Universidad de San Andrés

Departamento de Derecho

Maestría en Derecho Penal

Elegía de lo íntimo

Ciberpatrullaje en la sociedad de la transparencia

Marcelo Sciegata

D.N.I. N° 34.490.378

Dr. Ignacio Francisco Tedesco

Ciudad Autónoma de Buenos Aires, 11/9/24

Universidad de San Andrés
Departamento de Derecho
Maestría y Especialización en Derecho Penal

Elegía de lo íntimo
Ciberpatrullaje en la sociedad de la transparencia

Marcelo Sciegata
D.N.I. N° 34.490.378
Dr. Ignacio Francisco Tedesco

Ciudad Autónoma de Buenos Aires, 11/9/24

Resumen

En la presente tesis se abordará el modo en que una nueva técnica de investigación penal orientada a la búsqueda de la verdad, el ciberpatrullaje, opera en un contexto de "panóptico digital" con la posibilidad de desentrañar la intimidad de las personas. La hipótesis que se plantea es que la ausencia de una ley que regule esta técnica de prevención, predicción e investigación penal podría implicar una afectación inconstitucional. Es por esto que el objetivo de este trabajo será evaluar si su utilización, mediante el uso de inteligencia artificial, redunda en mayor vigilancia y control social, en detrimento de garantías constitucionales.

Palabras claves: transparencia, psicopolítica, microfísica del poder, panóptico digital, inteligencia artificial, búsqueda de la verdad, ciberpatrullaje e intimidad.

ÍNDICE TEMÁTICO

I) Introducción al objeto de estudio

Los avances tecnológicos de las dos últimas décadas a nivel mundial han impulsado el nacimiento de novedosos métodos de investigación penal, legitimados a través del concepto de transparencia en la toma de decisiones y eficiencia en las investigaciones. Bajo este discurso y la lucha contra la inseguridad, con la implementación de medios tecnológicos e inteligencia artificial se persigue, por un lado, la prevención de determinados delitos (ciberdelitos) y, por el otro, poner un freno al incesante acrecentamiento de la criminalidad.

Uno de ellos es el ciberpatrullaje, mediante el cual se autoriza a las fuerzas de seguridad a realizar tareas de prevención en fuentes digitales abiertas, en el ciberespacio. La pregunta que se intentará responder en esta tesis es si esta medida de investigación afecta la intimidad de las personas.

En este contexto, se entiende que el autor Byung Chul Han, filósofo surcoreano contemporáneo, puede ayudar a repensar la manera en que tradicionalmente se respondería a este interrogante. El autor es crítico de la implementación tecnológica como herramienta del capital. Parte del análisis de que el discurso de la transparencia domina el arco político y, bajo el lema de lucha contra la corrupción y la libertad de información, se esconde una falta de confianza social y una apuesta por la vigilancia y el control como método sistémico de coacción.

La idea central de esta tesis versará respecto a cómo el ciberpatrullaje, en un contexto de "panóptico digital", podría provocar en una intromisión violatoria del derecho a la intimidad de los ciudadanos. La hipótesis que se plantea es que la carencia de su regulación legislativa como técnica de prevención e investigación penal podría implicar una afectación inconstitucional. Es por ello que el objetivo de este trabajo será evaluar si su utilización, mediante la inteligencia artificial, redunda en mayor vigilancia y control social, en detrimento de garantías constitucionales.

Para esto, en primer lugar, se abordará el concepto de transparencia, su origen histórico y su desarrollo actual. A modo de ejemplo, se hará mención al método de implementación y las consecuencias que trajo el sistema de videovigilancia y

reconocimiento facial en la Ciudad Autónoma de Buenos Aires (CABA), desde la idea desarrollada por Byung Chul Han en su libro *La sociedad de la transparencia*[1].

Luego, se desarrollará el pensamiento de Byung Chul Han a partir de sus obras *La sociedad de la transparencia, Psicopolítica: neoliberalismo y nuevas técnicas de poder*[2], *La topología de la violencia*[3] y *En el enjambre*[4], las cuales serán el esquema de pensamiento y marco teórico crítico.

Posteriormente, se describirán algunas innovaciones en materia de investigación penal como inteligencia artificial, *machine learning*, etcétera. A partir de eso, se abordará la discusión actual referente a la búsqueda de la verdad en el marco del proceso penal, pues se entiende que asistimos a un cambio de paradigma de la mano de los descubrimientos tecnológicos en la averiguación criminal. En consecuencia, lo que se concibe por verdad procesal penal será nuevamente puesto en discusión, en tanto estos avances posibilitarán como nunca antes la reconstrucción de esa "verdad histórica u objetiva".

Por esto, resultará imprescindible determinar conceptualmente cuál es la verdad procesal penal por averiguar, para establecer límites y metodologías claras en su búsqueda, principalmente para las agencias a cargo de la prevención y persecución del delito.

Luego, se abordarán cuestiones referentes al ciberpatrullaje como método de investigación policial, la reciente regulación normativa y la posible afectación al derecho constitucional a la intimidad[5], desde el marco teórico de Byung Chul Han. Se explicarán las razones por la que se entiende que su aplicación requiere de la sanción de una ley formal o, en el caso concreto, de autorización judicial.

Para finalizar, se elaborará una conclusión respecto a los peligros inherentes a la falta de regulación, la posible afectación al derecho a la intimidad y la necesidad de redefinir este concepto para adecuarlo al nuevo contexto. Con el presente se buscará, en

[1]HAN, *La sociedad de la transparencia* (Traducción a cargo de Raúl GABÁS), 1 ed., Herder, Barcelona, 2013.
[2]HAN, *Psicopolítica: neoliberalismo y nuevas técnicas de poder* (Traducción a cargo de Alfredo BERGÉS),1ed., Herder, Barcelona, 2014. Disponible en: https://onx.la/6665d [Enlace verificado el día 11 de septiembre de 2024].
[3]HAN, *Topología de la violencia* (Traducción a cargo de Paula KUFFER), 1 ed., Herder, Barcelona, 2016. Disponible en: https://is.gd/OQdBq4 [Enlace verificado el día 11 de septiembre de 2024].
[4]HAN, *En el enjambre* (Traducción a cargo de Raúl GABÁS), 1 ed., Herder, Barcelona, 2015. Disponible en: https://is.gd/SSJVA3 [Enlace verificado el día 11 de septiembre de 2024].
[5]Artículos número 1,18,19,33 y 75 inciso 22 de la Constitución Nacional, 12 de la Declaración Universal de los Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos.

definitiva, realizar un aporte teórico y práctico para demostrar los riesgos que conlleva esta metodología de investigación y prevención, que sirva como aporte a la discusión jurisprudencial.

II) Transparencia

A) Orígenes y concepto

La ONG *Transparency* Internacional emparenta el concepto de transparencia con el de la lucha contra la corrupción, específicamente, con el poder de la ciudadanía en el acceso a la información[6]. De igual forma, es descripto en el portal oficial del Estado Argentino. Allí, se describe la cualidad de transparencia en la gestión pública como una de las bases fundamentales de la democracia, pues enarbola el deber de los poderes públicos que componen al Estado de rendir cuentas a la ciudadanía respecto a su accionar[7].

Así, en el año 2016, se sancionó la ley 27.275[8] como un método preventivo de lucha contra la corrupción dentro del Estado [9]. Pese a estar emparentados, no es lo mismo hablar de transparencia que del derecho al acceso a la información pública[10].

Pero este concepto no es nuevo, sino que se remonta a tiempos pasados, donde se plasmó la necesidad de contar con gobiernos donde reinen las leyes y no los hombres, tanto en la Antigua Grecia como en China. Desde Adam Smith en *La riqueza de las naciones*, a Kant, enalteciendo el respeto a la ley para la conformación de una sociedad y Rousseau, en su desdén del secreto como característica propia de los regímenes injustos, todos contribuyeron a la formación del concepto de transparencia que hoy conocemos[11].

Sin embargo, fue Jeremy Bentham el primero en nombrar el concepto de transparencia a finales del siglo XVIII. Este, en el Código Constitucional de 1830 estableció la creación de un "Tribunal de la Opinión Pública" cuyos integrantes tenían la función de proporcionar a la ciudadanía las estadísticas o datos requeridos, para llevar a

[6]Disponible en: https://is.gd/XZgXbu [Enlace verificado el día 11 de septiembre de 2024].
[7]Disponible en: https://is.gd/R0Ahl9 [Enlace verificado el día 11 de septiembre de 2024].
[8]Disponible en: https://is.gd/UUFWlu [Enlace verificado el día 11 de septiembre de 2024].
[9]Hasta el año 1994, se entendía que el derecho de acceso a la información pública estaba contenido implícitamente los artículos número 1, 14 y 33 de nuestra Constitución Nacional (CN). Al incorporar a través del art. 75 inc. 22 de la CN los tratados internacionales de derechos humanos y otorgarles jerarquía constitucional, el derecho al acceso a la información pública pasó a ser un deber derivado de la libertad de expresión (véase en BASTERRA, *Acceso a la información pública y transparencia*, 1 ed., Astrea, Buenos Aires, 2018, pp. 1-10).
[10]El primero responde a un método por el cual se brinda la información de determinada forma a la ciudadanía y el segundo refiere al derecho que tienen los ciudadanos de obtener esa información. (Véase en AGUILAR RIVERA, "Transparencia. ¿nueva o vieja?*", Transparencia y Democracia. Claves para un concierto*, Capítulo 1, p. 1 (https://is.gd/0cjLuO; última visita: 11 de septiembre de 2024).
[11]Idem, p. 2.

cabo los juicios contra el accionar de los funcionarios públicos[12]. Pero, su mayor reconocimiento fue a partir del desarrollo del panóptico[13]. Para el autor, mientras más vigilados estamos mejor nos comportamos.

B) La sociedad de la información

El Dr. Sueiro describe el paso de la sociedad analógica del siglo XX a la de la información, caracterizada por el impacto y la influencia de la informática[14]. Esta última es aquella que está estrictamente vinculada con el avance de las Tecnologías de la Información y la Comunicación (TIC)[15], como por ejemplo, la web 2.0, los juegos multiusuario, las redes sociales y la moneda digital o criptomoneda, entre otras[16].

Debido a esta revolución tecnológica, los jóvenes son llamados nativos digitales, pues perciben la realidad social y el mundo a través de las pantallas que transmiten los datos, la información y las noticias de lo que sucede[17].

En consecuencia, la cantidad de información y datos recopilados es inmensa. El grado de dependencia que tienen los seres humanos actualmente para el desarrollo de sus actividades es, por momentos, alarmante. Desde que se despiertan hasta que se acuestan, están en constante uso de los dispositivos electrónicos que van recabando sus datos. Difícilmente se podría imaginar la realidad sin su uso, ya sea para trabajar como para relacionarse. Esta dinámica los ha expuesto a los ojos de los demás de una forma nunca vista, ya que la información se recopila y su privacidad se desmorona ante el caudal de datos que no para de crecer.

Combinando esto con las revelaciones de Julián Assange y Edward Snowden respecto a cómo los servicios de inteligencia los espían, a través de las interacciones con estos dispositivos (mensajes, correos electrónicos, chats, redes sociales y programas de geolocalización), el resultado es preocupante[18].

---

[12]Idem., p. 3.
[13]Aquel "establecimiento propuesto para guardar los presos con más seguridad y economía, y para trabajar al mismo tiempo en su reforma moral, con medios nuevos de asegurarse de su buena conducta, y de proveer a su subsistencia después de su soltura" (véase en BENTHAM, *Tratado de legislación Civil y Penal*, Traducción a cargo de Ramón SALAS, 1 ed., México, Edigráfica, 2004, Tomo VI, p. 201).
[14]SUEIRO, *Vigilancia Electrónica y otros modernos medios de prueba*, 2 ed. Hammurabi, Buenos Aires, 2019, p. 42.
[15]Son "(…) como herramientas para acceder, recuperar, guardar, organizar, manipular, producir, intercambiar y presentar información por medios electrónicos; estos incluyen hardware, software y telecomunicaciones en la forma de computadores y programas, tales como aplicaciones multimedia y sistemas de bases de datos" (véase en DOBRATINICH, *Derecho y nuevas tecnologías*, 1ed., La Ley, CABA, 2021, p. 420).
[16]Idem, p. 39.
[17]SUEIRO, *Vigilancia…,* op. cit., p. 43.
[18] Idem, p. 44.

Así, la sociedad de la información, mediante el concepto de transparencia como principio rector, conduce hacia un horizonte desconocido, donde la posibilidad de control y vigilancia, a través de la utilización de los datos, podría ser moneda corriente. Por esto, resulta imprescindible ahondar en una férrea defensa de los derechos constitucionales en estos entornos.

C) La cuarta revolución industrial y el principio de transparencia

En la actualidad, de la mano de las nuevas tecnologías, se abre paso a una nueva era donde el almacenamiento y el procesamiento de datos son claves para el desarrollo económico-social. Los avances en inteligencia artificial, robótica y nanotecnología, entre otros, son los cimientos de la cuarta revolución industrial, caracterizada por la conexión entre miles de millones de personas a dispositivos móviles[19].

Gerard Wajcman realiza una interesante reflexión que describe la característica principal de una nueva cultura en esta nueva fase industrial: la máquina de ver. La caracteriza como una época donde todo está sometido a la luz plena y debe ser visible, para necesariamente ser visto. La cultura de ver —científica, tecnológica, policial, médica o de espionaje— es masiva y, el autor, advierte que en la hipermodernidad la sociedad va camino hacia la transparencia, donde no haya nada que escape a la luz y donde existe una mirada que vigila y controla. Para él, "(…) un ojo sin párpado está sobre el mundo. La mirada es nuestro nuevo Leviatán"[20].

Para explicar el paradigma de la transparencia, Wajcman hace referencia a un estudio científico. En el año 2007, un grupo de investigadores del Instituto de Biología de Anfibios de la Universidad de Hiroshima, aplicó ingeniería genética sobre una rana blanca albina japonesa, para volverla transparente. De esta forma, podían observar el desarrollo de sus órganos y, eventualmente, saber cómo afectan al organismo determinadas sustancias. Destaca el autor que, con este experimento, se buscó a un enemigo interior —el desarrollo de un cáncer, por ejemplo— dentro de las ranas para vigilar su futuro. Es decir, la transparencia dejó de ser solo la cualidad de transparente para incorporar una instancia más de observación y vigilancia. A partir de esto, Wajcman se pregunta si este ensayo no avizora el futuro del género humano y, si eventualmente, no seremos todos virtualmente visibles[21].

[19]BOTTO, "La cuarta revolución industrial una visión economicista del cambio social", *Question/Cuestion*, Vol.2,2020, p.5 (https://is.gd/pnufhx; última visita: 11 de septiembre de 2024).
[20]WAJCMAN, *El ojo absoluto* (traducción a cargo de Irene AGOFF),1 ed., Manantial, Buenos Aires, 2011, pp. 17/21.
[21]Idem, p. 26.

En esa línea, para definir el concepto de transparencia, hace especial énfasis en la nueva cultura: verlo todo. Así, define que el salto característico de esta nueva era es una concepción positivista donde el hombre sería un objeto y es aquí donde esta concepción tiene una característica política amenazante, esto es, la tiranía de la transparencia[22].

Concluye, que la sociedad se encuentra en un presente donde la vida privada, como la entendemos, pierde sentido y es urgente resignificarla como valor predominante en el desarrollo de los individuos. En sus palabras "(…) nos hallamos en estado de legítima defensa de la vida privada donde lo íntimo es sacado por la fuerza para obtener del sujeto su verdad"[23].

D) La sociedad de la transparencia de Byung Chul Han

En todo su trabajo Byung Chul Han[24] analiza las características actuales de esta revolución tecnológica y las implicancias que está generando en la sociedad.

En *La sociedad de la transparencia*, el autor detalla los matices propios que presenta. En su razonamiento, la doctrina imperante de la transparencia —relacionada con la libertad de información— domina el discurso político y no se circunscribe únicamente a la economía y a la política, sino que se trata de un cambio de paradigma exigente y totalizador[25].

En primer lugar, hace referencia a que el ingreso de esta idea totalizante elimina la negatividad —entendida esta como obstáculo al flujo de información o capital— para dar paso a una sociedad positiva operacional, sometida constantemente a procesos de cálculo, dirección y control. Al no existir negatividad, no se reconoce un "otro" o extraño pues todo se expresa a través del dinero. La sociedad transparente es "un infierno de lo igual"[26].

De esta forma, la transparencia opera como una coacción sistémica que cambia todos los procesos sociales, con el objeto de recrearlos como operaciones y, así, acelerarlos. En su parecer, este procedimiento busca objetivizar al ser humano (a través de una masa de datos e información incalculable) hasta convertirlo en una mera pieza fungible de una operación y, para lograrlo, lo despoja de toda singularidad que actúe como un obstáculo en el proceso. Allí, reside su violencia[27].

[22]Idem, p. 33.
[23]Idem, pp. 41-44.
[24]Disponible en: https://is.gd/1CCHfw [Enlace verificado el día 11 de septiembre de 2024].
[25]HAN, "*La sociedad…*", op. cit, p. 5.
[26]Ibídem.
[27]Idem, pp. 5-10.

Esta positividad, daría paso a una sociedad cuyas "cosas" (los seres humanos) se exponen a diario para poder ser, pues sólo adquieren valor al ser vistos. En este juego, cada individuo es "su propio objeto de publicidad" y se somete a una "coacción icónica" para transformarse en una imagen, haciendo sospechoso a quien no se allane a la luz. Afirma que se vive en la "tiranía de la visibilidad"[28].

Asimismo, detalla que este mecanismo aspira a eliminar cualquier estado de asimetría y para ello, necesita suprimir el secreto como técnica cultural que contiene profundidad. También, prescinde de todo ritual y ceremonia que se interpone en su dinámica operacional, en pos de la aceleración de los ciclos de información, comunicación y producción. Continúa describiendo que el mundo transparente es un mercado donde se exponen como mercancías las intimidades. Lo íntimo funciona como método de exposición mercantilista y, a la vez, como cebo para presentar únicamente, a quien se expone, la versión del mundo que se acomoda a sus intereses[29].

La sociedad íntima se vale de la confesión, mediante el desnudamiento, la falta de distancia y la exposición constante, para acelerar el flujo de información. La sociedad del control basa su subsistencia en el éxito de la coacción interna del sujeto, que cede su intimidad y esfera privada en la necesidad de exhibirse sin vergüenza[30].

E) Un caso testigo: la implementación del Sistema de Reconocimiento Facial de Prófugos en CABA y sus efectos

En el año 2009, en virtud de las facultades otorgadas al Registro Nacional de las Personas (RENAPER) mediante la ley 17.671[31], se sancionó el decreto número 1501/09[32] mediante el cual se lo autorizó —en su artículo 1º— a utilizar tecnologías digitales para la identificación de ciudadanos, con el objeto de emitir nuevos documentos nacionales de identidad. El 4 de marzo de 2011, el RENAPER firmó un convenio con la Policía Federal Argentina (PFA) para dotarla de la información obtenida, a raíz de la tramitación de los documentos nacionales de identidad.

Ese mismo año, a través del decreto número 1766/11[33], se creó el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS). Al año siguiente, se celebró otro convenio entre el Ministerio de Justicia y Seguridad de la CABA y su homónimo de

[28]Idem, p. 13-16.
[29]Idem, p. 23-38.
[30]Idem, p. 54.
[31]Disponible en: https://is.gd/LVAWKe [Enlace verificado el día 11 de septiembre de 2024].
[32]Disponible en: https://is.gd/hKO0dO[Enlace verificado el día 11 de septiembre de 2024].
[33]Disponible en: https://is.gd/F2NklW [Enlace verificado el día 11 de septiembre de 2024].

la Nación, para que puedan efectuar consultas biométricas en tiempo real en el SIBIOS. Posteriormente, se sancionó la ley número 5688[34] que creó el Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires, que luego fue modificada por la ley número 6339[35]. Esta, en su artículo número 9º, establece como principio rector la transparencia, implementando mecanismos eficaces y eficientes para tutelar y proteger la seguridad pública.

Así, a través de la Resolución número 398/19[36], se creó el Sistema de Reconocimiento Facial de Prófugos (SRFP). Este funcionaría cruzando las distintas bases de datos para detectar —mediante la utilización de las cámaras instaladas y los datos biométricos de las personas— a toda persona requerida judicialmente, con el objeto de lograr mayor eficacia en su búsqueda. Los fundamentos de su creación se basaron en que: i. el sistema de videovigilancia tenía como principio rector la utilización de nuevas tecnologías e innovación, para mejorar la gestión institucional en materia de seguridad pública y dotarla de mayor transparencia y ii. de acuerdo a la ley número 25.326[37], no era necesario el consentimiento del titular del dato cuando este se obtenga de fuentes de acceso público irrestricto y se recabe para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

A raíz de su puesta en marcha, el Observatorio de Derecho Informático Argentino (ODIA) presentó un recurso de amparo contra su implementación. Basó su solicitud en que su puesta en funcionamiento no estuvo precedida de una evaluación en materia de protección de datos y, en consecuencia, no era posible establecer el impacto y la afectación de los datos personales y otros derechos de los ciudadanos.

A consecuencia de esa petición, se resolvió declarar la inconstitucionalidad del artículo 1º de la Res. 398/19, entendiendo que la implementación se llevó a cabo sin los recaudos legales pertinentes y se declaró la nulidad de todo lo actuado por el Ministerio de Justicia y Seguridad de la CABA, por haber violado el artículo número 3 del Anexo de la Resolución mencionada, es decir, no contar con orden judicial constatable. Por último, se supeditó la puesta en marcha del sistema a la constitución y debido funcionamiento de los órganos de control[38].

[34]Disponible en: https://is.gd/6atI2m [Enlace verificado el día 11 de septiembre de 2024].
[35]Disponible en: https://is.gd/xihrut [Enlace verificado el día 11 de septiembre de 2024].
[36]Disponible en: https://is.gd/k5J9rJ [Enlace verificado el día 11 de septiembre de 2024].
[37]Disponible en: https://is.gd/QBzCXK [Enlace verificado el día 11 de septiembre de 2024].
[38]JCAyT Nº 4 "ODIA y otros contra GCBA s/amparo", 7/9/22 (expediente número 182908/2020).

En lo que aquí importa, se comprobó que existieron discordancias entre los registros del Sistema de Consulta Nacional de Rebeldías y Capturas (CoNaRC) y los datos biométricos que fueron requeridos al RENAPER por el Ministerio de Justicia de CABA. De acuerdo con la normativa, para enviar esos datos e incorporarlos al sistema de reconocimiento facial, el pedido debía fundarse en una orden judicial. Al respecto, la Sra. Jueza explicó que de acuerdo con la información recabada de la causa al 25/4/19 el listado del CONARC era de 35.000 a 40.000 personas pero que —conforme lo informado por el RENAPER— durante el periodo de 2019 hasta 2022 las solicitudes efectuadas por el citado ministerio fueron de 9.900.282, principalmente en los años en que el sistema estuvo inactivo por la pandemia de COVID19.

En resumen, el Ministerio accedió, manipuló y posteriormente eliminó —mediante 17 usuarios no identificables con una persona humana— de forma ilegal los datos biométricos de millones de personas no incluidas en la base de datos y los utilizó con fines inciertos. Además, se comprobó que 15.459 personas fueron cargadas en el sistema para ser buscadas. Del listado que se acompañó como anexo a la resolución, se desprende que los perjudicados fueron dirigentes políticos, sociales y gremiales, como así también magistrados y funcionarios del Poder Judicial de la Nación, del Ministerio Público Fiscal de la Nación y de la Defensoría General de la Nación, entre otros[39].

La Cámara[40] confirmó el resolutorio y ordenó que, antes de rehabilitar el SRFP, correspondía llevar a cabo investigaciones y pruebas en el *software*, para determinar si tenía un impacto diferenciado según las características personales de los individuos. Además, agregó que la imagen de una persona —en los términos del art. 3 de la ley Nº 1.845— es un dato personal. Resaltó que la falta de transparencia y la omisión de actuar conforme a la propia regulación que establecía el sistema resultó un acto violatorio de los derechos constitucionales de los ciudadanos (intimidad, privacidad, honor, imagen e identidad) y que no había justificación para las discrepancias numéricas producidas por la migración de datos.

Respecto a su constitucionalidad, entendió que había una colisión entre el servicio esencial de seguridad pública y los derechos constitucionales de los ciudadanos (no discriminación, privacidad, intimidad, presunción de inocencia, libertad ambulatoria y protección de datos personales). Hizo especial referencia a que el ámbito de la privacidad

[39]Disponible en: https://is.gd/wXqKAo [Enlace verificado el día 11 de septiembre de 2024].
[40]CATyRC, Sala I, "Observatorio de Derecho Informático y otros c/GCBA s/amparo y otros", 28/4/23 (expediente 182908/2020).

no comprende únicamente a aquel que se desarrolla dentro de los domicilios privados, sino que abarca las acciones que se realiza de modo reservado —con la intención de no exhibirse— fuera del domicilio[41]. Así, dejaron asentado que, para evaluar la invasión en la esfera de la intimidad, debía tenerse en cuenta si la medida respondió a criterios de necesidad, adecuación y proporcionalidad.

Especial mención se hizo a un planteo donde se sostuvo que el SRFP es un sistema de vigilancia masiva. Al respecto, mencionó que no admitir el planteo no implicaba necesariamente avalar mecanismos de seguridad de tinte autoritarios y que la falta de controles en la implementación resultaba un obstáculo insalvable para analizar la medida y no incurrir en esferas de poder constitucionalmente denegadas al Poder Judicial. Para concluir, se hizo alusión a que la hipotética eficacia y eficiencia de la medida podría dar lugar a una eventual revisión jurisdiccional.

A consecuencia de estos dos precedentes, la Procuración de Investigaciones Administrativas (PIA) tomó conocimiento y detalló que desde el año 2019 hasta el 2022 el Ministerio de Justicia y Seguridad de CABA había efectuado 18.320.988 consultas y eso no se condecía con los 40.000 prófugos que había en los datos del CONARC, por lo que entendió conducente, iniciar una denuncia penal por violación de los artículos números 157 y 157 bis del Código Penal. Al final del dictamen, hizo especial referencia a que se consultaron los registros obrantes en el RENAPER de 84 magistrados[42].

Se resalta este caso, para dar una muestra de cómo actúa la lógica cultural de la transparencia en la aplicación de métodos de investigación penal, sus consecuencias y el trato que se le puede dar a los datos personales. Además, se introdujo uno de los temas que se abordarán con posterioridad, referente al derecho a la intimidad que tienen los ciudadanos en espacios públicos. No se puede dejar de destacar que, la puesta en marcha del SRFP, en la práctica significó la afectación a derechos constitucionales de la sociedad que derivó en la obtención de los datos biométricos de muchas personas.

Una reflexión tuvo el Dr. De Luca —cuyos datos biométricos emigraron mediante este sistema— al ser consultado por medios periodísticos. Aquel manifestó que "hay gente que juega a esto como si estuviera en el Tinder. O juegan a la Play Station con los ciudadanos. No se puede vivir así. No vivimos en una sociedad transparente. Tenemos

[41]CSJN "Spinosa Melo, Oscar Federico", 5/9/06 (Fallos 329:3617).
[42]Disponible en: https://is.gd/g09Y1u [Enlace verificado el día 11 de septiembre de 2024].

que poder mantener en reserva lo que cada uno quiera. No puede estar todo expuesto. No hay ninguna sociedad que pueda funcionar así"[43] (el resaltado es propio).

Como se mencionó, mediante la utilización de sistemas tecnológicos, bajo el lema de la eficacia y eficiencia en la investigación criminal para "tutelar y proteger la seguridad pública", se violaron los datos biométricos de personas con fines inciertos hasta ahora, pero con una certeza: la transparencia es total.

III) El pensamiento de Byung Chul Han

En este apartado, se desarrollarán las nociones fundamentales del pensamiento del autor, con el objeto de establecer un marco teórico que posibilite el análisis que se hará en los siguientes capítulos. Se elaborará un breve resumen conceptual de sus obras —que se complementan con el libro citado anteriormente— para detallar las nociones básicas de lo que denomina "psicopolítica", "topología de la violencia" y "enjambre digital".

A) Psicopolítica: neoliberalismo y nuevas técnicas de poder

En este libro, Han desarrolla el concepto de "psicopolítica", como una nueva fase del sistema de explotación neoliberal caracterizado por un sujeto de rendimiento que se explota voluntariamente, en nombre de la libertad individual[44].

Para él, esta "libertad individual de poder hacer" no es más que una coacción encubierta, donde el ser humano se emplea así mismo en pos de la producción y el rendimiento. La psicopolítica es esta coacción que afecta la libertad. Su característica principal reside en una vigilancia pasiva y un control activo, operando como un dispositivo de dominación que afecta la psiquis del individuo y lo condiciona en forma prerreflexiva. Así, mediante este engaño, el capital se expande a través de la comunicación ilimitada y el uso de los datos personales que los sujetos entregan diariamente. No coacciona ni prohíbe, sino que hace creer al sujeto que para ejercer plenamente esa libertad es necesario contar su vida. Así, se vale de esos datos para alimentarse constantemente, haciendo que los sujetos sean dependientes[45].

Según el autor, las personas están inmersas en un panóptico digital, que vigila y controla constantemente lo que hacen, cuya eficiencia está asociada a esta necesidad

[43]Ibídem.
[44]Es aquél sujeto obligado a rendir que "se ha liberado de las instancias externas de dominio que lo fuerzan a trabajar y lo explotan. Solo está sometido a sí mismo. Pero con la desaparición de instancias dominantes externas no se elimina la estructura coercitiva, sino que lo que sucede entonces es que libertad y coerción pasan a identificarse (…) se somete libremente a la presión para maximizar el rendimiento. Así es como se explota a sí mismo. El explotador es al mismo tiempo el explotado, a la vez verdugo y víctima, señor y vasallo" en HAN, *La sociedad del cansancio* (traducción a cargo de ARREGI), 1 ed, Herder, Barcelona, 2012, pp. 58-59. Disponible en: https://is.gd/R6vH6j [Enlace verificado el día 11 de septiembre de 2024].
[45]HAN, *Psicopolítica*…, op.cit., p. 29.

interior de volcar sus vidas en planos virtuales. Así se vigilan y controlan así mismos inaugurando una crisis de libertad novedosa, que afecta la voluntad libre[46].

En este panóptico las personas no se sienten vigiladas o amenazas, ya que no es necesario el uso de la tortura para obtener sus secretos. Ahora, se desnudarán en forma voluntaria en las redes, donde se incentiva la exposición de las emociones. El sistema logra llegar a lo profundo de las personas y, valiéndose de eso, las hace vigilarse otorgando sus datos[47]. El autor, continúa describiendo que el uso del b*ig data* —donde las elecciones, preferencias y decisiones se evidencian como datos— permite adquirir un conocimiento pleno de las acciones pasadas, presentes y tiene la facultad de hacer pronósticos de los comportamientos futuros. De ese modo, el futuro comienza a ser predecible y controlable para quien disponga de esta herramienta[48].

A su vez, entiende que el concepto de protección de datos resulta ser obsoleto para este sistema, pues ralentiza su circulación, comunicación y, consecuentemente, la del capital[49], a la vez que menciona que este dispositivo augura el fin de la libertad. A través del *big data* —que solo acumula y no olvida— hasta sería posible establecer patrones de comportamientos colectivos inconscientes. La consecuencia social de este sistema es la clasificación de las personas en datos, que se comercializan en el mercado[50].

A partir de esto, el autor plantea que debería reinventarse el concepto de libertad, para escapar de esta trampa. La libertad, necesariamente, es la posibilidad de las personas de realizarse unas con otras y allí reside su negatividad para el sistema, pues obstruye el ciclo de información y obtura el desarrollo del capital[51].

B) La topología de la violencia

En *La topología de la violencia* el autor parte del concepto de psicopolítica y de sujeto de rendimiento para redefinir las características propias del ejercicio de la violencia en la modernidad.

Menciona que, en la edad antigua, la utilización de la violencia como método de ejercicio del poder era de afuera hacia adentro, es decir, externa. A esta metodología la llama macrofísica del poder, dado que implicaba una relación entre dos personas, donde una se impone a la otra —por medio de la infiltración, invasión y/o infección— y roba su

[46] Idem, p. 25.
[47] Idem, p. 61.
[48] Idem, p. 25.
[49] Ibídem.
[50] Idem, p. 98.
[51] Idem, p. 13.

libertad, sin su consentimiento. La violencia se aplicaba, pero no era interiorizada por el sometido[52].

Tanto el poder como la violencia son fenómenos de la negatividad, entonces, son consecuencia de una dialéctica interior-exterior que la precede y le da un sentido constitutivo[53]. De esta manera se presenta la relación negativa que obstruye la circulación: existe una persona que piensa y actúa diferente. Para Han, la característica de la sociedad actual es su positivización donde la dinámica violencia-poder explícita —al vivir de la relación de negatividad— va perdiendo cada vez más espacio. Entonces, se va diluyendo esa relación de negatividad porque la "lucha" es interior[54]. Pero esto no significa el fin de la violencia sino una nueva modalidad, donde esta toma una forma psíquica interior: a través del exceso de positividad, se expresa dentro del sujeto en modo implícito e implosivo y lo coacciona. A esta nueva forma de obligar Han la denomina microfísica del poder[55].

El autor explica que este pasaje denota una manera distinta de ejercer la violencia pues, ahora, esta es sistémica y positiva y a diferencia de la macrofísica —que aparece en la falta— esta se produce en la abundancia de comunicación, creada por la necesidad de poder todo, que desinterioriza al sujeto dispersándolo constantemente en un sinfín de actividades que lo llevan a la hiperactividad[56]. La sociedad disciplinaria de Foucault, con el biopoder como forma de administrar los cuerpos, dejó de existir y asistimos a la nueva sociedad del rendimiento[57].

En conclusión, el cambio topológico de la violencia radica en que esta dejó de ser una parte trascendente en el ejercicio de la comunicación política y social para ser ejercida en el interior —en la psiquis— de cada individuo.

C) En el enjambre

En el enjambre Han describe el cambio de paradigma que estamos viviendo a través del medio digital. Menciona el autor, que nos encontramos en una era sin respeto (al que define como mirar hacia atrás), pilar fundamental de lo público pues presupone

[52] HAN, *Topología…*, op. cit, p. 51.
[53] Idem, p. 56.
[54] Idem, p. 9.
[55] Idem, p. 57.
[56] Idem, p. 64.
[57] "La sociedad disciplinaria de Foucault, que consta de hospitales, psiquiátricos, cárceles, cuarteles y fábricas, ya no se corresponde con la sociedad de hoy en día. En su lugar se ha establecido desde hace tiempo otra completamente diferente, a saber: una sociedad de gimnasios, torres de oficinas, bancos, aviones, grandes centros comerciales y laboratorios genéticos. La sociedad del siglo XXI ya no es disciplinaria, sino una sociedad de rendimiento…" (véase en Han, *…del cansancio*, op. cit., p 17).

una mirada distanciada para con la otra persona. En la actualidad, mediante la exposición constante de la intimidad, por medio de las redes sociales se destruye esa distancia, entre lo íntimo y lo público, favoreciendo la producción privada de información. Desde esa lógica, afirma que transitamos una era donde no existe la privacidad, porque siempre estamos expuestos a una mirada de algo o alguien[58].

Para el autor, asistimos a una crisis de masas que da paso a un enjambre digital de puras unidades. El *homo digitalis* se desarrolla en el entorno digital en forma aislada, no forma parte de una masa constitutiva y tampoco tiene posibilidad de acción en términos colectivos. Está acompañado y comunicado, pero solo. Al dejar de ser receptor de información, el individuo la produce y consume a todo momento, pero de forma privada[59].

Así, la lógica de la transparencia, exige la accesibilidad inmediata e irrestricta en la respuesta e información. Este sistema coactivo, es fortalecido constantemente por las redes sociales y la utilización de teléfonos inteligentes, generando en el sujeto una relación de carácter obsesivo[60].

Concluye su obra afirmando que la sociedad, en vez de basarse en la confianza, construye sus relaciones en base al control y la vigilancia. Pues "(c)ada clic que hago queda almacenado. Cada paso que doy puede rastrearse hacia atrás. En todas partes dejamos huellas digitales. Nuestra vida digital se reproduce exactamente en la red. La posibilidad de una protocolización total de la vida suplanta enteramente la confianza por el control. En lugar de Big Brother aparecen los big data (grandes datos). La protocolización total, sin lagunas, de la vida consuma la sociedad de la transparencia"[61].

IV) Investigación mediante el uso de recursos tecnológicos

La revolución tecnológica ha creado un nuevo lugar donde se desarrollarán las principales actividades delictivas: el ciberespacio[62].

Los Estados, a fin de luchar contra la "ciberdelincuencia", han desarrollado el Convenio de Budapest. En su preámbulo, este detalla que tiene por objeto la creación de una política penal común para combatir la ciberdelincuencia, creando para ello una legislación adecuada que garantice la cooperación internacional y el desarrollo de las tecnologías de la información. Su finalidad es incrementar la eficacia en las

[58] Han, *Enjambre…*, op. cit., p. 15.
[59]Idem, pp. 29-30.
[60]Idem, p. 60.
[61]Idem, p.101.
[62]Según la Real Academia Española es el "ámbito virtual creado por medios informáticos". Disponible en: https://is.gd/wGNZaG [Enlace verificado el día 11 de septiembre de 2024].

investigaciones y procedimientos penales, permitiendo la utilización de medios especiales en materia de delitos informáticos, armonizando el ejercicio de la acción penal y el respeto de los derechos humanos fundamentales[63].

Nuestro país, mediante la ley número 27.411[64], lo aprobó, con algunas reservas, y desde el año 2017 forma parte de nuestra legislación. Desafortunadamente, y pese a haber sido ratificado, en el ámbito federal principalmente no se ha cumplido con la obligación de legislar procesalmente cómo deben llevarse a cabo materialmente estas medidas de investigación. Esto trae como principal consecuencia que, en el marco de una investigación penal de este tipo, los agentes judiciales se amparen en una interpretación amplia del concepto de libertad probatoria que rige en materia penal[65], lo cual podría acarrear vulneraciones a los derechos constitucionales[66].

En este capítulo, se mencionarán algunas de estas metodologías y sus principales características, con el objeto de evidenciar las posibles afectaciones a garantías constitucionales y dar una breve perspectiva del contexto actual en materia de investigación penal.

A) Allanamiento remoto y uso de drones

El allanamiento remoto es una forma de acceder —a distancia— a un dispositivo informático, con el objeto de obtener los datos privados (pasados, presentes o predecir comportamientos futuros) de su usuario[67].

Para llevarlo a cabo, se utiliza un *software*[68] que, mediante el envío de un correo electrónico o un mensaje de texto al celular de la persona imputada, introduce un *malware* con un *exploit* (programa o código), para vulnerar la seguridad del dispositivo y sustraer la información, sin alterar o perturbar su funcionamiento[69].

---

[63]Fue sancionado en noviembre de 2001 por el Consejo de Europa y en 2004 entró en vigencia https://is.gd/flGESw [Enlace verificado el día 11 de septiembre de 2024].
[64]Disponible en: https://is.gd/O6zmb7 [Enlace verificado el día 11 de septiembre de 2024].
[65]"…todo hecho, circunstancia o elemento (…) objeto del procedimiento (…) puede ser probado (…) por cualquier medio de prueba" (véase en MAIER, "*Derecho Procesal Penal. Tomo I. Fundamentos*", 2da. Ed., Editores del Puerto, Buenos Aires, 1996 y p. 864).
[66]Máxime si tenemos en consideración que el artículo número 30 del Pacto de San José de Costa Rica limita la aplicación de nuevas metodologías de investigación, en tanto establece que el alcance de las restricciones al goce y ejercicio de los derechos y libertades allí reconocidas, no pueden ser aplicadas sin el dictado de una ley por razones de interés general y con el propósito para el cual ha sido establecida.
[67]STRATIOTIS, "Los allanamientos remotos y el uso de drones", en DUPUY, *Innovación en investigaciones digitales*, 1ed., Hammurabi, Buenos Aires, 2022, p. 451. Disponible en: https://is.gd/U6xtyz [Enlace verificado el día 11 de septiembre de 2024].
[68]Para la RAE un software es un "conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora". Disponible en: https://is.gd/AixIv9 [Enlace verificado el día 11 de septiembre de 2024].
[69]STRATIOTIS, Los allanamientos, op. cit. pp. 457/460.

Empero, actualmente existen nuevos métodos para obtener la información a distancia, sin necesidad de enviar un correo electrónico. En Argentina, se desarrolló un mecanismo —proyecto "Crozono"— que registra los dispositivos mediante la utilización de un *software* (instalado en un dron o robot) que accede a la red de *wi-fi* de la persona que está siendo investigada[70].

En cuanto a su tratamiento jurisprudencial, existen algunos precedentes internacionales que han analizado esta clase de allanamientos. El Tribunal Supremo de España entendió que la utilización de binoculares sin autorización judicial —para observar el interior de un domicilio— resultaba una injerencia indebida y una intromisión al derecho de la inviolabilidad del domicilio. En lo que hace a la utilización de drones, expresó que la protección constitucional frente al acceso a un domicilio abarcaba las intromisiones físicas y virtuales. A su vez, mencionó que la revolución tecnológica ha generado el nacimiento de nuevas herramientas de investigación con alcances ilimitados, que previamente deben ser autorizadas por un juez[71].

A su vez, la Corte Suprema de Estados Unidos, en "Florida v. Riley"[72] y "California v. Ciraolo"[73], decidió por mayoría que la inspección policial mediante el uso de un helicóptero o un avión, sin autorización judicial previa, no era una pesquisa en los términos de la 4ta. enmienda y, en consecuencia, no estaba amparada por la garantía de inviolabilidad del domicilio, pues bajo esas condiciones el imputado no tenía una expectativa razonable de privacidad. Especial mención corresponde hacer al voto disidente, ya que en ambos casos se destaca que los avances tecnológicos permiten una injerencia en espacios constitucionalmente protegidos, que está más allá de una intromisión física, y requiere de una interpretación que se amolde a esta nueva realidad.

En nuestro país también se ha tratado esta cuestión; así, en "Sandoval y otros"[74], se resaltó la tensión entre el aumento de eficacia en las investigaciones por el uso de estas

[70]El procedimiento, se basa en aprovechar alguna debilidad del sistema de conexión ocasionada intencionalmente (por ejemplo: un corte de luz). Cuando se reinicia la conexión, al intentar vincularse nuevamente los dispositivos electrónicos a la red, el dron registra el usuario y contraseña, para acceder a toda la información que posee el dispositivo mientras esté prendido (véase en Idem, pp. 460/464).

[71]TRIBUNAL SUPREMO DE ESPAÑA, Sala de lo penal, "Evelio, Ildefonso e Rosana por el delito de tráfico de sustancias estupefacientes", 20/4/2016, STS 1709/2016. Disponible en: https://is.gd/avKli4 [Enlace verificado el día 11 de septiembre de 2024].

[72]CORTE SUPREMA DE ESTADOS UNIDOS, "Florida v. Riley", 23/1/89. Disponible en: https://is.gd/h9bC6L [Enlace verificado el día 11 de septiembre de 2024].

[73]CORTE SUPREMA DE ESTADOS UNIDOS, "California v Ciraolo", 19/5/1986. Disponible en: https://is.gd/K1A7ls [Enlace verificado el día 11 de septiembre de 2024].

[74]CÁMARA DE APELACIONES DE GENERAL ROCA, "Sandoval y otros", 12/8/21 (FGR 787/2021/CAI). Disponible en: https://is.gd/V6MQtX [Enlace verificado el día 11 de septiembre de 2024].

herramientas y el derecho a la intimidad de los ciudadanos. Bajo esa tesitura, se entendió que era necesaria una autorización judicial previa para captar imágenes del patio de un domicilio mediante la utilización de un dron. A su vez, en otro precedente[75], se ratificó la exclusión de fotos obtenidas mediante un dron de un patio particular por ausencia de autorización judicial y se recomendó el uso prudente y cuidadoso de estas herramientas, con participación activa de órganos jurisdiccionales para evitar intromisiones ilegítimas. En sentido contrario, en "SG"[76] por mayoría, se determinó que la utilización de un dron para instrumentar tareas de inteligencia en un domicilio no era equiparable a un allanamiento, por lo que no había necesidad de autorización judicial previa. Además, se dejó abierta la posibilidad de tomar fotografías satelitales o por cámaras de monitoreo.

En conclusión, la ventaja que tienen estos métodos de acceso remoto es obvia, pues obsta del ingreso al domicilio y secuestro de los elementos que luego serán peritados. Su utilización provee evidencia en tiempo real ocultando a su propietario que está siendo investigado, lo que puede resultar beneficioso para vigilarlo, perseguir a otros implicados y recopilar información para prevenir la comisión de nuevos delitos.

B) Videovigilancia con vehículos aéreos no tripulados

En los últimos tiempos, ha tomado notoriedad el uso de vehículos aéreos no tripulados para tareas de videovigilancia. Su empleo es habitual en operativos policiales, recitales, sucesos deportivos o eventos masivos, con fines preventivos. Es una nueva metodología de vigilancia estatal para recolectar y tratar datos a gran escala, ya sea para prevenir, sancionar delitos o como prueba en el proceso penal. Los drones poseen tecnología de avanzada que permite, entre otras cosas, captar las caras de las personas que están siendo filmadas, vía reconocimiento facial[77].

Desafortunadamente, no existe regulación procesal que establezca la forma en que debe utilizarse, los límites y la necesidad de una orden judicial para su utilización.

C) Sistema de reconocimiento facial

Actualmente, el sistema de reconocimiento facial tomó notoriedad por sus beneficios en materia de seguridad ciudadana, ya que posibilita la localización en tiempo

[75]CÁMARA DE APELACIONES Y GARANTÍAS EN LO PENAL DE BAHÍA BLANCA, Sala I, "NN", 6/11/2019, Expediente IPP 17673/I. Disponible en: https://is.gd/hX0bfl [Enlace verificado el día 11 de septiembre de 2024].
[76]CÁMARA FEDERAL DE MAR DEL PLATA, "SG",15/5/19, causa nro. FMP 1110/2017. Disponible en: https://is.gd/JgYTPo [Enlace verificado el día 11 de septiembre de 2024].
[77]LABANCA, "Videovigilancia y uso de vant en el marco de investigaciones penales en la argentina" en DUPUY "*Innovación…*" op. cit., pp. 481-483.

real de personas con pedido de captura, además de ser utilizado como elemento probatorio en una investigación penal.

Se trata de una nueva herramienta tecnológica, que funciona a través de un algoritmo a base de inteligencia artificial. Para identificar a una persona, compara sus rasgos y contornos faciales, establece un "patrón facial del rostro" y lo coteja con los datos biométricos obrantes en su base de datos[78].

De todos modos, continúa el debate por su inclusión en las pesquisas, debido a los riesgos en términos de vigilancia, control social y las eventuales afectaciones a derechos constitucionales.

D) Vigilancia electrónica por inteligencia artificial

La política sanitaria de lucha contra la propagación del virus COVID-19 trajo consigo la implementación de métodos de vigilancia electrónica, asistidos por inteligencia artificial, a través de las TICs[79].

Los avances en materia de investigación no se han quedado atrás. Se han desarrollado métodos de vigilancia electrónica tanto para controlar al imputado mientras transita su proceso en libertad, como para investigarlo. En nuestra legislación procesal penal federal está prevista como un tipo de morigeración de prisión preventiva (art. 210 inc. i del CPPF), pero es probable que en un futuro pase a ser un método de investigación. Anteriormente, hubo un intento infructuoso por incluirla de ese modo, mediante el Proyecto de Reforma del Código Procesal Penal (ley 27.063)[80]. Pese a esto, la falta de regulación autónoma de la prueba y evidencia digital fue la principal razón por la que resultaron excluidas: la técnica legislativa careció de cuestiones imprescindibles, a la hora de armonizar los métodos de investigación con las garantías constitucionales[81].

Las cuestiones planteadas resultan imprescindibles para poder ser utilizadas sin poner en peligro las garantías constitucionales de los ciudadanos. Ahora bien, la llegada de la inteligencia artificial abre la posibilidad de procesar datos con una velocidad sobrehumana. De ser empleada para investigaciones penales, su regulación resulta imperiosa para no avasallar los derechos y garantías que conocemos de un estado democrático de derecho.

---

[78]CINOCI, ¿Queremos la tecnología de reconocimiento facial al servicio de la investigación penal?, en Idem, pp. 536-538.
[79]SUEIRO, *Vigilancia…*, op. cit. p. 28.
[80]Allí, se incluyeron cinco variantes de vigilancia electrónica: acústica, sobre comunicaciones electrónicas, remota sobre equipos informáticos, por captación de imágenes y a través de dispositivos de seguimiento y localización (cfr. artículo número 175 y ss.) en Idem, p. 143.
[81]Idem, p. 148-175.

E) La inteligencia artificial aplicada a la investigación penal

Los antecedentes que más se asemejan a lo que hoy conocemos como inteligencia artificial son dos invenciones de la empresa IBM (*Deep Blue* y *Watson*), antecesores en el intento de recrear la inteligencia humana mediante el uso de la tecnología, pese a que aún hoy existe controversia al respecto[82].

La definición que más consenso tiene es que "los sistemas de inteligencia artificial (IA) son sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido. Los sistemas de IA pueden utilizar normas simbólicas o aprender un modelo numérico; también pueden adaptar su conducta mediante el análisis del modo en que el entorno se ve afectado por sus acciones anteriores"[83]. En esa línea, los sistemas de inteligencia artificial se basan en lógica algorítmica[84].

Tanto el *machine learning* como el *Deep learning* son sistemas de aprendizaje basados en algoritmos. El primero consiste en una máquina que aprende constantemente de sí misma y, para tomar una decisión, aplica lo asimilado. El segundo, utiliza una estructura de red neuronal artificial similar a la humana. Combinados con la incalculable información existente en la nube (a través del b*ig data y el data mining)*[85], la inteligencia artificial posee una capacidad incalculable de información para procesar, clasificar y calcular[86].

[82]PASTOR/HAISSINER, *Neurociencias, tecnologías disruptivas y tribunales digitales*, 2 ed., Hammurabi, Buenos Aires,2019, pp.61-64. Disponible en: https://is.gd/63ZIcd [Enlace verificado el día 11 de septiembre de 2024].
[83]DANESI, *Inteligencia artificial, tecnologías emergentes y derecho 1*, 1 ed, Hammurabi, Buenos Aires, 2020, p. 41. Disponible en: https://is.gd/zfhYiq [Enlace verificado el día 11 de septiembre de 2024].
[84]Los algoritmos son un conjunto metódico de pasos que pueden emplearse para hacer cálculos, resolver problemas y alcanzar decisiones. No es un cálculo en sí mismo, son los pasos que se deben seguir para hacer la operación (véase en KIEFER, "Daño informático", en DUPUY, *CIBERCRIMEN*, 1º Ed., B de F., Buenos Aires, 2018, p. 318).
[85] El *big data* es el "conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios" y el *data maining* es el "proceso en el que se analizan grandes volúmenes de datos con el fin de hallar patrones que expliquen su comportamiento en un contexto determinado". Disponible en: https://is.gd/LSWk0d y https://is.gd/dVDE6u, respectivamente [Enlaces verificados el día 11 de septiembre de 2024].
[86]PASTOR/HAISSINER, *Neurociencias…*, op. cit. p. 66.

Ahora bien, actualmente existen sistemas de inteligencia artificial que se aplican en la investigación y la prevención del delito, mediante la utilización de algoritmos. Uno de ellos es el *software* de predicción criminal *Predpol*, capaz de procesar información relevante a través de datos (reportes criminales, denuncias, estadísticas, *modus operandi*, etcétera), que permite establecer con precisión estadística los lugares en donde es posible que se produzcan hechos delictivos[87]. En esa línea, en Estados Unidos de Norteamérica se utiliza el sistema *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) para predecir —mediante un *software* estadístico— el riesgo de reincidencia de un imputado, evaluar su libertad en el proceso y determinar el *quantum* de una pena[88].

Este tipo de herramientas pueden resultar muy eficaces para la prevención de delitos, pero también proveen a las autoridades policiales de facultades de investigación y vigilancia sin precedentes. Por eso, la recopilación y el análisis de los datos obtenidos en la red, en conjunción con la falta de transparencia algorítmica[89] pueden ocasionar sesgos y resultar un instrumento de cuantiosa peligrosidad si no es utilizado correctamente.

F) Consideraciones finales

En resumen, las nuevas tecnologías aportarán novedosas formas de investigación, con mayor eficacia y agilidad para el desarrollo de las pesquisas. Pero, mediante la aplicación de sistemas de inteligencia artificial a través del procesamiento masivo de datos, será posible predecir conductas futuras individuales o colectivas bajo un rigor estadístico sin precedentes. Así, asegurar su ejecución conforme a los principios y directrices de un Estado Constitucional de Derecho y armonizar su funcionamiento con el principio de tutela judicial efectiva será de suma importancia.

Este nuevo paradigma trae aparejado un viejo desafío de larga data: lograr el equilibrio entre la búsqueda de la verdad y la aplicación de la ley como fin del proceso y el respeto de las garantías constitucionales de los individuos. Este no es menor, pues resulta trascendental para elaborar a futuro un sistema procesal penal con un evidente fin

[87]DANESI, *Inteligencia…*, op. cit. p. 89.
[88]Idem, p. 71.
[89]"Esto es, que el proceso de toma de decisiones del sistema basado en IA sea transparente y auditable para poder tener garantías de que no viola derechos fundamentales de los usuarios, y que, si así lo hicieran, o provocaran algún tipo de efecto no deseado o perjuicio sobre los usuarios, que existan las herramientas legales que aseguren la responsabilidad sobre distintos tipos de daños y/o efectos" en Idem, p. 66.

antropocéntrico, respetuoso de los deberes, derechos y garantías emanados de la Constitución Nacional.

V) La verdad como fin del proceso penal

En este capítulo se mencionará el relato histórico que desarrolla Foucault para explicar el concepto de verdad y sus implicancias en la construcción de los métodos de validación. Esto resultará de interés para el abordaje posterior de determinados conceptos, en particular la implicancia que tiene en las garantías constitucionales la búsqueda de la verdad sin límites y la inclusión en el proceso penal de elementos probatorios obtenidos bajo esa lógica.

A) Una historia de la verdad

Según Foucault, la verdad tiene una historia y, para abordarla, debemos partir de que el conocimiento no está presente en la naturaleza humana, sino que fue inventado. Nietzsche, al negar la existencia de Dios como intermediario de esa relación, entiende que el conocimiento es producto de un juego, de una disputa y, por ende, para entenderla debemos saber cuáles son las relaciones de poder y de lucha[90].

En esa línea, Foucault utiliza como ejemplo el desarrollo de las prácticas judiciales que dieron origen a la indagación y el examen como métodos de averiguación de la verdad, condicionando las prácticas sociales y la ciencia. Para demostrarlo, hace referencia al modo de descubrirla a través del tiempo.

En la Grecia Antigua, la verdad se obtenía a través de un juego, prueba o desafío reglado entre dos personas: una lanzaba un reto y, si otra lo aceptaba, la palabra final la tenía Dios. Pero, a través del relato de Edipo, se inauguró un nuevo método de investigación de la verdad llamado la ley de las mitades y, a partir de esto, se crea el *mito de Occidente*, donde la verdad no pertenece al poder político, sino que proviene del testimonio[91]. En el Derecho Germánico, previa invasión del Imperio Romano, los conflictos se regían por un duelo o juego de prueba, como modo de hacer la guerra[92]. Y en el derecho feudal, existió un sistema que no tenía como objetivo investigar la verdad, donde las partes ofrecían los elementos probatorios, los aceptaban y se sometían a ellos[93].

[90]FOUCAULT, *La verdad y las formas jurídicas* (Traducción a cargo de LINCH), 5ta. ed., Gedisa, Barcelona, 2017, p. 20. Disponible en: https://is.gd/tHQ11z [Enlace verificado el día 11 de septiembre de 2024].
[91]Idem, pp. 43-81.
[92]Idem, p. 79.
[93]Idem, p. 71.

A partir de la segunda mitad de la Edad Media se impone nuevamente la indagación, pero con connotaciones diferentes. Este nuevo método de averiguación de la verdad nace para asegurar la circulación de los bienes en el comercio y la concentración del poder en el monarca, por sobre los señores feudales. Así, aparece como nuevo actor el poder judicial y se inaugura un método diferente a los conocidos[94].

Para esto, se inicia un procedimiento de autentificación de la verdad basado en la prueba de verificación, para obtener la confesión, como único elemento. De esta forma, a través del modelo eclesiástico —de la *inquisitio generalis y especialis*— se instauró un proceso judicial reglado como ejercicio del poder, para controlar las almas y los bienes[95]. A finales del siglo XVIII y comienzos del XIX, nace lo que el autor denomina como la "sociedad disciplinaria", edificada en el concepto de peligrosidad[96]. En lo que hace a la forma de la obtención de ese saber, operó su trasladó desde la indagación al examen mediante vigilancia caracterizado por la falta de trascendencia del hecho histórico, donde la importancia residía en establecer una vigilancia ininterrumpida para formar y transformar a los individuos[97].

De esta forma, el autor retoma el concepto de Nietzsche para hacer notar que tanto la indagación como el examen fueron métodos de construcción de saber-poder que fueron revisados, pues no existe la relación de sujeto-objeto por fuera de ese entendimiento. Y que, es por esa razón que los métodos de averiguación de la verdad en el proceso judicial fueron variando a través del tiempo.

Ahora bien, surgen los interrogantes referentes al significado de la verdad en el proceso penal, el tipo de verdad que se busca, su influencia en los métodos de averiguación y las posibles consecuencias para las garantías constitucionales de los individuos. A continuación, se intentará responderlos.

B) Concepto de verdad procesal

Pese a las distintas definiciones, el proceso penal consiste, en términos prácticos, en un método para averiguar qué sucedió, en qué tiempo, lugar y bajo qué condiciones.

---

[94]Las partes deberán someterse a un poder exterior que administrará el conflicto, el soberano será representado por el procurador (quien tendrá a su cargo el ejercicio de la acción) y la infracción generará un daño al gobernante que tendrá el derecho de multar, confiscar bienes y exigir una reparación, para acumular riqueza en Idem, p 78.

[95]Idem, pp. 89-92.

[96]Básicamente, se entiende como la materialización del derecho penal de autor por sobre el derecho penal de acto: el sujeto debe ser considerado por lo que puede, es capaz, o está dispuesto a hacer que por lo que verdaderamente hace. Entonces, hay que controlarlo (con un sinfín de instituciones ajenas al poder judicial) para castigarlo.

[97]FOUCAULT, *La verdad…*, op. cit. p. 104.

Para esto, se deberá constatar que ciertas situaciones efectivamente sucedieron y, así, determinar si la reconstrucción de los hechos es verdadera.

Sin embargo, la verdad siempre ha sido difícil de definir, pues se trata de un concepto metafísico[98]. Maier la define como una relación de conocimiento entre un sujeto y un objeto: cuando ese juicio de sentido ya sea por identidad, adecuación o conformidad, culmina de forma exitosa y coincide la verdad ontológica del objeto con la idea que tiene el sujeto de este. Su búsqueda en el proceso penal representa un ideal político del sistema, que puede (o no) ser alcanzado. Pero, su fin primordial es arribar a la paz jurídica para recomponer el conflicto suscitado en el caso[99].

La forma en la que se llega a ese conocimiento, es decir, el método de investigación y sus límites, va a estar determinado por su objeto y el cumplimiento de reglas que hacen a su propia legitimación. Sin embargo, no todos los autores coinciden con esta definición. Algunos entienden que existe una dicotomía entre "verdad formal" y "verdad material", haciendo énfasis en lo que se comprueba judicialmente y lo que realmente sucedió. Otros plantean que existe una "verdad relativa", producto del proceso judicial y una "verdad absoluta" ajena a este.

Guzmán, sostiene que existe mucha confusión en la dicotomía verdad material/formal cuando se la asocia a un método determinado. Así, subraya que hay una percepción de que existe un modelo procesal "bueno" donde la verdad no es un valor en sí mismo y uno "malo", donde la verdad es un valor y se relaciona con los procesos inquisitivos. El autor explica que renunciar a los procedimientos de índole inquisitivos no implica renunciar a la búsqueda de la verdad como valor[100].

Pese a esto, Maier entiende que la diferencia no es conceptual, sino que reside en las formas mediante las cuales los diferentes procedimientos regulan la averiguación de la verdad, los límites formales para su investigación y el método de incorporación de la prueba para conocer la verdad histórica[101].

Ahora bien, existen diferentes teorías que intentan contestar el interrogante acerca de qué es la verdad, en el marco de un procedimiento penal. Por un lado, se encuentran

---

[98]AROCENA, *Valoración de la prueba*, 1 ed., Hammurabi, Buenos Aires,2020 (https://is.gd/LsX9gb; última visita el día 14 de agosto de 2024).
[99]MAIER, *Derecho Procesal…*, op. cit., pp. 841-852.
[100]GUZMÁN, *La verdad en el proceso penal: una contribución a la epistemología jurídica*, 2da. Edición, Del Puerto, CABA, 2011, p. 42.
[101]Así, en los procedimientos civiles caracterizados por la búsqueda de una "verdad formal", ésta estará estrictamente limitada por la actuación de las partes en el proceso, a diferencia del proceso penal, donde existe un interés público por saber qué fue lo que "objetivamente" pasó, sin importar la voluntad de las partes (véase en MAIER, *Derecho Procesal…*, op. cit. p. 851).

las subjetivas, que establecen criterios para saber si una creencia es verdadera o falsa. Una de ellas es la teoría coherentista, que sostiene que mientras aquello que se asevera forme parte del conjunto de creencias "verdaderas", será indefectiblemente verdad. Otra es la pragmatista, que equipara la verdad a aquello que sea conveniente. Por otro lado, está la consensualista, que supone que un enunciado será verdad siempre que sea asentido por los demás[102].

En la vereda opuesta, se encuentran las teorías de la verdad como correspondencia, que sitúan su origen en la lógica aristotélica y en la búsqueda de una verdad absoluta, o en su intento. Esta corriente define a la verdad como aquella situación donde un enunciado se ajusta en forma absoluta o perfecta a aquello que esboza. Es decir, algo será verdad, en tanto y en cuanto, esa operación intelectual se corresponda con el enunciado[103].

No es menor esta distinción respecto a qué es la verdad, pues delimitarlo tiene consecuencias en la estructuración del proceso respecto a: el papel de los sujetos intervinientes, el fin a alcanzar, la función de la prueba, los límites para su obtención y la importancia que tendrán las garantías constitucionales.

Por esta razón, se partirá del entendimiento de la verdad como correspondencia descripta, teniendo en especial consideración la calidad del valor epistemológico de la teoría y la correlación de la realidad con la prueba objetiva de un procedimiento. Además, implica reconocer implícitamente el principio de estricta legalidad y estricta jurisdiccionalidad, en tanto parte de la concepción semántica del concepto, y ello resulta nodal para el desarrollo de las garantías penales y procesales. Si se parte de la base de una teoría de tipo utilitarista o pragmática, al desconocerse esta relación sujeto-objeto en términos probatorios, la arbitrariedad y ganancia del más fuerte en el proceso serían frecuentes, por estar condicionada a un fin de mayor entidad[104].

Ferrajoli relata con precisión lo mencionado precedentemente. Su modelo garantista consta de dos elementos constitutivos: uno que hace a la definición legal (convencionalismo penal y estricta legalidad) y otro ligado a la comprobación jurisdiccional de la desviación punible (cognoscitivismo procesal y estricta jurisdiccionalidad)[105]. En esa línea, son las garantías penales y procesales las que

[102]GUZMÁN, *La verdad…,* op. cit, pp. 51-65.
[103]Idem, p. 64.
[104]Idem, p. 75.
[105]En cuanto al primero, explica que la desviación punible es aquella que se define por ley y habilita la imposición de una pena (*nulla poena et nullun crimen sine lege*), pero siempre sobre un hecho empírico y objetivo, que debe ser probado, desligado de condiciones subjetivas del autor (*nulla poena sine crimine et sine culpa*). De ahí, extrae dos consecuencias importantes: la esfera de libertad de hacer todo aquello que

instrumentan los límites a los cuales tiene que estar ligado el ejercicio del poder punitivo para garantizar la legitimidad de la pena a imponer, desde un punto de vista epistemológico, y evitar la arbitrariedad en la toma de decisiones. Por esa razón, representan no solo garantías de libertad sino también garantías de verdad[106].

Para evitar que la construcción de esa verdad sea dependiente de la correlación de fuerzas ligada al poder —como describió Foucault— resulta de vital importancia partir de un modelo garantista, que asuma la búsqueda de una verdad en los términos mencionados y actué como garantía de libertad y verdad del ciudadano. Su objetivo será minimizar al máximo la arbitrariedad y el ejercicio ilegítimo de violencia en la actividad jurisdiccional, con el fin de darle legitimidad política y contribuir al desarrollo de un Estado de Derecho, por sobre los resabios de carácter absolutista.

C) El fin del proceso penal

Usualmente, se define al proceso penal como un medio para aplicar la ley sustantiva y averiguar la verdad. Para la mayoría, el único objetivo es el ejercicio de la jurisdicción pero se olvidan de una parte trascendental: respetar los derechos fundamentales de las personas, conforme lo dispone la Constitución Nacional[107].

Se adhiere a esta afirmación, toda vez que el respeto de los derechos fundamentales hace a la legitimación política constitucional del sistema. Si esto no fuera así y la búsqueda de la verdad fuera el exclusivo objetivo del proceso, los derechos fundamentales evidenciados en las garantías serían meras declaraciones formales, desoyendo las principales razones que dieron origen a la Constitución Nacional. Esta última exige eliminar la arbitrariedad, ejercer la jurisdicción con un sentido de verdad que tenga correlación epistemológica, respete sus normas y los derechos que enuncia.

En materia penal, esta búsqueda está ligada a un sistema de garantías cimentado por valores morales, que no permiten la obtención y valoración de los elementos probatorios de cargo violando los derechos individuales, pues, la verdad procesal no puede ser a cualquier precio[108].

---

no se encuentra prohibido por ley y la igualdad jurídica de las personas, por cuanto se castigan hechos y no personalidades. Del segundo, explica que el hecho descripto en la ley debe ser probado (*nulla poena et nulla culpa sine uidicio*), con la posibilidad de ser rebatido por la persona acusada (*nullum iudicium sine probatione*) (véase en FERRAJOLI, *Derecho y razón. Teoría del garantismo penal* (Traducción a cargo de IBAÑEZ/RUIZ/BAYÓN/BASOCO/BANDRÉS), 1 ed., Trotta, Madrid, 1995, pp. 34-37.

[106]Idem, p. 40.

[107]GUZMÁN, *La verdad…*, op. cit., pp. 123/4.

[108]COPPOLA/CAFFERATA NORES, *Verdad procesal y decisión judicial*, 1 ed., Alveroni, Córdoba, 2014, pp. 7-16. Disponible en: https://is.gd/Y1LuAO [Enlace verificado el día 11 de septiembre de 2024].

Así, de la misma forma que dota al investigador de normas para llevar a cabo su función, existen otras que están dirigidas a proteger al ciudadano del ejercicio arbitrario e injusto por parte del Estado[109]. En efecto, nuestra normativa prohíbe y sanciona la producción, obtención e incorporación de pruebas cuando se violentan estos intereses y, en algunos casos, extiende su alcance nulificante a sus consecuencias o derivados. Como se mencionó en el cuarto capítulo, para comprobar un hecho la regla es la libertad probatoria y las prohibiciones probatorias son sus excepciones.

En esa línea, la Corte Suprema de Estados Unidos creó la regla de exclusión como una herramienta para afianzar la vigencia de los derechos de los ciudadanos contra intromisiones estatales irrazonables. Luego, para definir su alcance, elaboró la doctrina del fruto del árbol venenoso, que proyecta la ilegalidad inicial de un procedimiento, a todos los elementos probatorios (frutos) que fueran obtenidos en violación a los preceptos constitucionales, pese a que su procedencia sea legítima en sí misma[110].

En nuestro medio, la CSJN receptó la regla, basándose en un argumento de carácter prioritariamente ético, bajo la premisa de que no corresponde que el Estado obtenga pruebas violando la ley, pues afecta la moral y la seguridad jurídica. Además, con posterioridad, se hizo notar que era inválido otorgarle valor a la prueba obtenida producto de un delito para sustentar una sentencia, porque esto implicaba beneficiarse de una ilegalidad y afectaba la buena administración de justicia[111]. Respecto a su alcance y el destino de los efectos obtenidos mediando una ilegalidad, se aplicó la doctrina del fruto del árbol venenoso creada por su homónima estadounidense[112].

En conclusión, la búsqueda de la verdad como fin del proceso penal es un ideal loable, pero para ser legítimo, debe respetar el modo y los límites que consagra nuestra Constitución Nacional.

Como sostiene Maier, "Lo expuesto hasta ahora demuestra (…) la necesidad de reafirmar la inadmisibilidad de la valoración judicial de aquella prueba inmediata o mediatamente adquirida mediante una acción estatal irregular, con total prescindencia de consideraciones complementarias, como la gravedad del hecho atribuido al investigado,

[109]GUZMÁN, *La verdad…*, op. cit. p. 128.
[110]CORTE SUPREMA DE ESTADOS UNIDOS, "Weeks v. United States" y "Silverthorne Lumber Co. v. United States", 24/2/14 y 26/6/20, respectivamente.
[111]CSJN, "Charles Hermanos y otro", del 5/9/1989 (Fallos 46:36), "Montenegro, Luciano Bernardino s/robo", del 10/12/1981 (Fallos 303:1938) y "Fiorentino, Diego Enrique s/tenencia ilegítima de sustancia estupefaciente", de fecha 27/11/1984 (Fallos 306:1752), entre otros.
[112]CSJN "Francomano" (Fallos. 310:2402), "Daray" (Fallos 317:1985), "Paulino" (Fallos 528;46); "Rayford" (Fallos 308:733) de fechas 19/11/89; 22/12/94;17/9/2013 y 13/5/86, respectivamente.

o el error del agente de la persecución penal sobre la ilicitud de su actuación. Ello aún más frente a las tendencias deformantes del procedimiento penal, que hoy son percibidas claramente, y que amplían las facultades de injerencia estatal a niveles que, poco tiempo atrás, no hubieran sido imaginables, tales como la introducción del ´agente encubierto´ en varias legislaciones, **o el desarrollo de nuevos métodos de vigilancia electrónica**"[113] (el resaltado es propio).

En el próximo capítulo, se dedicará a explicar la razón por la cual el ciberpatrullaje, como medida de investigación penal para averiguar la verdad, debe ser sometido a normas legislativas que limiten su alcance y establezcan la forma en que se puede utilizar. Sin esta limitación, cualquier elemento probatorio obtenido podrá ser excluido del proceso por violar la intimidad de la persona investigada.

VI) Ciberpatrullaje

A) Concepto

De la misma forma en que una persona puede dejar sus huellas dactilares cuando toca un objeto con la mano, su interacción constante en el ciberespacio deja rastros o *huellas digitales*. Estas representan aquello que hace dentro de la red, expresando y transmitiendo un historial cierto y preciso que posibilita el desentrañamiento de su intimidad personal[114].

El proceso de recolección, análisis y uso de esa información en la interacción social, se conoce como SOCMINT (*social media intelligence*). La recolección en fuentes abiertas, sin la necesidad de esconderse, es uno de sus géneros y se denomina OSINT (*open source intelligence)*. Es decir, mediante este procedimiento se recolecta y analiza la huella digital de una persona con el propósito de hacer inteligencia criminal, comercial, laboral, etcétera[115].Asimismo, algunos autores diferencian entre ciberpatrullaje y ciberinvestigación, de acuerdo a si se desarrolla con o sin control judicial, respectivamente[116].

[113]MAIER, *Derecho Procesal Penal. Tomo 3. Parte general. Actos procesales*, 1 ed, Del Puerto, CABA, 2011, p. 126.
[114]VANINETTI, *Derecho a la intimidad en la era* digital, vol. 3, 1º ed,, Hammurabi, Buenos Aires, 2021, p. 128. Disponible en: https://is.gd/2g7Y6v [Enlace verificado el día 11 de septiembre de 2024].
[115]CANDIOTTO/ARGIBAY MOLINA, *Ciberpatrullaje*, 1 ed., Hammurabi, Buenos Aires, 2020, p. 30. Disponible en: https://is.gd/8K9vAf [Enlace verificado el día 11 de septiembre de 2024].
[116]RIOS, "Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras",IDP,Nº36,2022,p 3 (https://is.gd/TxxiJ3; última visita: 11 de septiembre de 2024).

Más allá de sus diferentes propósitos, el presente análisis se concentrará en su utilización por agentes policiales para ciberpatrullar. Al respecto, existen diferentes definiciones, que buscan abarcar con precisión y exactitud su contenido.

La Policía Federal Argentina, define al ciberpatrullaje como la búsqueda de información en fuentes abiertas y públicas del ciberespacio[117]. Para la doctrina, representa las actividades que lleva a cabo la policía para vigilar, prevenir y evitar la comisión de delitos en fuentes abiertas o la práctica de vigilancia de la huella digital, centrada sobre las comunicaciones, visitas a determinados dominios, archivos subidos en redes sociales, entre otros[118]. Tiene fines preventivos e investigativos de ciertos delitos (el terrorismo, tráfico de drogas, trata de personas y pornografía infantil) y se emparenta con la actividad del agente encubierto[119]. Además, comprende las actividades de rastreo y sondeo de contenidos que llevan a cabo las agencias policiales y del Estado en el medio cibernético abierto[120].

Argibay Molina y Candiotto lo describen como "una práctica de indagación en fuentes abiertas de información, que se realice con fines de prevención general de delitos y sin vinculación a investigaciones concretas"[121]. La alocución a la prevención general excluye la persecución de los ciudadanos por ideas expresadas en fuentes abiertas y determina que solo deberá ser utilizada en forma general, bajo parámetros objetivos que lo justifiquen. Esta definición obliga al investigador a no inquirir a un individuo en particular ni a un hecho concreto y, por último, permite hacer una distinción entre las actividades de ciberpatrullaje y la utilización de OSINT con fines de inteligencia, vedado por la ley 25.520[122].

Se considera que esta última definición resulta la más acertada, pues establece límites claros al ejercicio de esta modalidad y permite diferenciar las actividades de prevención general de las de inteligencia criminal. La importancia en definir exhaustivamente su significado está ligada a que conlleva repercusiones al momento de evaluar su legalidad. Partiendo de esta definición, se comenzará a desarrollar algunas cuestiones que son necesarias para determinar su alcance.

---

[117]CANDIOTTO/ARBIBAY MOLINA, *Ciberpatrullaje*, op. cit, p. 53.
[118]BENTIN, "El agente encubierto en el ciberespacio: la ausencia de regulación en la argentina y su impacto en las garantías constitucionales" en DUPUY "*Innovación…*" op. cit., p 420.
[119]VANINETTI, *Derecho…*, op. cit., p. 92.
[120]TAVOLA SERRA, "Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje", *IDP*, 2022, p. 21 (https://is.gd/8Ghl05; última visita:11 de septiembre de 2024).
[121] CANDIOTTO/ARBIBAY MOLINA, *Ciberpatrullaje*, op. cit., p. 54.
[122]Idem, p. 53.

B) Datos que pueden ser objeto de SOCMINT/OSINT.

Definido el concepto, se enumerarán los datos disponibles en estas fuentes, para que se entienda con amplitud el tipo de información que puede ser obtenida mediante estas tareas.

Se debe considerar que, con la llegada de las aplicaciones y las redes sociales, la información personal dejó de ser privada o de acceso restringido. Lo que las personas hacen, dicen, ven y hablan está registrado y forma parte de sus huellas digitales que eventualmente pueden buscarse.

Mediante la utilización de las técnicas —OSINT y SOCMINT— un policía podría obtener sin mayores dificultades los siguientes datos de una persona: DNI, CUIL/CUIT, domicilio, teléfono, círculo de amigos, familiares, trabajo, deportes que realiza, lugares que frecuenta, transportes que utiliza, gustos, hábitos, rutinas, situación financiera, entre otros. Todos estos datos están registrados en las aplicaciones que las personas utilizan a diario.

De acuerdo a la ley 25.326, mediante esta técnica pueden ser recolectados datos personales, que detallan información de cualquier tipo referente a personas físicas o de existencia ideal determinada o determinables, y datos sensibles, que revelan el origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual[123]. Esto significa que, un cúmulo de información que años atrás era considerada de índole privada, hoy se encuentra en la red y puede ser monitoreada, procesada y recolectada por personal policial.

Pese a esto, no existe consenso respecto a qué es un dato proveniente de una fuente abierta. Para algunos, es toda la información con acceso público en internet y para otros, puede abarcar también a aquélla que se puede obtener sin el uso de medidas coercitivas

[123]Asimismo, con fecha 30/11/2022, mediante la ley nro. 27.699, se aprobó el Convenio 108+ que es "…una versión modernizada del Convenio 108 (…) y constituye el único instrumento multilateral de carácter vinculante en materia de protección de datos personales, que tiene por objeto proteger la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos. Algunos de los puntos más destacados (…) son: se reconocen nuevos derechos para los titulares de datos. Se actualizan los mecanismos de transferencias internacionales. Se amplía el concepto de datos sensibles, pasando a incluir datos genéticos y biométricos. Se obliga a informar incidentes de seguridad. Se incorporan requisitos más estrictos respecto a los principios generales sobre tratamiento de datos, como el principio de proporcionalidad, de minimización de datos y licitud. Se incluye condiciones especiales para el tratamiento de datos personales de niños y niñas. Se refuerza la exigencia de la destrucción o anonimización de datos personales". Disponible en: https://is.gd/A8LPOQ [Enlace verificado el día 11 de septiembre de 2024].

para su acceso[124]. Argibay Molina y Candiotto, aclaran que diferenciar entre una fuente pública y una privada no es una tarea fácil, pero resulta nodal para dilucidar si se afectaron derechos fundamentales. Para los autores, existen tres niveles de acceso a fuentes: i. libres (a las que se accede sin impedimentos de ningún tipo como el Boletín Oficial), ii. semipúblicas y no pagas (las que se necesita registrarse para acceder a determinada información como Linkedin) y iii. semipúblicas y pagas (que requieren registrarse y pagar para acceder a la información). Así, conciben que la implementación del ciberpatrullaje, sin un marco regulatorio con límites claros, puede ser riesgoso[125].

Todo esto dificulta en la práctica su caracterización, resultando difuso determinar si se está ante un dato de una fuente pública o no. Sin embargo, a raíz del incesante crecimiento de datos que existe en este tipo de fuentes, las fuerzas policiales han comenzado a darle importancia, tanto para investigar a una persona identificada como para prevenir delitos. Así, se ha comenzado a desarrollar y utilizar sistemas, plataformas y herramientas —en algunos casos mediante inteligencia artificial— para mejorar la capacidad de los usuarios y automatizar la búsqueda[126].

Finalizadas estas aclaraciones, se hará mención a la regulación del ciberpatrullaje en nuestro país y la situación actual.

C) Su regulación en Argentina.

En el año 2018, la ex Secretaría de Seguridad de la Nación —mediante la resolución número 31-2018— dispuso que las fuerzas policiales y de seguridad debían intervenir en hechos presuntamente delictivos cometidos en fuentes abiertas. En la normativa, se hizo hincapié en que las tareas estaban justificadas por la situación de emergencia —COVID 19— y las facultades policiales para intervenir ante la comisión o sospecha de actividades ilícitas (artículos números 183 CPPN y 243 CPPF). Por esa razón, eran tareas de investigación que no requerían de autorización judicial, a diferencia de las tareas de inteligencia criminal[127]. Para su ejercicio, estableció los principios de actuación

[124]SALT/POLANSKY, La investigación penal en el entorno digital, vol. 3, 1 ed,, Hammurabi, Buenos Aires, 2023, p. 138. Disponible en: https://is.gd/VWk10E [Enlace verificado el día 11 de septiembre de 2024].
[125]CANDIOTTO/ARBIBAY MOLINA, *Ciberpatrullaje*, op. cit. p. 53.
[126]SALT/POLANSKY, *La investigación…*, op cit. p.125.
[127] Definió al ciberpatrullaje como las "tareas de prevención policial del delito en el espacio cibernético …" que "…se llevarán a cabo únicamente mediante el uso de fuentes digitales abiertas, entendiéndose por tales a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales…". En su artículo 1º instruía a "…a tomar intervención (…) en (…) Venta o permuta ilegal de armas por Internet. Venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito. Hechos

a los que debía someterse[128], agregando que debía respetarse la ley de datos personales, el derecho a la libertad de expresión, la criminalización de la protesta en línea, entre otros.

D) Repercusiones críticas de los organismos en defensa de los derechos humanos. Resoluciones número 428/24 y 710/2024.

A causa del efecto mediático que generó la resolución número 31-2018 y los cuestionamientos de entidades vinculadas a la defensa de los derechos humanos, se sancionó el "Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas", que se utilizaría en el marco de la emergencia pública de salud[129].

Ante esto, el Centro de Estudios Legales y Sociales (CELS) en el informe "Sobre el Proyecto de protocolo de ciberpatrullaje", solicitó su derogación inmediata. Destacó, que no podía ser considerado un protocolo de actuación por su carácter general y difuso, ya que no definía claramente qué constituían los "actos investigativos" y eso habilitaba las "excursiones de pesca". En particular, detalló que las actividades mencionadas eran tareas de inteligencia criminal sin un mínimo grado de sospecha sustantiva, que habilitaban su producción en cualquier tipo de delitos. Eso evidenciaba que las fuerzas policiales lo utilizaban sin control, pues tampoco se sabía si las tareas eran llevadas a cabo en forma manual o por *softwares* especializados[130].

En esa misma línea, la Asociación por los Derechos Civiles (ADC) expresó su preocupación e hizo saber que un instrumento de este tipo, para ser constitucionalmente válido, requería de una ley formal. Sumado a esto, indicó que el momento de excepción que se vivía no justificaba la criminalización de los discursos en la red y que la inclusión del delito de intimidación pública era alarmante. Además, mencionó que era necesario proteger el anonimato en la protesta online, para garantizar que la red sea un espacio libre

(…) vinculados a la aplicación de la Ley 23737. Difusión de mensajes e imágenes que estimulen o fomenten la explotación sexual o laboral, tanto de mayores como de menores de edad, y que prima facie parecieran estar vinculados a la trata y tráfico de personas. Hostigamiento sexual a menores de edad a través de aplicaciones o servicios de la web. Venta o permuta de objetos que, presumiblemente, hayan sido obtenidos en infracción a las disposiciones aduaneras. Hechos que presuntamente, transgredan lo normado en los artículos 4, 5, 6, 7, 8 y 9 de la Ley 26388. Los actos investigativos deberán limitarse a sitios de acceso público, haciendo especial hincapié en redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de internet, darkweb y demás sitios de relevancia de acceso público (…)". Disponible en: https://is.gd/rHqh1E [Enlace verificado el día 11 de septiembre de 2024].

[128]Entre ellos: i. legalidad (su objeto debían ser las conductas vinculadas a la situación de emergencia y detalladas en el protocolo), ii. necesidad (debía ser utilizada como metodología de prevención si resultaba el medio más adecuado para el fin buscado), iii. proporcionalidad (las tareas debían ser idóneas y necesarias para evitar el peligro ajustándose al logro), iv. razonabilidad (la judicialización debía estar precedida de un análisis del contexto comunicacional en el que se daban) y v. protección de la razonable expectativa de privacidad (se debían omitir todas las actividades que resultaban inherentes al uso de Internet y no evidenciaran una intención de delinquir, sin posibilidad de acumulación de registros).

[129]Disponible en: https://is.gd/HaJ7m6 [Enlace verificado el día 11 de septiembre de 2024].

[130]Disponible en: https://is.gd/CguO21 [Enlace verificado el día 11 de septiembre de 2024].

y seguro para efectuarla; y que la definición dada no tenía la precisión necesaria, porque habilitaba su utilización para un universo muy amplio de delitos, tornándose en una vigilancia masiva. Por último, aconsejó prohibir el uso de bases de datos privadas filtradas en forma ilegal y la utilización del agente encubierto sin autorización judicial[131].

Haciendo eco de estas críticas, mediante la resolución número 720/22, se derogó la norma cuestionada. Entre sus argumentos, se destacó que era necesaria la autorización judicial para llevar a cabo estas tareas, por la tensión generada con el uso y tratamiento de datos personales. Además, se indicó que la recolección en fuentes abiertas no autorizaba la falta de cumplimiento de los requerimientos (calidad de dato, de información, seguridad y confidencialidad) y que el amplio radio de intervención respecto de los delitos perseguidos era excesivo, ya que no tenía vinculación alguna con la emergencia decretada[132].

Desde su derogación hasta el mes de mayo del año 2024, el ciberpatrullaje careció de protocolo específico, sin perjuicio de que se sospecha su utilización como método de investigación por agencias estatales[133].

El 28 de mayo del 2024, el Ministerio de Seguridad publicó la resolución número 428-2024[134] reinstaurando el ciberpatrullaje, dotando a las Fuerzas de Seguridad Federales de herramientas técnico legales adecuadas que simplifiquen sus tareas de investigación. Justificaron su aplicación en la necesidad de generar mecanismos coordinados y proactivos para la investigación policial, ante la expansión de los delitos cibernéticos (artículos números 183 del CPPN, 235 y 243 del CPPF). En su artículo 1º, se precisó que los actos de investigación únicamente debían limitarse a sitios de acceso público (redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de internet y *dark-web*) y espacios de relevancia de acceso público, de acuerdo a la ley de datos personales. Además, se definió a estas fuentes de la misma forma que en la resolución 31-2018 limitando su uso para investigar una amplia gama de delitos y para la búsqueda de personas requeridas por la justicia o extraviadas[135].

---

[131] Disponible en: https://is.gd/QPIZl3 [Enlace verificado el día 11 de septiembre de 2024].
[132] Disponible en: https://is.gd/O76zbW [Enlace verificado el día 11 de septiembre de 2024].
[133]SCHATZKY/ZARA, "Inteligencia basada en fuentes abiertas (OSINT) en Argentina: un diagnóstico sobre su utilización por parte del Estado", *Revista pensamiento penal*, Nº 483,2023 (https://is.gd/88bU6p; última visita: 11 de septiembre de 2024).
[134]Disponible en: https://is.gd/ISPNCX [Enlace verificado el día 11 de septiembre de 2024].
[135]Entre ellos, se menciona narcotráfico, amenazas y otras formas de intimidación o coacción, infracciones a las leyes números 20.429, 26.388, 22.362 y 14.346, venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito u obtenidos en infracción a las disposiciones aduaneras, falsificación y comercialización de instrumentos públicos en sitios web y otros

En los artículos 3º y 4º, se establece que las actividades preventivas deberán adecuarse a la normativa constitucional, utilizarse en fuentes abiertas y judicializarse luego de un análisis comunicacional. Sin embargo, no podrán judicializarse aquellas conductas inherentes al uso de internet (que no evidencien características delictivas) ni acumularse información (la no judicializada deberá ser destruida) y el "agente revelador" deberá contar con autorización judicial. A su vez, se limitó su accionar a la ley de datos personales, quedando prohibido el tratamiento sin autorización judicial de datos sensibles, las publicaciones efectuadas por menores de edad y la interferencia con la libertad de expresión[136].

Por último, se incluyó en su artículo 5º que el uso de *softwares* o cualquier dispositivo o herramienta tecnológica de tratamiento de la información automatizada (basada en inteligencia artificial, aprendizaje automático, sistema experto, redes neuronales, aprendizaje profundo o cualquier otra que en el futuro se desarrolle) se ajustará a las estrictas necesidades de la actividad y deberá ser supervisado por el propio Ministerio.

Posteriormente, con fecha 26 de julio del 2024, se publicó la Resolución nro. 710/24, mediante la cual se creó la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS), con la misión de aplicar inteligencia artificial en la prevención, detección, investigación y persecución del delito y sus conexiones. Sus funciones serán: patrullar las redes sociales abiertas, aplicaciones y sitios de Internet (profunda), identificar y comparar imágenes en soporte físico o virtual, analizar imágenes de cámaras de seguridad en tiempo real utilizando reconocimiento facial, utilizar algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos, identificar patrones inusuales en las redes informáticas y detectar amenazas cibernéticas, procesar grandes volúmenes de datos de diversas fuentes para extraer información útil y crear perfiles de sospechosos o identificar

espacios virtuales, acoso o violencia por motivos de género, amenaza o extorsión de dar publicidad a imágenes o datos no destinados a la publicación o sin consentimiento de quienes figuran en tales imágenes, delitos relacionados con el acoso sexual y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes, trata de personas y tráfico de personas, lavado de dinero, terrorismo, venta libre de elementos para los cuales se requiera autorización o dispensa legal, cualquier otro delito del que se pueda obtener noticia a través del ciberespacio.

[136]Además, se asentó la prohibición de obtener información, producir inteligencia o almacenar datos sobre personas por su raza, fe, acciones privadas u opinión política, emplear métodos ilegales, prohibidos, invasivos y violatorios de la dignidad de las personas, comunicar o publicitar información que viole los principios descriptos e incorporar datos o información falsos.

vínculos entre diferentes casos, patrullar mediante drones áreas extensas para proporcionar vigilancia aérea, analizar actividades en redes sociales para detectar amenazas potenciales, identificar movimientos de grupos delictivos o prever disturbios, detectar transacciones financieras sospechosas, entre otras[137].

En suma, por medio de estas resoluciones, se autorizó el ciberpatrullaje para una gama amplia de delitos, se detallaron criterios de aplicación difusos y se permitió el uso de *softwares* basados en inteligencia artificial u otras innovaciones tecnológicas, con control por parte del Ministerio.

Luego, al tratar la cuestión en forma particular se volverá sobre estas dos resoluciones, pero, previo a eso, se mencionarán algunos precedentes en la materia.

E) Antecedentes jurisprudenciales relevantes

Es importante resaltar algunos casos, sea por su origen de ciberpatrullaje como su relevancia para entender su significado.

i. El caso Halabi

Uno de los procesos más emblemáticos, pese a que no se inició mediante esta técnica, es el fallo "Halabi"[138] de la CSJN. En este precedente, se declaró la inconstitucionalidad de los artículos 1º y 2º la ley número 25.873 (telecomunicaciones) y, además, se entendió que las comunicaciones a las que se refería y todo lo que las personas transmiten mediante esa vía, formaban parte de la esfera de intimidad personal de cada ciudadano y, en consecuencia, debían ser requeridas por un juez[139].

ii. Kevin Guerra y la criminalización de los dichos en redes sociales

El 7 de abril del 2020, Kevin Guerra publicó en la red social Twitter (actualmente X), un tweet que rezaba: "che qué onda los que no cobramos el bono de 10mil pesos, ¿sigue en pie lo del saqueo no?". La expresión fue captada por personal de Gendarmería Nacional, mientras realizaba tareas de ciberpatrullaje, que realizó la denuncia por el delito de intimidación pública. Luego de la repercusión mediática que generó, el titular a cargo del Juzgado Federal número 3 de Mar del Plata entendió que esta no constituía delito y lo

[137]Disponible en: https://is.gd/sS7C5z [Enlace verificado el día 11 de septiembre de 2024].
[138]CSJN "Halabi, Ernesto s/amparo ley 16.986", 2/11/95 (Fallos 318:2148).
[139]Lo trascendente aquí es que, en el decreto reglamentario número 1563/2004 al que se remitía la ley (hoy derogado), se definió a las telecomunicaciones como "toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, cable eléctrico, atmósfera, radio electricidad, medios ópticos y/u otros medios electromagnéticos, o de cualquier clase existentes o a crearse en el futuro". Disponible en: https://is.gd/hM9DNJ [Enlace verificado el día 11 de septiembre de 2024].

sobreseyó[140]. Lamentablemente, en la resolución no se evaluó la metodología de recolección de la prueba (tweet), ya que se optó por descartar típicamente la conducta.

iii. El Ministerio Público Fiscal (MPF) y el monitoreo de redes

En otro fallo[141], se analizó si un pedido del MPF para confeccionar un informe relevando las manifestaciones públicas de funcionarios en redes sociales, con contenidos críticos y peyorativos hacia distintos magistrados para intervenir en sus funciones, resultaba violatoria de derechos fundamentales de los imputados y otras personas no identificadas. Ante el recurso de apelación presentado, los Sres. Jueces entendieron que este tipo de medidas resultaba invasivo de derechos vitales del sistema democrático, como la libertad de expresión, sumado a que constituía una violación al debido proceso porque no respondía a criterios de necesidad, racionalidad y proporcionalidad y, pese a que la búsqueda de la verdad resulta de vital importancia, la medida no tenía fundamento suficiente.

En este caso, aunque no se evaluó la constitucionalidad (ya sea de ciberpatrullaje o ciberinvestigación), se reconoció que para confeccionar informes de este tipo era necesaria una autorización judicial previa, basada en criterios propios de un debido proceso.

iv. El caso Bejarano

En este proceso[142], se analizó si las impresiones obtenidas por la policía de un perfil público de Facebook, estaban amparadas en la inviolabilidad de la correspondencia epistolar y, en consecuencia, debían ser obtenidas con autorización judicial previa. Los integrantes de la Sala IV entendieron que, como el perfil del imputado en la red social era público y toda la información que subía podía ser vista por cualquier persona, no gozaba de la protección de la privacidad que alegaba el defensor, y convalidaron el procedimiento.

v. El precedente de "La gorra leaks"

En otra investigación, llamada "La gorra leaks", una persona que habría sido recientemente identificada[143] vulneró los sistemas de información reservados de la PFA y la Prefectura Naval Argentina y los publicó en la red bajo ese pseudónimo. Luego de realizar una investigación, mediante la utilización de ciberpatrullaje, fueron acusadas 15

[140]Disponible en: https://is.gd/fgO35I [Enlace verificado el día 11 de septiembre de 2024].
[141]CCCF, Sala I, "Ministerio Público Fiscal s/recurso de apelación", 14/3/2022(CFP 8991/2019/11CA5).
[142]CFCP, Sala IV, "Bejarano, Alexis Ezequiel s/recurso de casación", 4/12/15 (causa nro. CCC 17200/2013/TO2).
[143]Disponible en: https://is.gd/ntF4J6 [Enlace verificado el día 11 de septiembre de 2024].

personas. Basándose en el dictamen fiscal, el Juez sobreseyó a todos los imputados destacando la falta de rigor científico y criterios objetivos de imputación en los elementos probatorios (publicaciones y referencias de los imputados en las redes respecto a la filtración), pues no podía interpretarse como un indicio de participación[144].

vi. El caso "Robles"

En otro precedente, a causa de la filtración de supuestas conversaciones mantenidas entre un funcionario público y un abogado defensor publicadas en una red social, se entendió que la obtención de este tipo de comunicaciones mediante actividades de inteligencia ilegal, resultaba violatorio del derecho a la intimidad de las personas involucradas y, en consecuencia, correspondía su exclusión probatoria[145].

vii. El sumario del "policía y los relojes"

Un agente, al realizar tareas de ciberpatrullaje en una página de ventas, advirtió que un usuario vendía relojes a un precio menor al valor de plaza, por lo que anotició al juzgado en turno, quien ordenó proseguir con la investigación y luego autorizó un allanamiento. Al llegar a una instancia recursiva, y ante un pedido de nulidad del defensor, se destacó que estas tareas eran meros relevamientos y no constituían una investigación policial que ameritara una orden judicial, pues al ser un sitio de acceso público no resultaba una intromisión indebida dentro del ámbito privado de las personas[146].

viii. El caso de Jujuy

Recientemente, tomó público conocimiento una investigación donde detuvieron a dos personas por difundir, mediante publicaciones replicadas y comentadas en redes sociales, una noticia falsa sobre una vinculación de carácter extramatrimonial entre dos personas que también involucraba a una menor de edad, sin resolución al día de la fecha[147].

ix. Ursic y el "buceo en redes sociales"

En este precedente, la Sala II de la CFCP resolvió un pedido de nulidad por un "buceo en redes sociales". Personal de Gendarmería Nacional, sin autorización judicial, localizó un perfil que se dedicaba a la venta ilegal de semillas, para el cultivo de marihuana. El funcionario sacó capturas de pantalla y elevó lo que consideró una noticia criminal a la fiscalía, que luego de requerir medidas al juzgado, logró determinar el

[144]JCCF Nº 9, "G,R y otros s/violación de correspondencia", 24/11/21 (causa nro. CCC 55276/2019).
[145]JCCF Nº 5, "Robles, Silvio Federico s/averiguación de delito", 17/1/2023 (causa nro. CFP 16/2023).
[146]CCCF, Sala II, "D. C. N., F. F.X. s/procesamiento", 3/2/20 (CFP 889/2018/3/CA1).
[147]Disponible en: https://is.gd/EI0Q2f [Enlace verificado el día 11 de septiembre de 2024].

abonado telefónico que creó la cuenta, la dirección de correo electrónico, el nombre de la persona, los movimientos migratorios y otros sujetos que la acompañaban. Esto derivó en intervenciones telefónicas y allanamientos donde se secuestró material estupefaciente.

En el caso, se cuestionó el accionar por constituir una "excursión de pesca", por la falta de autorización judicial oportuna. Los Sres. Jueces descartaron el planteo y entendieron que el espacio de redes sociales era equiparable a espacio público, hasta que no se estipule expresamente lo contrario, y que el magistrado a cargo estuvo en todo momento en control de las tareas investigativas, por lo cual, no avizoraban intromisión indebida u afectación irreparable a las garantías constitucionales[148].

x. El Tribunal Europeo de Derechos Humanos y el monitoreo en redes

En un fallo reciente, el TEDH entendió que se violó el derecho a la privacidad de un ciudadano ruso al usar sus datos personales. La policía, a través de un control rutinario en redes sociales, descubrió fotografías y un video del sujeto en el marco de una protesta. Luego de utilizar tecnología de reconocimiento facial para identificarlo, a partir de capturas de pantalla de redes sociales e imágenes de las cámaras de vigilancia del metro de Moscú, lo descubrieron y lo condenaron. El TEDH falló en su favor dejando constancia de que el uso de sus datos combinando este tipo de tecnologías resultaba violatorio de la intimidad del sujeto, sin perjuicio de haberse desarrollado en un espacio público[149].

xi. Breves conclusiones

De lo mencionado se desprende que cada vez son más frecuentes las investigaciones penales digitales y los casos vinculados a ellas. Constantemente los operadores del sistema de justicia se topan con este tipo de "pesquisas" que, en muchas ocasiones, resultan ser el disparador o indicio para la recolección de prueba de cargo. Así, la actividad policial se desarrolla tanto en un plano material como digital, haciéndose cada vez menos distinguible y tornándolo en una mezcla de dificultoso encuadre en términos procesales.

El interrogante que funciona como disparador para el desarrollo de esta tesis está dado a partir de reflexionar hasta qué punto el ciberpatrullaje afecta la intimidad de las personas. Hechas las aclaraciones respecto al concepto, su regulación y los precedentes que se mencionaron, intentaré responderla.

[148]CFCP, Sala II, "URSIC, Alfredo Gerardo y otros s/ recurso de casación", 25/4/24 (Causa Nº FSM 25882/2019/TO1/CFC13).
[149]TEDH, "Glukhin v. Russia", 4/7/23, *application* no. 11519/20. Disponible en: https://is.gd/oqXD5R [Enlace verificado el día 11 de septiembre de 2024].

F) Ciberpatrullaje. Análisis desde la perspectiva de Byung Chul Han.

Como se mencionó en el capítulo II ap. D, para Han la irrupción del nuevo paradigma de transparencia a "la sociedad de la información", opera constantemente en nuestra actividad o huella digital en el ciberespacio, acelerando los procesos informativos y transformando al ser humano en datos —mercancía— que se ofrece al mercado y adquiere mayor valor al ser visto. Así, sostiene que se vive en una sociedad transparente donde la actividad de las personas es vista y estas contribuyen a que así sea. Por esa razón, el autor plantea la mercantilización de las intimidades, debido a que las personas nutren el ciberespacio con sus datos privados, retroalimentando el tiempo que interactúan en ese medio.

A partir de esta reflexión, surgen dos interrogantes: i. si las personas tienen presente que los datos proporcionados podrán ser monitoreados por personal policial y ii. si su propia actividad en la red legitima y consiente tácitamente esto.

De acuerdo a la ley de datos personales y su decreto reglamentario número 1558/2001[150], su tratamiento es lícito cuando su titular presta consentimiento y, a modo de excepción, será tácito cuando provengan de fuentes de acceso público irrestricto. Es decir, la regla es que debe ser consentido (libre, expreso e informado) pero, como excepción, se entiende dado cuando los datos están en fuentes abiertas.

Etimológicamente, la palabra consentimiento proviene de la voz latina *consensus*, que significa sentir en común y supone el acuerdo o coincidencia voluntaria sobre algo determinado. Tiene dos momentos en su formación, la voluntad interior y su manifestación externa[151]. Respecto a los datos que van alimentando el ciberespacio, la pregunta a formular es si se podría aseverar que existe una verdadera voluntad interior de las personas al brindarlos o si en realidad lo hacen por otras razones. Además, de ser así, si esto convalida que puedan ser objeto de la mirada policial sin autorización judicial previa o ley que determine los criterios de actuación.

Las ideas de Han resultan interesantes para contestar este interrogante ya que, su visión es esclarecedora y novedosa. Para él, no existe voluntariedad en la dación de datos. Lo que existe es un mecanismo de coacción, al que llama "psicopolítica", que afecta la psiquis de las personas y los hace exponer su intimidad en forma constante en la red. Esta

[150]Disponible en: https://is.gd/sAg5T4 [Enlace verificado el día 11 de septiembre de 2024].
[151]IBAÑEZ, *Contratos,*1ed., Hammurabi, BuenosAires,2021, p. 225. Disponible en: https://is.gd/iQSGfj [Enlace verificado el día 11 de septiembre de 2024].

violencia interior, a la que denomina "microfísica del poder", no se caracteriza por ser infringida por otra persona para obligarla a hacer o no hacer algo (relación de negatividad); sino, por el contrario, está determinada por la acción positiva de no poner freno al flujo de información de los datos hacia el ciberespacio, es decir, no hay una tercera persona a quien oponerse, pues "rebelarse" consiste en frenar ese impulso interno a hacerlo. El sujeto sube constantemente sus datos bajo la premisa de que puede hacerlo y, cuanto más lo haga, más satisfactorio y libre será (ver capítulo III ap. A).

De acuerdo a este análisis, se podría suponer que no existe un verdadero consentimiento (libre, informado y expreso) en la suba de datos a la red, lo que en principio imposibilitaría su monitoreo, recolección o tratamiento con fines preventivos, sin autorización legal. Conforme lo describe Han, un mecanismo coactivo jamás podría asimilarse a un consentimiento en los términos de la ley de datos personales. Además, al transformar a las personas en mercancía a exponer, se los convierte en un objeto que, por ser una cosa, carece de libertad para consentir.

Al mismo tiempo, no se puede dejar de mencionar que hablar de consentimiento o voluntad en la dación de datos o metadatos, resulta paradójico. El día a día de las personas esta intermediado necesariamente por la interacción tecnológica, por lo que la entrega de datos a empresas privadas o públicas resulta necesaria para poder formar parte de la comunidad. No hay voluntariedad, hay necesidad[152]. Por otro lado, otra cuestión relevante para analizar el consentimiento es la adicción que genera el uso de las redes sociales (principalmente en los menores de edad), que ha dado lugar a que Estados (como el de Nueva York) demanden a las plataformas en base a los perjuicios en salud mental que registra la población por su uso[153].

La cuestión a dirimir en esos casos, es si una persona que sufre de una adicción puede consentir libremente la suba de datos. Igualmente, debe tenerse en cuenta que en las recientes resoluciones se detallan que los actos de prevención, detección, investigación y persecución mediante inteligencia artificial deberán concentrarse, principalmente, en las redes sociales.

Sin perjuicio del análisis que hace Han, lo cierto es que la cantidad de información existente sobre las personas en la red es incalculable. Esto hace que existan razones de

[152]POLANSKY, *Garantías constitucionales del procedimiento penal en entorno digital*, 1 Ed., Hammurabi, p. 61. Disponible en: https://is.gd/ubpcoL [Enlace verificado el día 11 de septiembre de 2024].
[153]Disponible en: https://is.gd/YsLr7C [Enlace verificado el día 11 de septiembre de 2024].

índole pragmática por las que correspondería replantearse la existencia de un consentimiento libre, expreso e informado o tácito. Así, se puede mencionar que:

i. La calidad de los datos que se pueden encontrar en fuentes abiertas o irrestrictas puede referirse a cuestiones personales o sensibles, que reflejan aspectos íntimos de las personas que merecen protección legal.

ii. El desconocimiento que tienen las personas de la magnitud de la información que publican en espacios digitales, tanto en lo que respecta a sus datos como a los metadatos[154].

iii. Que los datos se encuentren en fuentes abiertas o irrestrictas no garantiza que hayan sido subidos por su titular[155].

iv. Los contratos de adhesión que se suscriben para formar parte de las redes sociales son dispares en cuanto a las políticas de privacidad y, en la práctica, son aceptados sin tener verdadera noción de qué es lo que se está consintiendo.

v. La posibilidad, a partir del uso de inteligencia artificial, de que se combinen los datos personales y se establezcan deducciones referentes a datos sensibles[156].

Dadas estas razones, el análisis respecto a la cuestión del consentimiento resulta de compleja resolución en los términos planteados, incluso por la normativa que regula su protección. Lamentablemente, esto no fue analizado por la jurisprudencia nacional mencionada ni por las recientes resoluciones del Ministerio de Seguridad.

Sobre esto, en el artículo número 3 inciso g) de la Resolución 428/24, se hace referencia en forma general y difusa a que el ciberpatrullaje deberá ajustarse a la ley de datos personales y que está prohibido el tratamiento de datos sensibles o de menores, sin autorización judicial. Pero nada dice si esos datos se encuentran en fuentes abiertas o irrestrictas, que, de acuerdo a esa normativa, autoriza su tratamiento sin la necesidad de un consentimiento expreso, libre e informado. Es decir, no es claro si la policía podrá recolectar datos sensibles sin autorización judicial o datos de menores si se encuentran en este tipo de fuentes. La carencia de una respuesta certera a esto se debe, a que el problema no radica en la fuente de donde se obtiene sino en el dato.

[154]"Los metadatos, entonces, se refieren a la información asociada a un elemento informativo determinado (material o virtual), sea este una comunicación telefónica, un correo electrónico, un libro, la lista es infinita" (véase en POLANSKY "*Garantías…*", op. cit., p. 30).
[155]GAMEN, *La privacidad y las nuevas tecnologías*, 1. ed, Hammurabi, Buenos Aires, 2023, p. 79. Disponible en: https://is.gd/mpOMTB [Enlace verificado el día 11 de septiembre de 2024].
[156] Idem, 76.

Pese a que se entiende que el consentimiento tácito es cuestionable, se debe reiterar que tampoco existe consenso respecto a qué es un dato de acceso público obtenido de una fuente abierta. Esto no es una cuestión de mero orden semántico, sobre todo teniendo en cuenta que el Convenio de Budapest autoriza su acceso transfronterizo, lo que da una pauta de la magnitud de lo que se está analizando[157].

En el último tiempo, se ha tomado conocimiento de todo tipo de filtraciones por parte de distintas empresas. A modo de ejemplo, se podría mencionar lo que ocurrió con Cambridge Analytica (Facebook), Linkedin (2012 y 2016), Snapchat (2014) y Twitter (2015, 2018 y 2019). La mera circunstancia de que nuestros datos se encuentren en fuentes de acceso público o irrestricto, no implica necesariamente que hayan sido subidos con nuestro consentimiento[158]. Además, teniendo en consideración los obrantes en las distintas redes sociales, podría aseverarse que tanto los personales como los sensibles se encuentran en este tipo de fuentes.

En virtud de esto, se sugiere repensar esta cuestión, ya que los datos de las personas forman parte de una gran masa de información a la que pueden acceder las fuerzas policiales por medio de prácticas que, impulsadas por sistemas de inteligencia artificial, podrían tener un alcance ilimitado. Principalmente, porque dar vía libre a la recolección de datos asociados a la población mediante inteligencia artificial, sin autorización judicial, la sometería a un estado de vigilancia sin precedentes en la historia de la humanidad. En particular, porque el acceso a los metadatos, invade esferas protegidas constitucionalmente, socavando principios democráticos elementales[159].

Su inclusión, en las recientes resoluciones del Ministerio de Seguridad, requiere de la mayor atención. Se entiende que lo más preocupante radica en la ausencia de supervisión por un ente ajeno al PEN, reeditando la falta de control expuesta en el caso testigo que se detalló con anterioridad (capítulo 1º apartado E). Más teniendo en cuenta que, en la resolución que creó el sistema de reconocimiento facial, también se mencionó que no era necesario el consentimiento del titular del dato cuando éste se obtenga de fuentes de acceso público irrestricto y se recabe para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. Es decir, existen similitudes con el caso testigo aportado, que alertan sobre el uso que se podrá dar a esta práctica.

[157]SALT/POLANSKY, *La investigación*, op. cit. p. 138.
[158]GAMEN, *La privacidad...*, op. cit. p. 79.
[159]POLANSKY, *Garantías…*, op. cit, p. 61.

Además, la utilización de softwares de este tipo requiere, necesariamente, de un proceso que avale la transparencia algorítmica, para descartar sesgos discriminatorios y evitar la criminalización de un sector de la población determinado.

En cuanto al uso de estas innovaciones, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) expresó su preocupación por la implementación de inteligencia artificial en la aplicación de la ley, la seguridad nacional, la justicia penal, la gestión de fronteras y la vulneración de los derechos humanos. Especialmente, resaltó que esta tecnología puede ser una herramienta para predecir conductas a través del tratamiento de datos, y que las consecuencias para la privacidad y los derechos humanos de las personas son enormes. Esto, en base a que el conjunto de datos incluye a un gran número de personas, afectando su privacidad, lo cual puede dar paso a medidas procesales como allanamientos y detenciones, generalmente basados en metodologías que no son transparentes, pudiendo resultar discriminatorias para minorías históricamente criminalizadas[160].

Cabe destacar que las flamantes resoluciones del Ministerio de Seguridad, dan paso al inicio de algunas actividades de este tipo que, además, han sido recientemente vedadas por la Unión Europea en el "Reglamente de Inteligencia Artificial" donde se describen prácticas de inteligencia artificial prohibidas[161].

En esa inteligencia, existen autores que han comenzado a analizar si la sociedad se encuentra ante una nueva fase del panóptico descripto por Foucault.

Entre ellos, Han entiende que por medio de la coacción microfísica, al permitir que la actividad de las personas sea monitoreada en tiempo real, se retroalimenta su propia vigilancia, en lo que denomina "panóptico digital". Pero, a diferencia del desarrollado por Foucault, no existe una vigilancia localizada ni una lógica de biopoder sobre la administración de los cuerpos, para conseguir la confesión mediante tortura. En esta fase digital, no es necesario torturar para obtener una confesión, ahora las personas se confiesan "libremente" en la red, otorgando sus datos privados (ver capítulo III ap. A).

Resulta significativo mencionarlo porque la "sociedad disciplinaria" que describió Foucault se basó en un sistema de vigilancia, cimentado en el concepto de peligrosidad

[160]ACNUDH, "El derecho a la privacidad en la era digital Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos Distr. General",13/9/21. Disponible en: https://is.gd/1DeAO5 [Enlace verificado el día 11 de septiembre de 2024].

[161]Para ahondar en las críticas a la creación de la UIASS, sugiero la lectura del reciente artículo: RIQUERT, "Libertad vs seguridad: nuevas tensiones a propósito del ciberpatrullaje y la creación de la unidad de inteligencia artificial aplicada a la seguridad", *RPP*, 516, 2024 (https://is.gd/O6XFPx; última visita: 11 de septiembre de 2024).

social, que dio origen a formas de ejercicio judicial determinadas (ver capítulo V apartado A). De acuerdo a esto, se podría estar en presencia de una nueva modalidad, la tecnológica, con repercusiones a futuro en la construcción del concepto de verdad, proceso penal y formas judiciales.

Por esto, se entiende que resulta vital reafirmar el valor de las garantías constitucionales —en este caso, el derecho a la intimidad o privacidad— en el marco de estas nuevas medidas de investigación que estarán orientadas en la búsqueda de la verdad.

Como se mencionó, los métodos de averiguación y la estructuración del sistema procesal tuvieron la función de asegurar la libre circulación de bienes en el comercio de esa época, lo que en la actualidad podría traducirse en la libre circulación de datos e información en la red digital. Esto, a su vez, tiene su reflejo en cómo se hacen valer los derechos fundamentales en pos de asegurar el descubrimiento de la verdad (ver capítulo V ap. A).

De la misma forma que Han destaca que el proceso de transparencia elimina las trabas al libre flujo de información, la incorporación de tecnología en los procesos de investigación penal, podría dar paso a un sistema que tenga por objeto la "transparencia" en la persecución, prevención y predicción del delito, eliminando cualquier obstáculo que se le presente e interrumpa el proceso, en detrimento de las garantías constitucionales de los ciudadanos.

Han acentúa que el concepto de protección de datos obstaculiza este flujo, con lo cual se deberá prestar suma atención a si el uso de inteligencia artificial para ciberpatrullar viola su contenido. Si se piensa en una investigación penal como un proceso de flujo de información para conformar un cuadro de imputación, la única traba o límite son las garantías constitucionales. Es decir, la inclusión del concepto de transparencia en los procesos de investigación para acelerarlos podría tener repercusiones en los derechos fundamentales a futuro.

Además, un sistema como el que describió Foucault, basado en el derecho penal de autor por sobre el derecho penal de acto, vigila y juzga a las personas por lo que pueden llegar a hacer y no por lo que hacen (peligrosidad). El método coactivo que Han describe asocia la idea de libertad con la facultad de poder hacer.

Entonces, considerando que la implementación de tecnologías como las mencionadas en el artículo 5º aumentaría exponencialmente las facultades para monitorear, analizar y procesar información, esta nueva fase podría dar paso a un sistema de vigilancia desconocido, alimentado por lo que las personas pueden hacer, en un

contexto donde las personas asocian su libertad a poder hacer. La suma de esos factores, podría implicar una vigilancia masiva de las personas en la red.

Esto ha sido expuesto por diferentes entidades preocupadas por la defensa de los derechos humanos. La ACNUDH, elaboró un informe manifestando su preocupación respecto a la vigilancia electrónica masiva. En particular, dijo que las actividades de monitoreo en línea, en espacios públicos o en plataformas de redes sociales, constituyen intromisiones al derecho a la privacidad. Afirmó que los individuos deben tener un espacio libre de observación e intrusión de parte de las autoridades estatales, porque la protección del derecho a la privacidad abarca también los espacios públicos y la información de acceso libre[162].

Lo más trascendente en las advertencias del ACNUDH, radica en que el derecho a la privacidad es una de las piedras angulares para el desarrollo de la personalidad del ser humano, que resulta trascendente a la hora del ejercicio de otros derechos fundamentales de la democracia moderna (como el derecho a la libertad de expresión y reunión, entre otros). Por lo tanto, cuando se avasalla la intimidad o privacidad de las personas en pos de un objetivo, se pone en juego valores intrínsecos que hacen a los sistemas democráticos de gobierno. Por esta razón, las injerencias a estos derechos deben ser analizadas con suma cautela.

En esa misma línea, en una declaración conjunta de la sociedad civil (donde firmaron asociaciones como Amnistía Internacional) se expresó que esta práctica reforzaba la vigilancia masiva y esto debía tener límites determinados, pues institucionalizaba la observación de un conjunto de la población indiscriminadamente, sin que exista sospecha de comisión de un determinado delito[163].

En esa tesitura, el Dr. Francisco Pérez de los Cobos Orihuel planteó que el ciberespacio, sin estar sujetos a controles, podría redundar en un gigantesco panóptico digital en el que nadie podrá escapar a su control, a raíz de toda la información que suben los individuos[164]. Sobre esto, el Dr. Riquert dijo que se vive la era del "hombre de cristal" donde el aforismo de "mi casa, mi castillo" dejó de ser cierto. Para él, la sociedad se encuentra en una era de vigilancia social, caracterizada por un ciudadano transparente y

[162]ACNUDH, "El derecho a la privacidad en la era digital",4/8/22. Disponible en: https://is.gd/4z7add [Enlace verificado el día 11 de septiembre de 2024].
[163]Disponible en: https://lc.cx/Z1aLLl [Enlace verificado el día 11 de septiembre de 2024].
[164]COBOS ORIHUEL, "El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado", p.3. Disponible en: https://is.gd/mSQFYs [Enlace verificado el día 11 de septiembre de 2024].

una administración que no lo es. Por eso, remarca la importancia de establecer límites claros al abuso de poder y la arbitrariedad, para defender los derechos fundamentales de los individuos, en particular, el respeto a la intimidad digital y la confidencialidad de los datos personales[165].

En este contexto, aseverar que existe un consentimiento tácito por parte de las personas al subir sus datos a fuentes irrestrictas y dar por finalizada esa discusión resulta presuroso.

Sobre esto, la jurisprudencia del TEDH está dando muestras de que la implementación de nuevas tecnologías en la investigación penal puede resultar invasiva de ámbitos expresamente tutelados. Se expondrán algunos ejemplos a continuación.

En "Benedik contra Eslovenia" y "Shimovolos contra Rusia" se entendió que seguir a un usuario sin orden judicial, en una red de intercambio de archivos e individualizarlo por la información asociada a un IP dinámica, o registrar a un activista en una base de datos de vigilancia que recopilaba información sobre sus movimientos, constituían violaciones a la privacidad, agregando que las reglamentaciones que lo legitimaban no ofrecían protección contra interferencias arbitrarias y abusos policiales, respectivamente. En "Brunet contra Francia" se aclaró que la inclusión de una persona en una base de datos policial por el plazo de veinte años, era desproporcionado e innecesario en una sociedad democrática. En "Szabó y Vissy. C. Hungría" se llegó a la misma conclusión y se dijo que la ley de vigilancia masiva de comunicaciones con tecnologías de vanguardia, aún en caso de sospecha de terrorismo, no ofrecía garantías para evitar los abusos, pues podría incluir a cualquier persona. Por último, en "Big Brother Watch y otros contra el Reino Unido", se analizó la interceptación masiva de comunicaciones y material, por gobiernos y agencias de inteligencia, y se entendió que estos sistemas violaban la vida privada y correspondencia de las personas. Además, se asentó que las medidas de vigilancia, debían estar autorizadas y sujetas a los principios (necesidad y proporcionalidad) por organismos independientes al poder ejecutivo determinando su alcance y objeto[166].

Es decir, el TEDH comenzó a evaluar estas nuevas formas de investigación desde la perspectiva del derecho a la intimidad, la protección de datos y su necesidad en una sociedad guiada por los principios democráticos.

[165]RIQUERT, *Ciberdelitos*, 2da. ed, Hammurabi, Buenos Aires, 2020, p. 145. Disponible en: https://is.gd/KAjJqt [Enlace verificado el día 11 de septiembre de 2024].
[166]Disponible en: https://is.gd/vQLGET [Enlace verificado el día 11 de septiembre de 2024].

Entre los antecedentes nacionales, los de mayor relevancia en este sentido son el caso "Halabi", donde se confirmó que es necesaria una autorización judicial para invadir las comunicaciones de las personas por cualquier medio, y el caso "Ministerio Público" en el que se destacó que el relevamiento de opiniones públicas indiscriminadas en la red violaba derechos fundamentales. Empero, no se han encontrado precedentes que abordaran esta temática como sí lo hizo el TEDH.

En resumen, la cuestión referente a la vigilancia masiva en la red es algo que está actualmente en discusión, por lo cual el ciberpatrullaje también debe ser evaluado teniendo en cuenta estas consideraciones. Es por esto que lo trascendente a la hora de evaluar su legalidad estará en valorar si se afecta o no el derecho a la privacidad de las personas, pero dicha tarea también resulta compleja.

En este sentido, Han remarca la dificultad de diferenciar aquello que es íntimo de lo que no lo es, porque los sujetos de rendimiento al autoexplotarse, exponen de manera constante su intimidad y, esa falta de distancia entre lo íntimo, lo público y el crecimiento exponencial de las redes sociales, dejó de existir (ver capítulo III ap. c).

En esa línea, no es similar obtener el número de documento de una persona que sus hábitos, gustos, familiares, amigos y rutina; estos datos, pese a estar publicados en una red social, no dejan de ser información íntima de quien lo publica y, por esto, no debería ser pasible de monitoreo por personal policial, sin justificativo previo. El interrogante que se sigue, radica en preguntarse por qué razón las personas deberían estar sometidas a observación sin autorización judicial.

Como se mencionó, Han describe que nos encontramos en la "tiranía de la visibilidad", donde todo aquel que no se allana a la luz es considerado un sospechoso. Una sociedad que se organiza en base a la positividad, reemplazando la confianza por la vigilancia y el control. En esa línea, Wajcman hace una reflexión interesante: sostiene que, en una sociedad sometida a la mirada disuasiva y preventiva, ser inocente es no tener nada que ocultar y no tener nada que ocultar es aceptar ser visto. Ergo, ser inocente es aceptar ser visto (ver capítulo II C).

Se entiende que esta pregunta debe ser formulada al momento de analizar los límites a los que debería estar sujeto el ciberpatrullaje. La vigilancia, sin sospecha y contralor, efectuada por personal policial no puede revertir el principio de inocencia sobre el que se edifica el sistema jurídico. Este es, de fondo, uno de sus mayores problemas para evaluar su constitucionalidad.

En el caso del "policía y los relojes" que se mencionó, se justificó un allanamiento porque, al parecer del funcionario que monitoreaba la actividad en Mercado Libre, los artículos estaban a un precio menor de lo que valían. Es decir, sin autorización judicial previa ni sospecha suficiente, el agente comenzó a investigar la actividad comercial de un sujeto determinado y, en base a un "olfato virtual policial", se inició un expediente penal que derivó en un allanamiento de su morada y su posterior detención.

Validar este tipo de prácticas —sin pautas de actuación y control inicial sobre la actividad— se cimienta en esa lógica conceptual de que ser inocente es aceptar ser visto, dando por tierra con la presunción de inocencia y, por ende, con el derecho a la privacidad de la persona. A su vez, esto justifica las llamadas "excursiones de pesca", donde el personal policial revierte la lógica del proceso penal en un Estado de Derecho[167]. Tampoco escapa a este entendimiento que las facultades policiales con este tipo de actividad pueden ser emparentadas a las tareas de inteligencia, en el marco de la ley número 25.520, que requieren de autorización judicial previa[168].

Por lo tanto, la circunstancia de que los datos estén en una fuente de acceso público e irrestricto tampoco es determinante para descartar una violación a un derecho fundamental. El caso "Robles" que se mencionó es un buen ejemplo.

i. La diferencia entre el ciberpatrullaje y el patrullaje a pie

Sin perjuicio de esto, una de las explicaciones que la jurisprudencia nacional ha dado, para sostener la legalidad del ciberpatrullaje, es que no dista del patrullaje a pie que realizan los agentes policiales en la calle (artículos 183 y 285 del CPPN). Estas situaciones que nominalmente serían similares, en la práctica no lo son.

La primera diferencia radica en el rango de actuación, ya que mediante técnicas de ciberpatrullaje, utilizando inteligencia artificial y *big data*, se extendería el alcance de vigilancia y análisis, a límites desconocidos. Principalmente, teniendo en cuenta que el artículo 5º de la resolución nro. 428/2024 autorizó su uso.

En segundo lugar, respecto al límite temporal, el objeto de examen podrá basarse en datos pasados, presentes y futuros (ver artículo 4º inc. "d" de la resolución 710/2024 que dispone la utilización de algoritmos predictivos para el análisis de datos históricos de

[167]Esto es, en vez de investigar un suceso presuntamente delictivo para determinar responsabilidades penales se procede, a poner el foco sobre un ciudadano en particular para cerciorar si realizó alguna conducta reprochable (véase en D'ALBORA, *Código Procesal Penal de la Nación. Anotado, comentado y concordado*, Tomo I, 1 ed, LexisNexis, Abeledo-Perrot, Buenos Aires, 2005, p. 521).

[168]ZARA, "Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay", *Revista pensamiento penal*, 483, 2023, p. 44 (https://is.gd/PQUFCg; última visita 11 de septiembre de 2024).

crímenes para predecir futuros delitos). Entonces, la lógica de prevención se amplía y pasa a ser hasta predictiva. De esta manera, varían ostensiblemente las características propias de la actividad que actualmente se lleva a cabo.

Además, la actividad policial tradicional actúa ante la comisión de un delito o una alerta sobre un sospechoso en particular, de forma reactiva, para detenerlo por un caso determinado. En la predictiva, mediante el análisis de datos, no se ha cometido un delito ni existe una alerta, pero se interviene de forma proactiva para preverlo, mediante la utilización de información de otros casos y el uso de procesos que se valen de grandes cantidades de datos[169].

En sus considerandos, la Resolución mencionada hace énfasis en que es necesario generar mecanismos coordinados y proactivos para la investigación por parte de las fuerzas policiales y de seguridad federales. Incluir específicamente la palabra "proactivo" en su justificación, implica el comienzo de análisis predictivos de criminalidad con los datos de las personas[170].

Como se mencionó, los *softwares* como *Predpol* y *COMPAS* ya son una realidad. Dotar a las fuerzas policiales de estas herramientas aumenta la capacidad para el procesamiento, cálculo y clasificación de datos en la nube, que posibilita predecir comportamientos a futuro (ver capítulo IV apartado E). A modo de ejemplo, se puede destacar el *MArIA Project*, utilizado para localizar plantaciones de marihuana mediante el tratamiento de datos del consumo de energía eléctrica de los usuarios o el CERT que permite, a través del examen de fuentes abiertas, detectar amenazas en el ciberespacio[171].

También, agencias como la CIA han expuesto que los avances en materia de inteligencia artificial resultarán a futuro de suma importancia para capitalizar el valor que tendrá la recopilación y evaluación de datos en fuentes abiertas[172].

De esta forma, emparentar estas modalidades de investigación o prevención implica no meritar su verdadero alcance.

Respecto al uso de algoritmos, pese a que existen discusiones de diverso calibre en la doctrina, el caso "SyRi" del Tribunal de la Haya acaparó la atención. Allí, se denunció al gobierno holandés por violar el derecho a la privacidad de sus ciudadanos al

[169]CUATRECASA MONFORTE, "La inteligencia artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos", pp. 217-8 (https://is.gd/bSTTfV; última visita el día 11 de septiembre de 2024).
[170]Durante el desarrollo de esta tesis, se sancionó la Resolución 710/24 que dispuso como una de las funciones de la UIAAS la utilización de algoritmos de aprendizaje automático para predecir futuros delitos.
[171]RIOS, "*Empleo…*", op. cit., p. 8.
[172]Disponible en: https://is.gd/27tuqW [Enlace verificado el día 11 de septiembre de 2024].

utilizar, ante una sospecha de fraude impositivo en un vecindario, un algoritmo (SyRI) para obtener informes de riesgos de sospechosos que serían objeto de investigación.

Al resolver el caso, en primer lugar, el Tribunal primero determinó que un algoritmo no conoce ni comprende la realidad y comprobó que se violó la privacidad de los ciudadanos ya que no se había informado el modelo de riesgo y los indicadores que lo componían, con lo cual, al ser secreto, no cumplía con los principios que lo regulaban (transparencia, limitación de propósito, minimización de datos, precisión, integridad, confiabilidad y responsabilidad). A su vez, destacó que esta herramienta tenía un sesgo discriminatorio y estigmatizante, ya que señalaba a los inmigrantes y a las personas con menores ingresos[173].

En esa inteligencia, en la reciente Resolución no se menciona la forma en que se dará cumplimiento con los principios que regulan los algoritmos de los dispositivos o herramientas que serán utilizados para ciberpatrullar. El uso de *softwares*, conlleva la obligación de determinar el modo en que se dará a conocer el modelo de riesgo e indicadores de los algoritmos que los componen, para garantizar los principios mencionados, a fin de evitar el efecto "caja negra"[174] y la criminalización de áreas emparentadas con el delito o grupos estereotipados como delincuentes, amparándolos de la discriminación y estigmatización.

Como menciona Ferrajoli, los algoritmos no son neutros, persiguen intereses, ideologías y fines de quienes los escriben, porque son instrumentos de poder y pueden ser utilizados para realizar un control panóptico de poblaciones enteras[175].

En conclusión, por lo expuesto, resulta controversial emparentar las actividades de patrullaje a pie con las de ciberpatrullaje, ya que implica asimilar actividades que, en la realidad, son diferentes.

ii. Hacia un equilibrio en la lucha contra el delito y el respeto de las garantías constitucionales

De la misma forma que avanza el fenómeno delictivo en el ciberespacio, también las medidas para prevenir delitos deben actualizarse y podrán ser receptadas por el

[173] Disponible en: https://is.gd/W51eyL [Enlace verificado el día 11 de septiembre de 2024].

[174]"El aprendizaje automático puede hacer que la tecnología sea extremadamente potente, aunque su proceso de toma de decisiones pueda ser complejo, ser similar a una "caja negra", donde no se puede conocer cómo ocurren las cosas ahí adentro" (véase en RIQUERT, *Sistema penal e informática*, vol. 7. 1 ed, Hammurabi, Buenos Aires,2024, p. 29). Disponible en: https://is.gd/8no81K [Enlace verificado el día 11 de septiembre de 2024]

[175]FERRAJOLI, *Por una Constitución de la Tierra. La humanidad en la encrucijada* (traducción a cargo de IBAÑEZ), 1 ed., Trotta, Madrid, 2022, p. 101.

ordenamiento local. No es intención de este trabajo plantear la impunidad de este tipo de delitos, pero, como menciona el Convenio de Budapest, es necesario lograr su armonización con los derechos fundamentales de las personas.

Como se señaló, la búsqueda de la verdad pese a ser un objetivo al que no debemos renunciar, para estar legitimado constitucionalmente debe respetar los derechos y garantías (ver capítulo V ap. C). De la misma forma, realizar ciberpatrullaje violando la intimidad de las personas en la red no debería ser avalado judicialmente.

Retomando el concepto de Han desarrollado *En el enjambre*, respecto a que la exposición ininterrumpida en redes sociales destruye la distancia entre lo público y lo privado e incentiva la producción de información haciendo desaparecer la privacidad de las personas, se cree que es necesario repensar el concepto de intimidad. Para romper con esa positividad que aísla a los individuos, es necesario comprender que la intimidad y libertad, va a estar dada por la posibilidad de las personas de relacionarse entre sí, de forma privada en la red (donde se interactúa a todo momento). Esto significa que cada acción de control y vigilancia sobre sus interacciones deberá ser evaluada a la luz de esta nueva realidad.

El riesgo de no hacerlo, consiste en que los ámbitos de tutela tradicional de las garantías constitucionales podrían volverse inadecuados ante el avance de los nuevos mecanismos guiados por inteligencia artificial[176]. Ante esto, los Tribunales han desarrollado diferentes teorías para evaluar si afectan o no derechos fundamentales.

iii. Criterios jurisprudenciales en búsqueda de ese equilibrio

La Corte Suprema de Estados Unidos de Norteamérica, al interpretar la 4º enmienda de su Constitución referente a la protección de la intimidad frente a investigaciones y registros, ha determinado que existen situaciones donde es necesaria una orden judicial previa. Al comienzo, estuvo emparentada con la idea de propiedad (domicilio) pero luego extendió su criterio, hasta llegar a lo que hoy conocemos como la doctrina de la "expectativa razonable de intimidad"[177].

[176]ROCA MARTÍNEZ, *Procesos y prueba prohibida*. 1 ed., Dykinson, Madrid, 2022, p. 244 (https://is.gd/CkS6td; última visita el día 11 de septiembre de 2024).

[177]Podemos situar sus comienzos en el precedente "Boyd v. United States", donde el juez Bradley destacó que cualquier invasión gubernamental o de agentes, a la santidad del hogar y vida privada, afectaba la privacidad. Luego, en "Olmstead v. The United States", determinaron que una intromisión injustificada en la vida privada de un individuo era una violación a esta enmienda y no podía utilizarse como prueba. Posteriormente, en "Osborn v. United States", el juez Douglas resaltó que, pese a que las acciones tomadas individualmente parecían no tener importancia, se evidenciaba una sociedad en la que el gobierno podía meterse en la vida privada de cada uno de los ciudadanos a voluntad. Finalmente, en el caso "Katz" nace el concepto de "razonable expectativa de privacidad" basado en dos requisitos, necesarios para hacer valer el

En investigaciones mediadas por innovaciones tecnológicas, se evalúa teniendo en cuenta: el objetivo de la vigilancia (comercio, casa, conversaciones, etcétera), la clase de información que se revela (si es privada o no) y la naturaleza de los medios utilizados (si son conocidos o no por la sociedad). A modo de ejemplo, se podrían destacar los casos "Dow Chemical", "Kyllo" y "Jones", donde la Corte entendió que vigilar satelitalmente una propiedad, o el uso de dispositivos térmicos para observar desde la calle el interior de un domicilio y el seguimiento por GPS durante un plazo prolongado en una investigación, sin orden judicial previa, vulneraban la expectativa de privacidad de una persona, respectivamente[178].

Todos estos casos, pese a no ser estrictamente sobre ciberpatrullaje, demostrarían que la incursión de la tecnología en la investigación penal trae aparejados nuevos desafíos respecto a la esfera de intimidad de las personas, que deberán ser equilibrados con la búsqueda de la verdad.

Por otro lado, el Tribunal Constitucional Alemán desarrolló el concepto de "autodeterminación informativa". Su génesis estuvo dado partir de una sentencia que declaró la inconstitucionalidad de determinados artículos de la Ley de Censo de la República Federal Alemana.

Allí, se entendió que existía un derecho de los ciudadanos a conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, para protegerlos contra la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. Además, se advirtió que en el futuro, los procesamientos automáticos de esa información podrían afectar la dignidad de las personas y se destacó que, el tratamiento jurisprudencial que habían desarrollado de las garantías y derechos —derivados del secreto a las comunicaciones, inviolabilidad del domicilio y la personalidad misma— no eran suficientes para evaluar la necesidad de protección de la intimidad frente a los avances tecnológicos[179].

A diferencia de su par norteamericano, que concibe al derecho a la intimidad como un deber pasivo de no interferencia ilegítima, este nuevo derecho —a la

derecho a la privacidad por sobre la validez de una prueba: la persona que lo esgrime debe haber actuado conforme a una real expectativa de privacidad y la sociedad debe considerarla razonable, pues, lo que una persona expone conscientemente al público no estaría protegido (véase En VANINETTI, *Derecho a la intimidad en la era digital*, vol. I,1 ed., Hammurabi, Buenos Aires, 2020, pp. 53-55). Disponible en: https://is.gd/jT8MDd [Enlace verificado el día 11 de septiembre de 2024].

[178]ORTIZ PRADILLO, "La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación", pp.18-20. Disponible en: https://is.gd/IqrO4Z [Enlace verificado el día 11 de septiembre de 2024]

[179]Idem, p. 22.

autodeterminación informativa— es una herramienta activa de los ciudadanos para hacer valer esa prerrogativa.

Bajo otra perspectiva, el Tribunal Supremo Español desarrolló el concepto del "derecho al propio entorno virtual" como derecho fundamental. En la sentencia número 342/2013, determinó que su contenido se basa en toda la información, en formato electrónico, que el usuario genera en forma consciente o inconsciente, voluntaria o involuntariamente por el uso de la tecnología, capaz de generar un rastro que luego podrá ser recolectado. Así, en la sentencia nro. 173/2011, se destacó que cuando las personas navegan por internet revelan datos de su personalidad que, analizados en forma aislada, podrían ser irrelevantes, pero en conjunto establecen perfiles descriptivos que deben ser protegidos frente a la intrusión de terceros. Justamente, en la sentencia número 204/2016, se remarcó la importancia de este derecho, debido a que analizar cada intento de invasión de estos datos, bajo las garantías constitucionales tradicionales, no proporciona una adecuada protección[180].

En resumen, las nuevas medidas de investigación han despertado el interés de los Tribunales para garantizar la intimidad de las personas, ya sea interpretando si existe una real expectativa de privacidad, o evaluando si se vulneró la autodeterminación informativa o el derecho al propio entorno virtual. Estos criterios jurisprudenciales, podrían ser la base para comenzar a analizar si la prueba recolectada mediante ciberpatrullaje puede ser incorporada en un proceso penal.

G) Redefiniendo el concepto de intimidad. Criterios: la teoría del mosaico y la privacidad como integridad contextual

El derecho a la intimidad es un derecho personalísimo, calificado también como derecho a la privacidad o a la vida privada y se deriva de numerosos cuerpos normativos del derecho continental. Anteriormente, se emparentaba este derecho con la facultad de ser dejados solos.

Para nuestra CSJN, se encuentra consagrado en el artículo 19 de nuestra CN. Protege un ámbito de autonomía individual (constituido por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física, las acciones, hechos o datos) que, teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservadas al propio individuo y cuyo

[180]CHARAJA COATA, *¿Existe un derecho al propio entorno virtual?*,1 ed., Hammurabi, Buenos Aires, 2022, pp. 53-55. Disponible en: https://is.gd/thYl2w [Enlace verificado el día 11 de septiembre de 2024].

conocimiento y divulgación por extraños significa un peligro real o potencial para la intimidad. Comprende, tanto la esfera doméstica como el círculo familiar y de amistad sumado a otros aspectos de la personalidad espiritual o física de las personas (como la integridad corporal o la imagen)[181].

Pero, actualmente, existen autores que entienden que esto se debe reformular, en atención a los avances tecnológicos que han modificado el escenario, para ampliar los ámbitos de tutela. Uno de ellos es el Dr. Rebollo Delgado.

Para él, la privacidad tiene dos esferas: la interna, constituida por ese derecho de defensa a la intromisión indebida, y la externa que es la herramienta de las personas para decidir lo que desean que se conozca de ellos. Para esto, lo divide en tres criterios: el objetivo (el derecho a estar solo), el subjetivo (ligado a la autodeterminación informativa) y la teoría del mosaico, cuya función radica en cuidar la intimidad de las personas ante las nuevas medidas de investigación. Respecto a este último, sostiene que existen datos que evaluados individualmente podrían ser tomados como irrelevantes, pero, uniéndolos revelarían aspectos importantes de la personalidad, de la misma manera que las piezas de un mosaico no dicen nada, pero al ser unidas adquieren significado[182].

Este último criterio podría ser un buen comienzo para evaluar si el ciberpatrullaje vulnera ámbitos tutelados por el derecho a la intimidad (ya sea el secreto o reserva de los actos de la vida privada, la correspondencia epistolar o papeles privados, el domicilio, la imagen, el nombre o el secreto profesional u otros no enumerados). Máxime teniendo en cuenta la cantidad y calidad de información que existe sobre las personas en el ciberespacio, principalmente en las redes sociales.

De todos modos, los criterios jurisprudenciales conocidos para determinar afectaciones a la vida privada fueron creados en un contexto muy diferente al actual. Hoy, las personas comparten durante gran parte de su tiempo lo que hacen con otras, por lo tanto, la rigidez conceptual para determinar si un mensaje vía red social constituye correspondencia epistolar o papel privado en los términos pretéritos, o si alguna actividad en la red puede ser categorizada como un acto de la vida privada, es de difícil aplicación. Así, al momento de evaluarlo, se deberían tener en cuenta estos extremos, para no

[181]Por ello, nadie puede inmiscuirse en la vida privada de una persona, ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares. Pues, sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de: la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen. (véase en CSJN, "DGI. c/ Colegio Público de Abogados" y "Franco, Julio César", resueltas el 13/2/96 y 30/10/17 respectivamente (Fallos 319:71 y 330:4615).

[182]VANINETTI, *Derecho…*, Vol. I. op. cit. p. 26.

descartar sin más, bajo parámetros descontextualizados, posibles afectaciones a la intimidad o vida privada.

En consideración a lo expuesto —respecto a la falta de consentimiento tácito en la suba de datos, el contexto de panóptico digital, la falta de certeza respecto a de dónde provienen y qué es una fuente abierta, el uso de inteligencia artificial y la diferencia entre esta práctica y el patrullaje tradicional— resulta necesario abordar el ciberpatrullaje redefiniendo el concepto de intimidad a los tiempos que vivimos.

Como sostiene nuestro Máximo Tribunal, la interpretación auténtica de la CN no puede olvidar los antecedentes que hicieron de ella una creación viva, impregnada de realidad histórica. Para, dentro de su elasticidad y generalidad, no envejecer con el cambio de ideas, el crecimiento o redistribución de intereses y seguir siendo el instrumento de la ordenación política y moral de la Nación[183].

De la misma forma que avanzan los métodos de investigación, la interpretación de las garantías constitucionales también debe ser dinámica, para dotarlas de sentido. De esa forma, el análisis para determinar si resulta necesaria una autorización judicial o una ley formal para realizar ciberpatrullaje e incorporar el producto al proceso, debe estar guiado por la realidad que viven las personas y la intención de los constituyentes de restringir la intromisión en su intimidad de forma arbitraria. Además, podría suceder que un dato aislado no parezca de la clase que merezca la protección mencionada, pero, unido con otros adopte otra significación.

A modo de ejemplo, en el caso "Bejarano" se extrajo un dato de su perfil público que, analizado en forma aislada, no pareciera ser relevante o digno de protección bajo los parámetros conocidos, pero resultó determinante para probar su responsabilidad, con lo cual debería haber sido recabado con los recaudos legales correspondientes. En idéntico sentido, en el caso "La gorra Leaks", a través de la recolección y análisis de publicaciones en redes sociales, se extrajeron datos para cimentar una imputación, afectando derechos fundamentales de las personas, que se vieron sometidas a un proceso penal sin haber cometido ningún delito. En esa tesitura, en el caso "Ministerio Público" citado, los jueces destacaron que el monitoreo de opiniones en redes sociales públicas resultaba invasivo de derechos fundamentales.

En consecuencia, el interrogante a responder es si es posible descartar sin mayor análisis invasiones a la intimidad por medio de esta práctica. Descartar de llano la

[183]CSJN, "Costa, Héctor Rubén"**,** 12/3/1987 (Fallos 310:508 disidencia del Dr. Fayt).

existencia de, por ejemplo, una expectativa razonable de intimidad en espacios públicos —virtuales— es cuestionable. La CSJN tiene dicho que el ámbito de privacidad protegido por el artículo 19 de la CN también alcanza las conductas realizadas fuera del domicilio y en espacios públicos, si posee determinadas características[184].

En esa línea argumental, los autores Lilian Edwards y Lachlan Urquhart entienden que las personas no renuncian implícitamente a cualquier expectativa de intimidad, cuando hacen *click* a los términos y condiciones —que no conocen— para unirse a una red social. Eso implicaría aseverar que solo los ciudadanos que tienen conocimiento del uso y extracción de sus datos por SOCMINT y están educados tecnológicamente conservan esta cuota de privacidad, lo cual, resulta ilógico. Para ellos, darle la espalda a la realidad de los jóvenes que plasman en las redes sociales toda su actividad y negarles así su derecho a la privacidad es surrealista[185].

Sobre todo, teniendo en cuenta que, como resaltó el TEDH en el caso "Peck v. United Kingdom"[186], la expectativa razonable de intimidad de los ciudadanos, incluso dentro del espacio público, debe ser un elemento a considerar y no puede ser descartado sin un análisis de necesidad y proporcionalidad. También, en "Rotaru contra Rumania"[187] y "Amann contra Suiza"[188], detallaron que la recopilación de datos por parte de los servicios de seguridad sobre individuos concretos constituía una interferencia en la vida privada de las personas. De igual forma, pese a que se expide respecto a las cámaras de vigilancias en la calle, Von Hirsch destaca que este tipo de medidas puede afectar la intimidad de las personas, en tanto se realice en forma oculta[189].

Trasladando esta lógica de razonamiento, no se podría descartar la existencia de una expectativa razonable de intimidad, incluso cuando las personas navegan en el ciberespacio, respecto a su huella digital, sin distinción del tipo de fuente.

Uno de los problemas que se entiende relevante es que aún hoy se asocia la invasión a la intimidad con una intromisión de un tercero, como un ataque externo. Esto

---

[184]CSJN, "Spinosa Melo, Oscar Federico", 5/9/06 (Fallos 329;3617).
[185]EDWARDS/URQUHART, "Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence?", p. 26. Disponible en: https://is.gd/vADCxZ [Enlace verificado el día 11 de septiembre de 2024].
[186]TEDH, "Peck v. United Kindom", 28/1/03, *application* no. 44647/98. Disponible en: https://is.gd/LcmZQ2 [Enlace verificado el día 11 de septiembre de 2024].
[187]TEDH, "Rotaru v. Rumania", 4/5/00, *application* no. 28341/95. Disponible en: https://is.gd/6hdoAv [Enlace verificado el día 11 de septiembre de 2024].
[188]TEDH, "Amann v. Switzerland", 16/2/00, *application* no. 27798/95. Disponible en: https://is.gd/tgdDuf [Enlace verificado el día 11 de septiembre de 2024].
[189]VON HIRSCH, "Cuestiones éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión". INDRET, Revista para el análisis del derecho, 2007, p 15.

no permite tener en consideración que, de acuerdo a lo expuesto por Han, la topología de la violencia en este nuevo panóptico se relaciona con un proceso interno que obliga al sujeto a vender su intimidad. En estos tiempos, los individuos proporcionan sus datos a la red e interactúan en ella, muchas veces por necesidad y eso, bajo los criterios conocidos, los deja vulnerables para hacer valer su privacidad.

El interrogante que se construye es cómo se podría evaluar una expectativa razonable de intimidad en estos términos. En este sentido, una solución sería aplicar la lógica de la integridad contextual —desarrollada por Nissenbaum[190]— para valorar si existen expectativas razonables de intimidad, incluso en espacios públicos en la red.

Para el autor, los avances tecnológicos han convertido al espacio público en una realidad hipermediada, que no se condice con la presencia física y genera divergencia entre el concepto de esfera privada y el significado real de privacidad. Así, las teorías filosóficas y jurídicas conocidas no logran dilucidar el problema que supone encontrar datos privados en espacios públicos[191].

Su marco teórico parte de la base de que, previo a estas innovaciones, no existía una vigilancia del espacio público como la actual, donde el procesamiento, tratamiento y análisis de datos son moneda corriente. A partir de esto, se deben olvidar las categorías conocidas (público frente a privado, gobierno frente a privado, etcétera) y dar paso al principio de la privacidad como integridad contextual[192].

El autor propone que la posible violación a la privacidad debe ser evaluada por las normas que regulan el flujo de información en que cada persona la proporciona. Es decir, el derecho a la intimidad sería el derecho al apropiado flujo de información, porque las normas que lo regulan son de propiedad y de distribución. Las primeras, se refieren a los datos que se consideran pertinentes revelar en un contexto determinado (cuando una persona debe emitir un voto en un proceso electoral, la autoridad le solicita el DNI pero no la libreta de casamiento) y, las segundas, a cómo se traslada o se distribuye esa información (el destinatario)[193].

A modo de ejemplo, partiendo de esa lógica, si los datos personales fueron requeridos por aplicaciones privadas o públicas y, a raíz de una filtración, son recolectados por personal policial sin autorización previa, se habrá violado las normas de

[190]SANCHEZ "La Privacidad como integridad contextual y su aplicación a las redes sociales", *ZER*, Vol. 20,Nº39,2015 (https://is.gd/vbLwvN; última visita: 11 de septiembre de 2024).
[191]Idem, p. 165.
[192]Idem, p. 167.
[193]Idem, pp. 169/70.

distribución. De la misma manera, si una persona mantiene una conversación en su perfil de red social con otra y es recabada por tareas de ciberpatrullaje (sin recaudos legales), corresponderá su exclusión del proceso, por haberse violado la regla de distribución (destinatario), ergo, el principio de intimidad como integridad contextual.

Esta forma de reinterpretar esta expectativa, daría la posibilidad de equilibrar, por un lado, la intimidad de las personas cuando navegan en la red, fomentando un espacio libre de intromisiones indebidas y, por el otro, el desarrollo de métodos de prevención acordes a un Estado de Derecho.

Para concluir, se debe destacar que, en la actualidad, las nuevas formas de interacción social pueden darse en un plano material o digital. No amparar constitucionalmente aquello que se realiza en la red por considerar que es público es darle la espalda a esta nueva realidad y desentenderse de los fines constitucionales de las garantías.

VII) Conclusiones

Las nuevas tecnologías de investigación traen aparejados nuevos desafíos a la hora de evaluar su legalidad y, si se desea perpetuar los valores de la Constitución Nacional, no es conveniente aplicar soluciones viejas a problemas nuevos.

Se entiende que la obtención de prueba mediante ciberpatrullaje sin orden judicial previa —hasta tanto no esté regulada por ley— podría afectar la intimidad, pues, en base a los argumentos expuestos, existiría una real expectativa de privacidad respecto a los datos que suben las personas a fuentes abiertas o irrestrictas.

Esto, debido a que el análisis de esta nueva realidad virtual, a los fines de convalidar investigaciones policiales, no puede partir de los mismos conceptos de antaño. El cambio de paradigma obliga a repensar los criterios para analizar esta nueva sociedad transparente. Como destaca Han, debe reinventarse el concepto de libertad e intimidad, para poder escapar a la lógica de violencia microfísica que genera vigilancia y control masivo en un contexto panóptico. De la misma manera, la interpretación de las garantías constitucionales, que son la forma de proteger el ejercicio de esos derechos, también debe adaptarse, para no vaciarse de sentido.

De esta forma, si se parte de la base de que existe una dación de datos —cuanto menos— sin razón aparente, se debe considerar que el monitoreo, recolección y análisis de esos datos con fines preventivos o predictivos debería estar limitado por ley o, en ausencia, por principios de actuación, para evitar su ejercicio abusivo. En esa tesitura, la

CIDH[194] estableció que el derecho a la intimidad no es un derecho absoluto, pero las exigencias para ingresar a ese ámbito debían estar: reguladas por ley en sentido material y formal, perseguir un fin legítimo, y cumplir con los principios de idoneidad, necesidad y proporcionalidad, propios de una sociedad democrática.

En esa línea, el protocolo nro. 144/2020 estableció criterios para evaluar si el ciberpatrullaje violaba derechos fundamentales y a comparación de la regulación actual, resultan convenientes para valorar la incorporación de las pruebas recolectadas, hasta tanto se sancione una ley específica. Sobre todo, teniendo en cuenta que la resolución nro. 720/22, pese a estar derogada, detalló que la ejecución de medidas de investigación en el ámbito digital, debe ser a petición de las autoridades jurisdiccionales por la tensión existente con la ley de protección de los datos personales y que, el hecho de que los datos estén en una fuente digital abierta, no implica que quien trate esos datos no deba cumplir con los principios establecidos en la ley.

Las recientes Resoluciones no dan respuesta acabada a estos interrogantes (pese a que enumera lineamientos, y no principios) y suman, además, el uso de *softwares* basados en inteligencia artificial y otras innovaciones, con los riesgos y problemas indicados.

Para finalizar este trabajo y a modo de reflexión para evaluar su contenido, resulta conveniente rememorar la definición de Han respecto al "justo" como "(…) aquél que escucha más a las cosas que a sí mismo (…) que se reserva su juicio, que siempre llega demasiado pronto (…). La justicia se ejerce manteniendo en suspenso la convicción propia, la opinión propia sobre el otro, oyendo y escuchando, absteniéndose uno del juicio propio, es decir, absteniéndose de sí mismo. Pues, en perjuicio del otro, el yo siempre llega demasiado pronto. Aquel singular abstenerse de juzgar no puede proceder del poder en cuanto a tal: de él no es propia la vacilación. El poder en cuanto tal nunca se niega a juzgar al otro o a pensar sobre él. Más bien consta de juicios y convicciones"[195].

Ya sea mediante un debate parlamentario o a través de criterios jurisprudenciales novedosos, el objetivo primordial será lograr un equilibrio entre el derecho a la intimidad de las personas y la lucha contra los delitos en el ciberespacio, propios de una sociedad democrática y de un Estado de Derecho.

[194]CIDH, "Tristán Donoso", 27/1/19 (https://is.gd/QuHVGi;última visita el día 14 de agosto de 2024) y "Escher y otros", 20/11/09. Disponible en: https://is.gd/6QnWWQ[Enlace verificado el día 11 de septiembre de 2024].
[195]HAN, *Sobre el poder* (Traducción a cargo de CIRIA), 1 ed., Herder, 2014, Barcelona, p. 80. Disponible en: https://is.gd/7fCPrO [Enlace verificado el día 11 de septiembre de 2024].

VIII) Bibliografía

Libros

.-AROCENA, Valoración de la prueba, 1 ed., Hammurabi, Buenos Aires,2020.

.- BASTERRA, Acceso a la información pública y transparencia, 1 ed., Astrea, Buenos Aires, 2018.

.-BENTIN, "El agente encubierto en el ciberespacio: la ausencia de regulación en la argentina y su impacto en las garantías constitucionales" en DUPUY, Innovación en investigaciones digitales, 1ed., Hammurabi, Buenos Aires, 2022.

.-BENTHAM, Tratado de legislación Civil y Penal, 1 ed., México, Edigráfica, 2004.

.-CANDIOTTO/ARGIBAY MOLINA, Ciberpatrullaje, 1 ed., Hammurabi, Buenos Aires, 2020.

.-CHARAJA COATA, ¿Existe un derecho al propio entorno virtual?,1 ed., Hammurabi, Buenos Aires, 2022.

.-COPPOLA/CAFFERATA NORES, Verdad procesal y decisión judicial, 1 ed., Alveroni, Córdoba, 2014.

.-DANESI, Inteligencia artificial, tecnologías emergentes y derecho 1, 1 ed, Hammurabi, Buenos Aires, 2020.

.-D'ALBORA, Código Procesal Penal de la Nación. Anotado, comentado y concordado, Tomo I, 1 ed, LexisNexis, Abeledo-Perrot, Buenos Aires, 2005.

.-DOBRATINICH, Derecho y nuevas tecnologías, 1ed., La Ley, CABA, 2021.

.-FERRAJOLI, Derecho y razón. Teoría del garantismo penal, 1 ed., Trotta, Madrid, 1995 y Por una Constitución de la Tierra. La humanidad en la encrucijada, 1 ed., Trotta, Madrid, 2022.

.-FOUCAULT, La verdad y las formas jurídicas, 5ta. ed., Gedisa, Barcelona, 2017.

.-GAMEN, La privacidad y las nuevas tecnologías, 1. ed, Hammurabi, Buenos Aires, 2023.

.-GUZMÁN, La verdad en el proceso penal: una contribución a la epistemología jurídica, 2da. Edición, Del Puerto, CABA, 2011.

.-HAN, La sociedad de la transparencia, 1 ed., Herder, Barcelona, 2013; Psicopolítica: neoliberalismo y nuevas técnicas de poder ,1ed.,Herder,Barcelona,2014; Topología de la violencia, 1 ed., Herder, Barcelona, 2016; La sociedad del cansancio, 1 ed, Herder, Barcelona, 2012 y Sobre el poder, 1 ed., Herder, 2014, Barcelona.

.-IBAÑEZ,Contratos,1ed.,Hammurabi,BuenosAires,2021.

.-KIEFER, "Daño informático", en DUPUY, CIBERCRIMEN, 1º Ed., B de F., Buenos Aires, 2018.

.-MAIER, "Derecho Procesal Penal. Tomo I. Fundamentos", 2da. Ed., Editores del Puerto, Buenos Aires, 1996 y Derecho Procesal Penal. Tomo 3. Parte general. Actos procesales, 1 ed, Del Puerto, CABA, 2011.

.-PASTOR/HAISSINER, Neurociencias, tecnologías disruptivas y tribunales digitales, 2 ed., Hammurabi, BuenosAires,2019.

.-POLANSKY, Garantías constitucionales del procedimiento penal en entorno digital, 1 Ed., Hammurabi.

.-RIQUERT, Ciberdelitos, 2da. ed, Hammurabi, Buenos Aires, 2020 y Sistema penal e informática, vol. 7. 1 ed, Hammurabi, Buenos Aires,2024.

.-SALT/POLANSKY, La investigación penal en el entorno digital, vol. 3, 1 ed,, Hammurabi, Buenos Aires, 2023.

.-STRATIOTIS, "Los allanamientos remotos y el uso de drones", en DUPUY, "Innovación en investigaciones digitales",1ed.,Hammurabi,Buenos Aires,2022.

.-SUEIRO, Vigilancia Electrónica y otros modernos medios de prueba, 2 ed. Hammurabi, Buenos Aires, 2019.

.-VANINETTI, Derecho a la intimidad en la era digital, vol. I,1 ed., Hammurabi, Buenos Aires, 2020 y Derecho a la intimidad en la era digital, vol. 3, 1º ed,, Hammurabi, Buenos Aires, 2021.

.- WAJCMAN, El ojo absoluto,1 ed., Manantial, Buenos Aires, 2011.

Artículos

.-AGUILAR RIVERA, "Transparencia. ¿nueva o vieja?", Transparencia y Democracia. Claves para un concierto.

.-ACNUDH, "El derecho a la privacidad en la era digital Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos Distr. General",13/9/21 y "El derecho a la privacidad en la era digital", 4/8/22.

.-BOTTO, "La cuarta revolución industrial una visión economicista del cambio social", Question/Cuestion, Vol.2,2020.

.-COBOS ORIHUEL, "El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado".

.-CUATRECASA MONFORTE, "La inteligencia artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos".

.-EDWARDS/URQUHART, "Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence?".

.-ORTIZ PRADILLO, "La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación".

.-RIOS, "Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras",IDP,Nº36,2022.

.-ROCA MARTÍNEZ, Procesos y prueba prohibida. 1 ed., Dykinson, Madrid, 2022.

.-SANCHEZ "La Privacidad como integridad contextual y su aplicación a las redes sociales", ZER, Vol. 20,Nº39,2015.

.-RIQUERT, "Libertad vs seguridad: nuevas tensiones a propósito del ciberpatrullaje y la creación de la unidad de inteligencia artificial aplicada a la seguridad".

.-SCHATZKY/ZARA, "Inteligencia basada en fuentes abiertas (OSINT) en Argentina: un diagnóstico sobre su utilización por parte del Estado", Revista pensamiento penal, Nº 483,2023.

.-TAVOLA SERRA, "Vigilancia e investigación policial en el ciberespacio: aspectos procesales del ciberpatrullaje", IDP, 2022.

.-VON HIRSCH, "Cuestiones éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión". INDRET, Revista para el análisis del derecho, 2007.

.-ZARA, "Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay", Revista pensamiento penal, 483, 2023.

Normativa

.-Declaración Universal de los Derechos Humanos (artículo número 12); Pacto Internacional de Derechos Civiles y Políticos (artículo número 17); Constitución Nacional (artículos números 1,18,19,33 y 75 inc. 22); Leyes nacionales: 17.671, 25.326, 25.520, 25.873, 27.063, 27.275 y 27.411; Leyes CABA: 1.845, 5.688 y 6.339;Decretos del PEN: 1558/2001 ,1501/09 , 1563/2004, 1766/2011 31/2018, , 720/2022, 428/2024 y 710/2024; Otros decretos y resoluciones: y 398/2019.

Jurisprudencia nacional

.- CSJN: "Spinosa Melo, Oscar Federico" (Fallos 329:3617), "Charles Hermanos y otro" (Fallos 46:36), "Montenegro, Luciano Bernardino s/robo", (Fallos 303:1938), "Fiorentino, Diego Enrique s/tenencia ilegítima de sustancia estupefaciente" (Fallos 306:1752), "Francomano" (Fallos. 310:2402), "Daray" (Fallos 317:1985), "Paulino" (Fallos 528;46); "Rayford" (Fallos 308:733), "Halabi, Ernesto s/amparo ley

16.986" (Fallos 318:2148), "DGI. c/ Colegio Público de Abogados" (Fallos 319:71), Costa, Héctor Rubén" (Fallos 310:508) y "Franco, Julio César", (Fallos 330:4615).

.-CFCP: Sala II, "URSIC, Alfredo Gerardo y otros s/ recurso de casación", (Nº FSM 25882/2019/TO1/CFC13) y Sala IV, "Bejarano, Alexis Ezequiel s/recurso de casación" (causa nro. CCC 17200/2013/TO2).

.- CCCF: Sala II, "D. C. N., F. F.X. s/procesamiento" (CFP 889/2018/3/CA1) y Sala I, "Ministerio Público Fiscal s/recurso de apelación" (CFP 8991/2019/11CA5).

.- CÁMARA FEDERAL DE MAR DEL PLATA, "SG2", causa nro. FMP 1110/2017.

.- CATyRC, Sala I, "Observatorio de Derecho Informático y otros c/GCBA s/amparo y otros", (expediente 182908/2020).

.-CÁMARA DE APELACIONES DE GENERAL ROCA, "Sandoval y otros", (FGR 787/2021/CAI).

.-CÁMARA DE APELACIONES Y GARANTÍAS EN LO PENAL DE BAHÍA BLANCA, Sala I, "NN", (Expediente IPP 17673/I).

- JCCF Nº 9, "G,R y otros s/violación de correspondencia" (causa nro. CCC 55276/2019).

.-JCCF Nº 5, "Robles, Silvio Federico s/averiguación de delito" (causa nro. CFP 16/2023).

.- JCAyT Nº 4 "ODIA y otros contra GCBA s/amparo", 7/9/22 (expediente número 182908/2020).

Jurisprudencia internacional

.- CIDH: "Tristán Donoso" 27/1/19 y "Escher y otros", 20/11/09.

.- TEDH: "Glukhin v. Russia", (4/7/23, sentencia 11519/20); "Benedik contra Eslovenia" (24/4/18; sentencia 62357/14); "Shimovolos contra Rusia" (21/6/11, sentencia *30194/09)*; Brunet contra Francia" (08/10/09, sentencia 12662/06); "Szabó y Vissy. C. Hungría (12/01/2016, sentencia 37138/14); Big Brother Watch y otros contra el Reino Unido" (13/09/2018; sentencia 58170/13) TEDH, "Peck v. United Kindom", 28/1/03 (sentencia no. 44647/98), TEDH, "Rotaru v. Rumania" (4/5/00, sentencia 28341/95) "Amann v. Switzerland" (16/2/00, sentencia 27798/95).

.- Tribunal de la Haya "SyRi".5 de febrero de 2020.

.-TRIBUNAL CONSTITUCINAL ALEMÁN: 9 Sentencia de la Primera Sala, del 15 de diciembre de 1983 (1 BvR 209, 269, 362, 420, 440, 484/83).

.- Corte Suprema de Estados Unidos: "Florida v. Riley" (23/1/89), Weeks v. United States" (24/2/14), "Silverthorne Lumber Co. v. United States" (26/6/20), "Dow Chemical" (19/5/1986), "Kyllo" (11/6/01) y "Jones" (23/1/2012).

.- TRIBUNAL SUPREMO DE ESPAÑA, Sala de lo penal, "Evelio, Ildefonso e Rosana por el delito de tráfico de sustancias estupefacientes" (20/4/2016, STS 1709/2016); 342/2013 (17/4/13) ; 173/2011 (7/11/11); 204/2016 (10/3/2016).

Páginas web

.- https://www.transparency.org/en/what-is-corruption;

.- https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm.

.- https://www.argentina.gob.ar/salud/inc/institucional/trasparencia.

.- https://www.argentina.gob.ar/normativa/nacional/decreto-1501-2009-159070.

.- https://historia-biografia.com/byung-chul-han/.

.- https://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/28130/texact.htm.

.- http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm.

.- https://boletinoficial.buenosaires.gob.ar/normativaba/norma/342041.

.- https://boletinoficial.buenosaires.gob.ar/normativaba/norma/533894.

.- https://boletinoficial.buenosaires.gob.ar/normativaba/norma/464360.

.- https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

.-https://www.mpf.gob.ar/pia/la-pia-identifico-una-gran-cantidad-de-consultas-respecto-de-distintos-organismos-que-se-encuentran-afectados-en-la-causa-que-investiga-el-posible-uso-ilegitimo-de-datos-del-renaper/.

.-https://www.ambito.com/caba-realizo-seguimientos-biometricos-jueces-y-fiscales-fallos-clave-cfk-n5721183.

.- https://dle.rae.es/ciberespacio.

.- https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

.- https://dle.rae.es/software.

.- https://dpej.rae.es/lema/big-data.

.-https://dle.rae.es/miner%C3%Ada.

.- https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-31-2018-308531/texto.

.- https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=338229.

.-https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf.

.- https://adc.org.ar/wp-content/uploads/2020/04/Regulacion-OSINT-SOCMINT.pdf.

.-https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-720-2022-373942/texto.

.- https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528.

.- https://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/100806/norma.htm.

.-https://www.cels.org.ar/web/2021/01/la-justicia-federal-sobreseyo-a-kevin-guerra-por-sus-expresiones-en-twitter/.

.-https://www.lanacion.com.ar/seguridad/gorra-leaks-despues-de-siete-anos-fue-detenido-el-hacker-que-robo-la-base-de-datos-de-la-policia-nid31012024/.

.-https://www.perfil.com/noticias/actualidad/paternidad-de-la-hija-de-gerardo-morales-la-justicia-de-jujuy-detuvo-e-imputo-a-dos-personas.phtml.

.- https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368.

.-https://www.clarin.com/sociedad/adictivas-peligrosas-nueva-york-justicia-principales-redes-sociales_0_7lr4kScoe6.html.

.-https://www.hrw.org/es/news/2020/04/02/declaracion-conjunta-de-la-sociedad-civil-los-estados-deben-respetar-los-derechos.

.- https://www.echr.coe.int/documents/d/echr/fs_new_technologies_eng.

.- https://www.cia.gov/static/9d89dd9a4fe41b63cfab00c5191a8803/IC-OSINT-Strategy.pdf.

.-https://www.openglobalrights.org/landmark-judgment-from-netherlands-on-digital-welfare-states/?lang=Spanish.

.-https://globalfreedomofexpression.columbia.edu/cases/peck-v-the-united-kingdom/#:~:text=The%20Chamber%20of%20the%20Fourth,to%20press%2C%20wherein%20the%20applicant.

.- https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368.