como, por ejemplo, analizar rápidamente grandes cantidades de datos, detectar anomalías y vulnerabilidades y automatizar procesos repetitivos.

Asimismo, se reparó en la importancia del cifrado para proteger los activos digitales. En suma, el cifrado es fundamental con respecto a la utilización de un algoritmo matemático que

tiene la capacidad de envolver un mensaje con la finalidad de que solo el receptor legítimo pueda abrirlo mediante la utilización de una clave única que desenvuelve el mensaje, es decir, el cifrado vuelve ininteligible un mensaje ante un tercero ajeno a esa comunicación. En resumen, el cifrado permite persuadir y desalentar las filtraciones de información en activos digitales en lo que respecta a la seguridad de los sistemas de administración.

Por último, se pudo advertir la trascendencia sustancia que posee replantear un marco para la IA, dado que para lograr que la IA tenga un efecto realmente significativo, es decisiva la objetividad para poder ser responsables sobre cómo aplicar esta tecnología con el fin de impulsar un mundo digital más fructífero, equitativo y moralmente transparente. Para alcanzar esto es fundamental establecer lineamientos éticos para determinar un marco sustancioso que regule las prácticas con respecto a la IA. Para ello, es necesario elaborar marcos normativos, tales como los propuestos por la UE, como es el caso de *AI Act* y ciertas iniciativas propuestas en Argentina que, si bien aún no fueron aprobadas y sancionadas, ayudan para planificar un marco sólido sobre el tema.

Referencias

Agencia de Acceso a la Información Pública (AAIP, 2024). Programa Nacional de Transparencia y Protección de Datos Personales en el uso de la Inteligencia Artificial. *Agentina.gob.ar.* https://www.argentina.gob.ar/aaip/programa-nacional-de-transparencia-y-proteccion-de-datos-personales-en-el-uso-de-la

Acurio Del Pino, S. (2010). Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0. *AR: Revista de Derecho Informático*, N.º 140. https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Amnistía Internacional. (2020). Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia. *Amnesty.* https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/los-estados-deben-respetar-los-derechos-humanos-al-emplear-tecnologias-de-vigilancia-digital-para-co/

Asociación por los Derechos Civiles. (2017). Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal. *ADC Digital*. https://adc.org.ar/wp-content/uploads/2019/06/032-evidencia-igital-investigacion-de-cibercrimen-y-garantias-del-proceso-penal-jornada-de-trabajo-12-2017.pdf

Balbix. (2023). Using Artificial Intelligence in Cybersecurity. *Balbix*. https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

Bartolomé, M. C. (2006). *La seguridad internacional en el siglo XXI, más allá de Westfalia y Clausewitz*. ANEPE.

Beccar Varela, E., Rosati, F., Beccar Varela, M. y Zavalia, F. (1 de agosto de 2024). Alerta Normativa: Creación de la Unidad de Inteligencia Artificial – Ministerio de Seguridad de la Nación. *Abogados.com*. https://abogados.com.ar/alerta-normativa-creacion-de-la-unidad-de-inteligencia-artificial-ministerio-de-seguridad-de-la-nacion/35227

Bhattacharya, D. (23 de julio de 2021). The Dark Web and Regulatory Challenges. *Manohar Parrikar Institute for Defence Studies and Analyses*. https://idsa.in/issuebrief/the-dark-web-and-regulatory-challenges-dbhattacharya-230721

Busaniche, B. (31 de julio de 2024). Ni artificial ni inteligencia, vigilancia ilegal. *Fundación Vía Libre*.

https://www.vialibre.org.ar/ni-artificial-ni-inteligencia-vigilancia-ilegal/

Carter, D. L. (2022). *Law Enforcement Intelligence*. Bureau of Justice Assistance. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Law_Enforcement_Intelligence_Guide_508.pdf

Centro de Estudios Legales y Sociales (CELS, 2020). Sobre el «Proyecto de protocolo de ciberpatrullaje». *CELS*. https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE, 2020). Protocolo de Ciberpatrullaje en fuentes abiertas". *CELE, Observatorio Regional*. https://observatoriolegislativocele.com/argentina-resolucion-144-2020-protocolo-de-ciberpatrullaje-en-fuentes-abiertas/

Chorny, V. (2020). Detenido por tuitear: el ciberpatrullaje contra los derechos humanos en Argentina. *R3D: Red en Defensa de los Derechos Digitales*. https://r3d.mx/2020/04/21/detenido-por-tuitear-el-ciberpatrullaje-contra-los-derechos-humanos-en-argentina/

Ciampa Dolárd, R. J. (30 de julio de 2024). Crean la Unidad de Inteligencia Artificial Aplicada a la Seguridad. *Palabras del Derecho*. https://palabrasdelderecho.com.ar/articulo/5270/Crean-la-Unidad-de-Inteligencia-Artificial-Aplicada-a-la-Seguridad#:~:text=El%20Ministerio%20de%20Seguridad%20de%20la%20Naci%C3%B3n%20cre%C3%B3%20la%20Unidad,Ministra%20de%20Seguridad%20Patricia%20Bullrich.

Conde, M. (17 de febrero de 2023). Nuevas herramientas contra el ciberdelito. *ANCCOM*. https://anccom.sociales.uba.ar/2023/02/17/nuevas-herramientas-contra-el-ciberdelito/

Consejo de Europa. (2001). *Convenio sobre Ciberdelincuencia*. STE, N.º 185. https://rm.coe.int/16802fa403

Consejo de Europa. (2021). Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios. *Convenio de Budapest sobre la Ciberdelincuencia*. https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

Consejo de Europa. (2022). Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas. *Serie de Tratados del Consejo de Europa*, N.º 224. https://rm.coe.int/1680a83724

Davidovsky, S. (30 de julio de 2024). Cómo funcionará la plataforma de ciberpatrullaje que anunció Patricia Bullrich. *La Nación*. https://www.lanacion.com.ar/tecnologia/como-funcionara-la-plataforma-de-ciberpatrullaje-que-anuncio-patricia-bullrich-nid30072024/

De Amo, D. (2020). Ciberpatrullaje: los expertos creen que es una práctica peligrosa y que pone en riesgo la libertad de expresión. *Fundación Vía Libre*. https://www.vialibre.org.ar/ciberpatrullaje-los-expertos-creen-que-es-una-practica-peligrosa-y-que-pone-en-riesgo-la-libertad-de-expresion/

Disposición 2/2023 sobre Recomendaciones para el uso de Inteligencia Artificial. Sancionada el 1 de junio de 2023. Publicada en el Boletín Nacional del 2 de junio de 2023. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-2-2023-384656/texto

Easterly, J. (2023). Artificial Intelligence. *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/ai

EU Artificial Intelligence Act. (2024). La Ley de Inteligencia Artificial de la UE. *Future of Life Institute*. https://artificialintelligenceact.eu/es/ai-act-explorer/

Europol. (2024). European police chiefs call for industry and governments to take action against end-to-end encryption roll-out. *European Union Agency for Law Enforcement Cooperation*. https://www.europol.europa.eu/media-press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end-to-end-encryption-roll-out

Flare. (28 de septiembre de 2023). Threat Spotlight: The Dark Web and AI. *Flare Systems*. https://flare.io/learn/resources/blog/threat-spotlight-the-dark-web-and-ai/

Flores, A. (22 de noviembre de 2023). Declaración de Bletchley: la seguridad de la IA. *Raia Diplomática*. https://raiadiplomatica.info/2023/11/22/declaracion-de-bletchley-la-seguridad-de-la-ia/

Fojón Chamorro, E. y Sanz Villalba, A. F. (2010). Ciberseguridad en España: una propuesta para su gestión. *ARI*. Real Instituto Elcano. https://www.files.ethz.ch/isn/118153/ARI102-2010_Fojon_Sanz_ciberseguridad_Espana.pdf

Gaimari, G. (2021). Inteligencia Artificial e impacto en el cibercrimen [Tesina de grado]. Universidad de Belgrano.

https://repositorio.ub.edu.ar/handle/123456789/9333

Ganesh, S. (18 de junio de 2023). Trained on the dark web, Darkbert AI can combat cyber crimes. *Analytics Insight*. https://www.analyticsinsight.net/artificial-intelligence/trained-on-the-dark-web-darkbert-ai-can-combat-cyber-crimes

Gargarella, R. (2021). *El derecho como una conversación entre iguales*. Siglo XXI.

Goldblum, M., Anandkumar, A., Baraniuk, R. & Goldstein, T. (2023). Perspectives on the State and Future of Deep Learning. *ArXiv.* https://arxiv.org/abs/2312.09323

Gómez Rodríguez, G. y González Reyes, R. (2023). Comunicación y sociedad de la vigilancia contemporánea. *Comunicación y Medios*, Vol. 32, N.º 47, pp. 15-23. https://www.scielo.cl/pdf/cym/v32n47/0719-1529-cym-32-47-00015.pdf

González Torre, A. P. (2011). Aspectos jurídicos del poder: los ilegalismos. *Cuadernos Electrónicos de Filosofía del Derecho*, N.º 23, pp. 422-431. https://ojs.uv.es/index.php/CEFD/article/viewFile/765/481

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and Harnessing Adversarial Examples. *ICLR 2015*. https://arxiv.org/pdf/1412.6572

Goodfellow, I., Bengio, Y. & Courville, A. (2016). *Deep Learning*. MIT Press. https://www.deeplearningbook.org/

Government Accountability Office (GAO, 2024). *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud*. United States Government Accountability Office. https://www.gao.gov/assets/d24105833.pdf

Government of the United Kingdom (Gov.UK, 1 de noviembre de 2023a). Countries agree to safe and responsible development of frontier AI in landmark Bletchley Declaration. https://www.gov.uk/government/news/countries-agree-to-safe-and-responsible-development-of-frontier-ai-in-landmark-bletchley-declaration

Government of the United Kingdom (Gov.UK, 1 de noviembre de 2023b). The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Government of the United Kingdom (Gov.UK, 2024). *"Criminals should be aware" says Minister as Government upgrades AI fraud detection tool*. https://www.gov.uk/government/news/criminals-should-be-aware-says-minister-as-government-upgrades-ai-fraud-detection-tool

Gutiérrez, R., Radesca, L. V. y Riquert, M. A. (2013). Violación de Secretos y de la Privacidad. *Revista Pensamiento Legal*. https://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37761.pdf

INTERPOL. (2019). Cybercrimes cross borders and evolve rapidly. *Cybercrime*. https://www.interpol.int/en/Crimes/Cybercrime

Kaspersky Digital Footprint Intelligence. (24 de enero de 2024). Cybercrime AI experimentation in the dark web. *Kaspersky*. https://www.kaspersky.co.uk/about/press-releases/2024_cybercrime-ai-experimentation-in-the-dark-web-new-kaspersky-study

Laje, D. (28 de noviembre de 2023). AI Cybersecurity: 22 Nations Sign Landmark Agreement. *Signal*. https://www.afcea.org/signal-media/ai-cybersecurity-22-nations-sign-landmark-agreement

Ley 27.411 de 2017. Convenio sobre Ciberdelito. Sancionada el 22 de noviembre de 2017. B.N.: 15 de diciembre de 2017. https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

Mak, L. (2024). Europol wants tech giants to roll back end-to-end encryption. *VPNoverview.* https://vpnoverview.com/news/europol-wants-tech-giants-to-roll-back-end-to-end-encryption/

Márquez Díaz, J. (2020). Inteligencia artificial y Big Data como soluciones frente a la COVID-19. *Revista de Bioética y Derecho*, N.º 50, pp. 315-331. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300019

Martín Ríos, P. (2022). Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras. *Revista de los Estudios de Derecho y Ciencia Política*, N.º 36. https://raco.cat/index.php/IDP/article/view/n36-martin

Martínez, V. (2023). Breves Consideraciones sobre el Estado de la Regulación de la Inteligencia Artificial en Argentina. *WSC Legal*. https://wsclegal.com/es/regulacion-de-la-inteligencia-artificial-en-argentina/

Ministerio de Seguridad. (2023). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*. Argentina.gob. https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf

Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. (3 de septiembre de 2021 Innovación e Inteligencia Artificial. *MPF CABA*. https://mpfciudad.gob.ar/institucional/2020-03-09-21-42-38-innovacion-e-inteligencia-artificial

Ministry of Electronics and Information Technology (MEITy, 2023). *The Digital Personal Data Protection Act, 2023*. Government of India. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

Monte, M. y Sánchez, S. I. (23 de abril de 2021). Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas. *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/index.php/doctrina/89035-tensiones-constitucionales-entre-derecho-intimidad-y-ciberpatrullaje-investigacion

Morgan Stanley. (2023). AI and Cybersecurity: A New Era. *Morgan Stanley Wealth Management*. https://www.morganstanley.com/articles/ai-cybersecurity-new-era

National Cyber Security Centre. (2024). AI and cyber security: what you need to know. *NCS*. https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know

National Institute of Justice. (15 de junio de 2020). Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs. *NIJ*. https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs

Nigro, P. (2024). The intersection of cybersecurity & artificial intelligence. *Security Magazine*. https://www.securitymagazine.com/articles/100312-the-intersection-of-cybersecurity-and-artificial-intelligence

Nyíri, T. (2023). AI Cybersecurity. *SC Magazine*. https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity#:~:text=How%20Does%20AI%20Apply%20to,common%20kinds%20of%20cyber%20attacks

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH, 2021). Pacto Internacional de Derechos Civiles y Políticos. *Naciones Unidas*. https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Onocko, S. (2024). Ciberpatrullaje para la seguridad. *Diario Judicial*. https://www.diariojudicial.com/news-97895-ciberpatrullaje-para-la-seguridad

Organización de Estados Americanos. (OEA, 2020). *Documentos claves de la OEA sobre ciberseguridad*. Banco Interamericano de Desarrollo.

Palos-Sánchez, P. R., Robina Ramírez, R. y Cerdá Suárez, L. (2018). Ética de la reputación online, marca personal y privacidad en el cloud computing: protección de los usuarios frente al derecho al olvido. *Biblios*, N.º 71, pp. 17-31. http://dx.doi.org/10.5195/biblios.2018.428

Pastorini, J. (2019). Prevención y persecución de Ciberdelitos: ¿Un nuevo terreno para la Inteligencia Artificial? *Programa Becas Iberoámerica Jóvenes Profesores Investigadores 2018-2019*. Universidad CEU San Pablo, "Ciberdelitos: España Argentina".

Peirano, N. (2 de agosto de 2024). Argentina: cómo trabajará la flamante Unidad de Inteligencia Artificial Aplicada a la Seguridad. *DEF.* https://defonline.com.ar/seguridad/argentina-como-trabajara-la-flamante-unidad-de-inteligencia-artificial-aplicada-a-la-seguridad/

Pisanu, G. (2023). Ciberpatrullaje en Argentina: los riesgos del monitoreo de redes sociales para los derechos humanos. *Access Now.* https://www.accessnow.org/ciberpatrullaje-en-argentina-los-riesgos-del-monitoreo-de-redes-sociales-para-los-derechos-humanos/

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, N.º 20, pp. 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. (2013). *13 Principios*. https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

Proyecto de Ley Anulación de la Resolución 710/2024 del Ministerio de Seguridad de la Nación, por Medio de la cual se Crea la "Unidad de Inteligencia Artificial Aplicada a la

Seguridad – UIAAS". Expediente: 4125-D-2024, del 5 de agosto de 2024. Publicado en: Trámite Parlamentario N° 109.
https://www.diputados.gob.ar/comisiones/permanentes/caconstitucionales/proyecto.html?exp=4125-D-2024

Quintana, Y. (2016). *Ciberguerra*. Editorial Catarata.

Resolución 161 de 2023 sobre el Programa Nacional de Transparencia y Protección de Datos Personales en el uso de la Inteligencia Artificial. Sancionada el 30 de agosto de 2023. Publicada en el Boletín Nacional del 4 de septiembre de 2023.
https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-161-2023-389231/texto

Resolución 428 de 2024. Fuerzas Policiales y de Seguridad Federales – Adecuación Delitos en Ambientes Cibernéticos. B.O.: 28 de mayo de 2024.
https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528

Resolución 710 de 2024. Unidad de Inteligencia Artificial Aplicada a la Seguridad. Creación. Sancionada el 26 de julio de 2024. B. N.: 29 de julio de 2024.
https://www.boletinoficial.gob.ar/detalleAviso/primera/311381/20240729

Riquert, M. A. (13 de agosto de 2024). Libertad vs. seguridad: nuevas tensiones a propósito del ciberpatrullaje y la creación de la UIAAS. *Revista Pensamiento Penal*.
https://www.pensamientopenal.com.ar/doctrina/91395-libertad-vs-seguridad-nuevas-tensiones-proposito-del-ciberpatrullaje-y-creacion

Roatta, S., Casco, M. E. y Fogliato, M. (2015). El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. *XXI Congreso Argentino de Ciencias de la Computación. Libro de actas*, Universidad Nacional del Noroeste de la provincia de Buenos Aires (UNNOBA).
https://sedici.unlp.edu.ar/bitstream/handle/10915/50586/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Romero Muñoz, J. (2017). CiberÉtica como ética aplicada: una introducción". *Dilemata*, N.º 24, pp. 45-63.
https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100

Rueda Laje, T. (12 de agosto de 2024). IA y seguridad: riesgos y desafíos de la nueva regulación nacional. *La Nación*.
https://www.lanacion.com.ar/opinion/ia-y-seguridad-riesgos-y-desafios-de-la-nueva-regulacion-nacional-nid12082024/

Russell, S. & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson.

Schatzky, M. y Zara, N. (2023). *Inteligencia basada en fuentes abiertas (OSINT) en Argentina: un diagnóstico sobre su utilización por parte del Estado*. Centro de Estudios en Libertad de Expresión y Acceso a la Información, Universidad de Palermo. https://www.palermo.edu/Archivos_content/2023/cele/papers/230621-reporte-OSINT.pdf

Schulkin, J. (13 de mayo de 2018). Argentina se suma a la Convención de Budapest para tratar delitos informáticos. *Infobae*. https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

Steele, G. (2024). Cybersecurity is on the frontline of our AI future. Here's why. *World Economic Forum*. https://www.weforum.org/agenda/2024/01/cybersecurity-ai-frontline-artificial-intelligence/

Trend Micro Research, UNICRI, Europol. (2020). Malicious Uses and Abuses of Artificial Intelligence. *Trend Micro Research*. https://igfspain.org/wp-content/uploads/2020/12/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

UNICRI / INTERPOL. (2020). *Towards Responsible Artificial Intelligence Innovation*. United Nations Interregional Crime and Justice Research Institute – International Criminal Police Organization. https://unicri.it/towards-responsible-artificial-intelligence-innovation

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) & Dirección General de Cooperación Regional e Internacional (DIGCRI) (2020). *Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero*. Ministerio Público Fiscal. https://www.mpf.gob.ar/ufeci/files/2021/07/UFECI-2020-Gui%CC%81a-de-Evidencia-Digital.pdf

Unión Internacional de Telecomunicaciones (UIT, 2008). Recomendación X.1205. Aspectos generales de la ciberseguridad. Aprobada en 18 de abril de 2008. https://www.itu.int/rec/T-REC-X.1205-200804-I/es

United States Department of the Treasury (USTD, 2024). *Managing Artificial Intelligence Specific Cybersecurity Risks in the Financial Services Sector.* https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf

Vassilev, A., Oprea, A., Fordyce, A. & Anderson, H. (2024). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*. National Institute of Standards and Technology, NIST. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

Velasco Rico, C. I. (7 de febrero de 2024). Un apunte sobre la Declaración de Bletchley y el futuro Reglamento de IA de la UE. *Revista Catalana de Dret Públic*. https://eapc-rcdp.blog.gencat.cat/2024/02/07/un-apunte-sobre-la-declaracion-de-bletchley-y-el-futuro-reglamento-de-ia-de-la-ue-clara-i-velasco-rico/

Vercelli, A. (2024). Regulaciones e inteligencias artificiales en Argentina. *Inmediaciones de la Comunicación*, Vol. 19, N.º 1, pp. 107-135. http://www.scielo.edu.uy/pdf/in/v19n1/1688-8626-in-19-01-52.pdf

Wisner-Glusko, D. C. (2022). Breves reflexiones sobre la importancia del Estado de Derecho en el desarrollo del marco legal sobre los sistemas de inteligencia artificial en la Unión Europea. En F. H. Llano Alonso (Dir.), *Inteligencia Artificial y Filosofía del Derecho* (pp. 529-548). Ediciones Laborum.

Wisner-Glusko, C. (9 de noviembre de 2023). La Declaración de Bletchley ¿una nueva mirada global sobre el desarrollo seguro y responsable de la Inteligencia Artificial? *Observatorio Sector Público e Inteligencia Artificial (OspIA)*. https://www.ospia.org/o-lab/la-declaracion-de-bletchley-una-nueva-mirada-global-sobre-el-desarrollo-seguro-y-responsable-de-la-inteligencia-artificial

Ybañez, N. (2020). Ciberpatrullaje: ¿cuál es el límite de las fuerzas de seguridad? *El Economista*. https://eleconomista.com.ar/debate/ciberpatrullaje-cual-limite-fuerzas-seguridad-n33610