Ciberpatrullaje, Privacidad y Derechos

D. J. Romero, *Ingeniero en Informática e Ingeniero Electrónico* [1] y A. Grisolia, *Becario*[2]

[1]*Universidad Nacional de La Matanza (UNLaM) y Universidad Nacional del Oeste (UNO)*
djromero@unlam.edu.ar
[2]*Universidad Nacional del Oeste (UNO) dgrisolia@uno.edu.ar*

***Resumen*– En este trabajo se examinará el concepto de ciberpatrullaje, entendido como una actividad de vigilancia e investigación realizada por las fuerzas de seguridad en el ciberespacio, y se explorarán sus implicaciones en relación con la privacidad y la posible vulneración de los derechos de los ciudadanos. Para analizar este tema, se indagará, 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 cuando se habla de ciberpatrullaje. A su vez, se tomarán en cuenta las leyes, así como las resoluciones internacionales y nacionales, que tratan 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.**

***Abstract*– This work will examine the concept of cyberpatrolling, understood as a surveillance and investigative activity conducted by law enforcement in cyberspace, and will explore its implications regarding privacy and potential violations of citizens' rights. To analyze this topic, each relevant concept will be scrutinized in detail, including cybersecurity, user privacy, and the protection of rights that may be compromised with cyberpatrolling. Addiotinally, laws, international and national resolutions addressing information security and privacy will be considered. The risks and challenges posed by cyberpatrolling to human rights, particularly freedom of expression and user privacy, will also be analyzed, along with delving into the ethical, political, and social implications of cyberpatrolling.**

I. INTRODUCCIÓN

El ciberpatrullaje es una forma de vigilancia que implica la observación, análisis y recopilación de información de fuentes digitales abiertas, como las redes sociales, con el propósito de prevenir o investigar delitos. No obstante, esta práctica presenta riesgos y desafíos para los derechos humanos, en particular 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 En Argentina, en 2020, el Ministerio de Seguridad derogó la Resolución 31/2018, que habilitaba el ciberpatrullaje, y la reemplazó por la Resolución 144/2020 que buscaba 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 y volver a configurar las bases de este tema.

Para comprender el ciberpatrullaje, es esencial examinar ciertos conceptos que permiten definir de manera más precisa este campo. Estos conceptos son: ciberseguridad, ciberespacio y, específicamente, dos conceptos impactados por el uso del ciberpatrullaje: la privacidad y, especialmente, los derechos humanos. En este trabajo se elaborará un examen acerca de estos conceptos para alcanzar una base sólida que permita indagar acerca de la problemática planteada en este trabajo.

II. CIBERSEGURIDAD Y PRIVACIDAD

No es posible discutir sobre ciberseguridad, ciberpatrullaje o la vulneración de derechos a través de la vigilancia sin abordar el ciberespacio, que es el entorno donde toda esta realidad ocurre. De esta forma, existe un escenario en el que las nociones de ciberseguridad y ciberespacio son familiares para todos los individuos. Sin embargo, no se posee un conocimiento completo sobre cómo estas pueden impactar la vida diaria de las personas, tanto en lo personal como en lo profesional. Los conceptos de ciberseguridad y ciberespacio son altamente complejos, dado que la ciberseguridad representa un nuevo modelo de seguridad global para los entornos afectados por la influencia y el uso del ciberespacio.

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; no obstante, ese programa no brinda un concepto propio de ciberseguridad [1].

Para el caso argentino, la Resolución del JGM N° 580/11 que crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), invoca el terminó ciberseguridad, pero no le reporta ninguna definición rigurosa. Por su parte, para la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de la Organización de las Naciones Unidas (ONU), 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 [2]. En resumen, la ciberseguridad asegura que se logren y se mantengan las propiedades de seguridad de los activos de la organización y de los usuarios frente a los riesgos asociados en el entorno digital. Estas propiedades de seguridad abarcan una o varias de las siguientes características: disponibilidad; integridad, que puede englobar autenticidad y no repudio; y confidencialidad. La UIT propone unos aspectos mediante los cuales se podría dividir el enfoque de la definición de ciberseguridad, que variará de acuerdo a 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 o proteger la infraestructura, 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. Se debe agregar, que el concepto ciberentorno aportado por la UIT resulta equivalente al de ciberespacio.

Además, para lograr una definición más sólida de la noción de ciberespacio que permita comprender y asimilar de manera eficaz las implicaciones mencionadas previamente, es crucial considerar el concepto de servicio, entendido como la prestación que un usuario o consumidor recibe de un proveedor. En consecuencia, el ciberespacio podría definirse como el conjunto de medios y de procedimientos basados en las tecnologías de la información y que se encuentran 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 OEA ofrece una perspectiva sobre el progreso alcanzado desde su primera edición. Este organismo 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 también, para aumentar y asegurar la confianza de los ciudadanos en las tecnologías digitales, y para permitirles sentirse confortables cuando acceden a dichas tecnologías [1].

Dada la temática escogida, resulta esencial discernir el concepto de seguridad en el ciberespacio. Por un lado, la seguridad se establece como una cualidad que percibe un determinado actor, respecto a una situación dada en su contexto. Por otro lado, la seguridad implica aquellas acciones llevadas a cabo por el actor en cuestión, a los efectos de alcanzar una situación ideal. En este sentido, la seguridad seria 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 [2]. De esta forma, 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 información recopilada deberá limitarse estrictamente a lo necesario para caracterizar y gestionar los tipos de amenazas, evitando en particular la recopilación y procesamiento que puedan comprometer 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, establecerá una red de trabajo.

Cuando se habla de ciberpatrullaje, entendido como la vigilancia y el monitoreo de actividades en el ciberespacio por parte de las fuerzas de seguridad, surgen diversas complejidades, dado que pueden vulnerarse ciertos derechos. Esta situación ha generado un intenso debate en Argentina.

Es importante indagar acerca de la constitucionalidad de estas prácticas de vigilancia por parte de las fuerzas de seguridad. En este sentido, se deben determinar las condiciones para comprender cómo se podrían establecer parámetros objetivos para construir una sospecha razonable que justifique la intrusión del Estado en la privacidad de los individuos a través de las tecnologías de la información y comunicación. Con el auge de la sociedad de la información y el uso intensivo de las tecnologías de la información y la comunicación (TIC), 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 [4].

III. IMPORTANCIA DE LA REGULACIÓN

Para realizar una labor sólida y transparente sobre este tema, es crucial establecer una legislación que regule adecuadamente el ciberpatrullaje. Dicha normativa debe ser precisa y proporcionada, asegurando que las garantías procesales y los derechos humanos sean respetados. Es imprescindible, como se ha visto, una normativa asentada en una base que no vulnere los derechos de las personas, y para ello es vital observar las regulaciones que se han establecido a nivel internacional. En Estados Unidos, 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. 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 (Children's Online Privacy Protection Act, COPPA) en 1998. 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 (General Data Protection Regulation, GDPR); 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). En la región sudamericana, 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, parece relevante pensar una manera eficiente que permita 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 mediante este tipo de vigilancia.

Por lo tanto, a partir de lo analizado en la primera parte de este trabajo, se puede sintetizar una idea de lo que se podría esperar de una sociedad en la que exista un ciberpatrullaje sólido y efectivo, pero que respete y se ajuste a una serie de reglas que garanticen 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 segura que vele por los derechos de las personas en los casos de monitoreo por ciberpatrullaje.

Argentina podría inspirarse en las normativas internacionales y regionales como base, y luego desarrollar métodos apropiados y específicos que se ajusten a su realidad, para asegurar que el ciberpatrullaje no afecte de manera negativa los derechos personales y la privacidad de los individuos. 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 estos datos se encuentren almacenados en el país o, en su defecto, en el extranjero.

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 y que ha quedado efectivo 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 [5]. El ciberpatrullaje desempeña un papel fundamental en la seguridad del ciberespacio. No obstante, su implementación debe realizarse de manera que se respete y proteja la privacidad de las personas. Las leyes internacionales como el Patriot Act y el CLOUD Act, así como las regulaciones argentinas, proporcionan un marco dentro del cual se puede lograr este equilibrio. Sin embargo, es crucial que se mantenga un diálogo continuo y se realicen modificaciones según sea preciso para asegurar la protección tanto de la seguridad como de la privacidad.

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 [5].

A pesar de la importancia del ciberpatrullaje, es fundamental que se lleve a cabo respetando la privacidad de las personas. La privacidad es un derecho humano fundamental que debe ser protegido, incluso en el ciberespacio. Por lo tanto, las actividades de ciberpatrullaje deben estar sujetas a regulaciones que garanticen el respeto a la privacidad. Para alcanzar un equilibrio entre la seguridad y la privacidad, es crucial establecer normativas claras y transparentes para el ciberpatrullaje. Estas normativas deben determinar qué información puede recopilarse, cómo puede utilizarse y cuándo debe eliminarse. Además, es fundamental que aseguren que todas las actividades de ciberpatrullaje estén sujetas a supervisión y rendición de cuentas.

Ahora bien, el tema tratado en este trabajo es un tema que está en constante progreso, dado que la tecnología evoluciona de manera cotidiana. Por esta razón, es crucial fortalecer continuamente los mecanismos de control, ya que los delitos ocurren a velocidades rápidas y requieren nuevas herramientas para abordarlos.

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 *big data* y la inteligencia artificial (IA), puesto que actualmente se utilizan estos instrumentos para asuntos 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, y esto incluye, claro está, 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 [6]. Es crucial enfatizar sobre la transparencia de los mecanismos utilizados para abordar los problemas derivados del ciberpatrullaje, garantizando así un pleno respeto de los derechos humanos sin comprometerlos.

El último informe de Freedom House (organización no gubernamental con sede en Washington D. C., 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 [5]. 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 los 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 [5]. 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 su propia privacidad cuando, por ejemplo, se crean un perfil en alguna red social.

Por lo tanto, es fundamental que cada ciudadano fortalezca su responsabilidad activa y dinámica. Cada persona debe tomar el control de manera proactiva y decidir cómo actuar en cada situación, anticipándose a los eventos que puedan surgir. ¿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 ciudadanos, pero también debe consolidarse la eficiencia y la transparencia de las distintas agencias de control del Estado. Para ello, como se pudo advertir 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 definitiva, se debe indicar que 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 [6].

IV. VIGILANCIA Y VULNERACIÓN DE DERECHOS

Aparte de las normativas establecidas, es crucial abordar ciertos problemas, dado que actualmente algunas prácticas de monitoreo y vigilancia en el ciberespacio no están reguladas por los Estados debido a la falta de leyes y normativas estrictas que protejan los derechos humanos en materia de ciberseguridad. Principalmente, es imperioso destacar el rol sustancial que debe tener el Estado valiéndose de la ética, para hacer frente a estas problemáticas.

La ética en ciberseguridad y privacidad es un tema emergente en la ética como campo de estudio, y por lo tanto requiere una profunda reflexión por parte de los expertos en este país. Comprender estos problemas podría contribuir significativamente a mejorar la regulación del ciberpatrullaje y proteger los derechos individuales.

Es esencial sugerir un enfoque renovado para entender y reflexionar sobre los dilemas éticos relacionados con las tecnologías de la información, buscando así generar recomendaciones prácticas para la acción. Las sociedades que se encuentran interconectadas son las que han exigido su nacimiento y actuación, son ellas las que precisan y demandan un saber interdisciplinar para su acción en la vida pública, siendo un bien de primera necesidad para determinar la altura moral de una sociedad [7].

Por su parte, es perentorio profundizar sobre el tema de la privacidad, dado que la aceleración de la tecnología implica poder gestionar grandes cantidades de datos, así como también, de informaciones y conocimientos, lo que a su vez lleva consigo importantes problemas de seguridad y privacidad [8]. Si 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. Esta problemática debe ser planteada de esta manera, puesto que 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, y muchas veces, como se vio en este trabajo, esta tarea se realiza a través del ciberpatrullaje, esa protección no debe vulnerar la privacidad de los ciudadanos.

Lo esencial en este caso, es indagar no solo 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 pueden llevar a cabo ciertas acciones que vulneran los derechos de la privacidad de las personas. Esta situación, 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 modernas, transformándose en una suerte de competencia o carrera tecnológica, como sucede con el caso de la IA

En consecuencia, en el marco de la persecución policial contra problemáticas como 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. Algo similar sucede 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 [6]. Se debe aclarar, que los *honey pots* (o *honey monkeys*) son herramientas de seguridad informática implementadas en una red o sistema para ser el blanco de un potencial ataque informático, con el fin de detectarlo y recabar información tanto sobre el ataque como sobre el atacante. 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, y es el de la protección de los derechos de las personas con respecto al ciberpatrullaje. Es sustancial atender el tema de los derechos humanos, porque son derechos que 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 implican la observación de 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 [9].

Estas acciones se encuadran en el marco de lo que se conoce como inteligencia de fuentes abiertas (*open-source intelligence*, OSINT) e inteligencia en redes sociales (*social media intelligence*, SOCMINT). ¿En qué medida corre riesgo la libertad de una persona cuando las fuerzas de seguridad realizan este tipo de operaciones? Cuando se realiza el monitoreo de, por ejemplo, las redes sociales por parte del gobierno implica importantes riesgos para la privacidad y la libertad de expresión de los usuarios [9]. Aquí se plantea una disyuntiva 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. Este reparo ya fue planteado por 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, es necesario mencionar que el protocolo propicia 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 [10].

Si no queda delimitada categóricamente esa división, la vulneración de los derechos humanos se volvería muy evidente. 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.

Para profundizar sobre este aspecto importante del tema analizado en este trabajo, es fundamental reparar en la trascendencia de la inteligencia de fuente abierta (OSINT), que es una práctica que se encuentra generalizada y que es incompatible con el estado de derecho. Es fundamental indicar, que la inteligencia de fuente abierta vulnera dos aspectos elementales. Un aspecto que se ve vulnerado es la privacidad de las personas. Puesto que 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. Otro aspecto que podría verse vulnerado, se evidencia claramente cuando la inteligencia de fuente abierta ejerce una forma de condicionamiento del discurso público, puesto que 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 [11].

Lo que los organismos de defensa de los derechos de las personas reclaman, es que en la realidad se impone una notoria diferencia, y es que las autoridades "parecen desaparecer" cuando las personas se hallan vigiladas a través del ciberpatrullaje. En concreto, 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.

Es por estos motivos que se cree necesario regular de manera eficiente el ciberpatrullaje para que se lleve a cabo de manera protegida y respetando los derechos humanos, para que las personas puedan conducirse en internet de manera segura, conociendo los límites y certezas. Asimismo, lo más importante es establecer que si la persona comete un delito,

sepa cuáles son las penas por ese delito cometido.

La posibilidad de cometer abusos sobre los derechos humanos está latente constantemente mediante el uso del ciberpatrullaje, y por este motivo es imprescindible elaborar procedimientos de vigilancia que deberán permanecer abiertos al escrutinio público y ser revisados regularmente. Sin esta condición, la confianza de la sociedad en el gobierno puede verse seriamente afectada [9]. Además, es insoslayable comprender, que si bien es necesaria la vigilancia dada la cantidad de delitos que se cometen en las redes con cada vez mayor asiduidad, no deben utilizarse mecanismos en base a engaños. En definitiva, las autoridades no pueden obtener acceso a información usando perfiles falsos como señuelo [9].

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, probados, 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 deberá estar disponibles para el público para su revisión [9]. 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 establezca en consonancia con los valores democráticos y tipificados de los derechos humanos. Este organismo, recomienda que las fuerzas federales de seguridad dejen de llevar a la práctica actividades de vigilancia de carácter indiscriminado en fuentes abiertas. A su vez, se cree imperioso que se constituya una sólida y contundente normativa general que discuta los protocolos para todas las policías provinciales [12].

En el mundo de las leyes, las autoridades solo pueden obrar de acuerdo a 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 [13]. 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. De este modo, 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 [13]. Siguiendo este tema, se puede indicar que 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.

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 *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 determinar cómo las normas y estándares internacionales de derechos humanos se aplican en el contexto de la vigilancia de las comunicaciones Estos fundamentos sostienen que la vigilancia debe ajustarse a un conjunto de principios para respetar los derechos humanos. Entre los más destacados se deben destacar 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 [14].

Esto 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 de las mismas. Es por motivos como estos, que 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. En efecto, 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 [15].

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. Sin embargo, 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 debe limitarse a combatir el delito. No debe infringir los derechos humanos de tal manera que las personas sientan amenazada su libertad y se auto-censuren excesivamente por temor a ser vigiladas por dicho mecanismo de vigilancia.

CONCLUSIONES

Como se ha visto reflejado en este trabajo, la privacidad en el ciberespacio es un tema de creciente importancia en la era digital actual. Con el incontenible avance de la tecnología, y a partir de 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 los ciberdelincuentes.

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. 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.

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. El ciberpatrullaje en Argentina requiere de una legislación cuidadosamente elaborada que equilibre la seguridad y la privacidad.

REFERENCIAS

[1] Organización de Estados Americanos, Documentos claves de la OEA sobre ciberseguridad. Banco Interamericano de Desarrollo, 2020.
[2] M. C. Bartolomé, La seguridad internacional en el siglo XXI, más allá de Westfalia y Clausewitz, ANEPE, 2006.
[3] Unión Internacional de Telecomunicaciones (UIT). Recomendación X.1205. Aspectos generales de la ciberseguridad. Aprobada en 18 de abril de 2008.
[4] M. Monte y S. I. Sánchez, "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, 2021.
[5] N. Ybañez, "Ciberpatrullaje: ¿cuál es el límite de las fuerzas de seguridad?", El Economista, 2020.
[6] P. Martín Ríos, "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, 2022.
[7] J. Romero Muñoz, "CiberÉtica como ética aplicada: una introducción". Dilemata, N.º 24, pp. 45-63, 2017.
[8] P. R. Palos-Sánchez, R. Robina Ramírez y L. Cerdá Suárez, "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, 2018.
[9] G. Pisanu, "Ciberpatrullaje en Argentina: los riesgos del monitoreo de redes sociales para los derechos humanos". Access Now, 2023.
[10] Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), "Protocolo de Ciberpatrullaje en fuentes abiertas", CELE. Observatorio Regional, 2020.
[11] D. De Amo, "Ciberpatrullaje: los expertos creen que es una práctica peligrosa y que pone en riesgo la libertad de expresión", Fundación Vía Libre, 2020.
[12] Centro de Estudios Legales y Sociales (CELS), "Sobre el «Proyecto de protocolo de ciberpatrullaje»", CELS, 2020.
[13] V. Chorny, "Detenido por tuitear: el ciberpatrullaje contra los derechos humanos en Argentina", R3D: Red en Defensa de los Derechos Digitales, 2020.
[14] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "13 Principios", 2013.
[15] Amnistía Internacional, "Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia", Amnesty, 2020.