“Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas.”[1]

Martina Monte y Santiago Ignacio Sánchez

I. La complejidad de la distinción jurídica entre lo público, lo privado y lo íntimo en las redes sociales

No cabe ninguna duda de que, durante las últimas décadas, a partir de la masificación de internet, surgieron nuevas y múltiples formas de comunicación virtual. En ese marco, y desde enfoques sociológicos, se desarrollaron conceptos como los de “*sociedad de la información*”[2] o “*sociedad-red*”[3] para designar el nuevo paradigma tecnológico y la manera en que afectó a las distintas formas de organización social a lo largo y ancho del mundo.

Esto dio lugar a que las distinciones sobre lo público, lo privado y lo íntimo se volvieron más ambiguas y difusas[4], y por ende, más problemáticas para el derecho, y,

[1] El presente artículo surgió como fruto de un trabajo de investigación final realizado para la materia “Régimen del Proceso Penal”, a cargo del Dr. Matías Mancini, para la orientación en derecho penal de la carrera de abogacía, de la Facultad de Derecho de la Universidad de Buenos Aires (UBA). Agradecemos las correcciones y comentarios realizados por el Profesor Mancini.

[2] El concepto de “*sociedad de la información*” fue primeramente acuñado por el sociólogo holandés Jan Van Dijk en su obra “The Network Society: Social Aspects of New Media” (*disponible online en idioma inglés en: http://www.forschungsnetzwerk.at/downloadpub/The_Network_Society-Jan_van_Dijk.pdf*).

[3] El concepto de “*sociedad-red*”, acuñado por el sociólogo español Manuel Castells, hace referencia a la comprensión de la sociedad como una estructura social hecha de redes de información, articulada en torno de las nuevas tecnologías de la información. Ver: Castells, M . (2006). La Sociedad Red, Madrid, Alianza Editorial, 2006.

[4] Siguiendo el clásico desarrollo de **Carlos Nino**, la privacidad podría significar una posibilidad ilimitada de acciones, siempre que ellas no supongan una afectación a terceros, ya sea que se realicen en público, o bien en un espacio cerrado, alejado de la mirada del resto de la sociedad. Por el contrario, “lo íntimo” se encuentra relacionado con todas aquellas esferas personales que quieran ser dejadas al margen del conocimiento generalizado, que podrían incluir aspectos vinculados con el cuerpo, la propia imagen, pensamientos, emociones, circunstancias de la vida familiar, etc. Véase: Nino, C. (2005). Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional, Buenos

especialmente para el derecho penal y la investigación del delito. En el contexto de esos avances, y específicamente desde la década de los noventa, los distintos ordenamientos jurídicos intentaron atrapar estos nuevos fenómenos.

En esa dirección, las primeras normativas surgieron con ciertas notas conservadoras, en la medida en que se encontraban restringidas a marcos nacionales, o, a lo sumo, regionales, y carentes de una perspectiva internacional o *desterritorializada*, pero aun así significaron cambios. Tal es el caso de las primeras normas dentro de la Comunidad Europea.[5]

Con el paso de los años, el cambio se sentiría también en el derecho penal y procesal penal, y especialmente, en relación a la complejidad de las conductas desplegadas dentro de la infraestructura virtual que provee internet. De acuerdo con Maximiliano Ruiz[6], la cuestión del territorio y el espacio resultan las dimensiones más relevantes del impacto que las nuevas tecnologías generaron sobre las normas penales: "la trama fáctica en los ciberdelitos podrá atravesar diferentes fronteras, dando inicio en un Estado bajo normas penales distintas a las de otro en el cual produce sus resultados y pudiendo a su vez, ramificar sus efectos hacia diversos espacios geográficos con una multiplicación de riesgos o daños concretos a víctimas indeterminadas".[7]

Aires, Ed. Astrea, 2005, p. 334. Por su parte, también **Alejandro Carrió** subraya la existencia de un "ámbito personal protegido" en el marco del proceso penal, articulado en torno al artículo 18 de la Constitución Nacional, que podría comprenderse como la base de "la intimidad" para nuestro ordenamiento jurídico. Así, según este autor, existen zonas de reserva o intimidad, ajenas a la interferencia estatal, que no aparecen de manera explícita en la Constitución Nacional, pero que no deben ser consideradas ajenas a la protección constitucional: tal el caso de las conversaciones telefónicas, los objetos dentro de un vehículo, o, incluso, un diálogo proferido en un bar. Véase: Carrió, A. (1994). Garantías constitucionales en el proceso penal, Buenos Aires, Ed. Hammurabi, pp. 269-270.

[5] Arévalo Mutiz, M; Navarro Hoyos, J; García Leguizamón, F; Casas Gómez, C. (2011). Modelos de regulación jurídica de las redes sociales virtuales, en: *Revista Via Iuris*, ISSN 1909-5759, Nº. 11, 2011, págs. 109-136. Disponible online en: https://dialnet.unirioja.es/servlet/articulo?codigo=3956735 (consultado 13/6/2020).

[6] El autor es abogado por la Universidad de Buenos Aires, Secretario de Primera Instancia en el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires, Especialista en Nueva Delincuencia por la Universidad de Salamanca, España, y profesor visitante en el Posgrado de Especialización en Derecho de Alta Tecnología de la Universidad Católica Argentina.

[7] Ruiz, M. (2018). Ciberterritorialidad: ¿Un nuevo principio de aplicación espacial de la ley penal?, MJ-DOC-13562-AR | MJD13562, en: *Revista MicroIuris.com Inteligencia Jurídica*, 5 de Julio de 2018.

De todos modos, más allá de esos efectos, nos interesa remarcar que las nuevas normativas podrían suponer una reformulación jurídica de lo público, lo privado y lo íntimo, siempre en el contexto de las nuevas tecnologías de la información y comunicación. Resulta especialmente problemático, entonces, responder si para el Derecho es factible hacer una traducción de las nuevas plataformas y tecnologías al ámbito normativo propio de las comunicaciones clásicas: si los límites entre el ámbito de lo privado, lo íntimo y lo público se modifican, entonces surge el interrogante acerca de la capacidad y justificación para que sea admisible la injerencia de las autoridades en esos espacios redefinidos.

Esto lleva aparejadas una serie de cuestiones: por un lado, el problema de la construcción de una "mínima sospecha razonable" a la hora de investigar y patrullar las redes sociales/actividades sociales en entornos virtuales, y por otro, la aplicación de los principios de proporcionalidad y razonabilidad a la hora de fundar una injerencia estatal en los nuevos entornos. En este marco, sin intenciones de ingresar en el campo sociológico, no es arriesgado afirmar que lo privado ya no surge –únicamente- de la inmunidad de aquellas conductas ajenas a la interferencia estatal, que no impliquen una afectación a terceros.

Esa mirada clásica suponía el resguardo de lo privado, como derecho a mantener ciertos niveles de la vida individual, las conductas y la personalidad, por fuera de la supervisión pública. No obstante, en la actualidad, existe una dimensión considerable de lo privado que, lentamente, se incrusta en la lógica de lo que –anteriormente- se consideró como exclusivamente público.[8]

Del mismo modo, a partir de las nuevas formas de comunicación virtual, también existe una reducción de lo privado y lo íntimo frente al espacio de lo público y comunitario. En esta instancia, se pueden inscribir algunos de los planteos sobre el derecho a la privacidad y a la intimidad realizados por Kenji Yoshino, jurista y profesor de la Universidad de Yale, para quien, no sólo se relacionan con el derecho autónomo

---

Disponible online en: https://aldiaargentina.microjuris.com/2018/11/06/ciberterritorialidad-un-nuevo-principio-de-aplicacion-espacial-de-la-ley-penal/ (consultado 14/6/2020).

[8] Garzón Valdés, E. (1999). Privacidad y publicidad. *Revista Jurídica de la Universidad de Palermo*, p. 7; citado en: Garibadi, G. Op. Cit.; p. 82.

del individuo a delinear su plan de vida, sino que, además, involucran la cuestión vinculada a la voluntad del sujeto de hacer público algún aspecto privado de su vida.[9]

De esta manera, podría pensarse que el ámbito de reserva incluye, para ser realmente operativo, la posibilidad de exhibir o manifestar aspectos vinculados al propio individuo y su plan de vida, en el devenir de su convivencia social. En términos del autor, existe una simetría entre el derecho a la privacidad y el derecho a la libertad de expresión.

Algunos autores sostienen una clasificación de las teorías del derecho a la privacidad como "control" –específicamente para el caso de los Estados Unidos- o como "dignidad", siendo éste el caso de la normativa europea. Dentro de este última concepción, "la privacidad conlleva el derecho a construir diferentes 'personalidades situacionales', por lo que el individuo divulga aspectos de su privacidad en diferentes ambientes y en diferentes contextos".[10] Ello sería esencial para el desarrollo de la personalidad del ser humano.

Utilizando estos conceptos, podemos sostener que las redes sociales y los vínculos establecidos a través de plataformas virtuales refuerzan la imbricación entre los ámbitos privado, íntimo y público. Por lo tanto, ello supone la necesidad de un reacomodo de los criterios de intervención estatal de ese tipo de comunicaciones.

En este orden de ideas, podría sostenerse que una manifestación vertida sobre una red social, que pueden leer cientos de personas ("contactos"), es una expresión que se ubica en el ámbito de lo público, ya sea por su alcance, ya por su accesibilidad. No obstante, siguiendo los lineamientos esgrimidos más arriba, surge el interrogante sobre el nivel de autonomía que se le permitiría alcanzar a un individuo, si lo expresado en el marco de una red social puede automáticamente ser objeto de injerencia estatal, sin

[9] Yoshino, Kenji (1999), *El Derecho a la publicidad*, en: Revista Jurídica de la Universidad de Palermo. Disponible online en: https://www.palermo.edu/derecho/publicaciones/pdfs/revista_juridica/Especiales_SELA/SELA%201998%20-%20Ed%201999/04SELA98Juridica04.pdf (consultado 14/6/2020). Según Yoshino, un ejemplo concreto del "derecho a hacer público" como aspecto fundamental del derecho a la privacidad, puede encontrarse en el caso de los soldados norteamericanos gays, y la política interna de las Fuerzas Armadas de Estados Unidos. Allí, observa Yoshino, existe una política de ocultamiento (política del escondite), que impide la expresión abierta de toda orientación sexual de los miembros de las Fuerzas Armadas que no sea heterosexual, y de esa manera, restringe el ámbito de privacidad.

[10] Vaninetti, Hugo Alfredo (2020); Derecho a la intimidad en la era digital. 1. Derechos Personalísimos; Ed. Hammurabi; Buenos Aires, p. 50.

necesidad de autorización, por el carácter meramente "abierto" del mensaje (esto es, sin necesidad de que existan criterios de "sospecha" que habiliten la intervención de las autoridades).

Si el derecho "a hacer público" emerge simétricamente del derecho a la privacidad, ¿cuáles podrían ser los parámetros objetivos en la construcción de una "sospecha razonable", bajo la cual sea admisible que el Estado profundice en la investigación de las manifestaciones o conductas desplegadas por los individuos en el marco de las nuevas tecnologías de la información y comunicación? Para comprender mejor ese interrogante, se hace necesario ingresar en una problemática relacionada: las investigaciones con fuentes abiertas (o, como afirman las organizaciones sociales, "inteligencia masiva de fuentes abiertas"[11]) en el "ciberespacio".

A la luz de esa cuestión, a continuación se intentará realizar un análisis de caso: el reciente "*Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas*". El objeto será indagar en la manera en que, actualmente, las autoridades comprenden y conceptualizan los márgenes de injerencia sobre las comunicaciones virtuales y las redes sociales, y consecuentemente, ensanchan o angostan los espacios de privacidad e intimidad en la persecución de los delitos.

II. El ciberpatrullaje y la protección de los derechos a la privacidad y la intimidad.

II.A. Introducción a los conceptos de ciberespacio, técnicas de investigación OSINT y aproximación a algunos problemas asociados a su utilización con fines de inteligencia criminal.

La revolución informática, el acceso globalizado a la web y su impacto en las relaciones sociales es un hecho que, muchas veces, en la vida cotidiana resulta difícil de mensurar. En un intento estadístico aproximado por abarcar este fenómeno, la Internet World Stats nos informa que, actualmente en la Argentina, existen alrededor de 41.600.000 usuarios de internet, sobre una población aproximada de 45.200.000 de personas que, tal como lo indica el sitio, representa en términos porcentuales un nivel de

[11] Leandro Uciferri (2018), Seguidores que no vemos – Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT). CABA: Asociación por los Derechos Civiles. Disponible en: https://adc.org.ar/informes/seguidores-que-no-vemos/

penetración del 92%, siendo por lejos, la cifra más alta de conexión a la red en América Latina[12].

De modo similar ocurre en el ámbito de la telefonía móvil, en el cual se informa la existencia de alrededor de 66.360.000 de líneas telefónicas, lo que representa en términos porcentuales un nivel de penetración telefónica del 148.5%, que ubica a la Argentina en segundo lugar en el ranking de suscripciones a líneas telefónicas después de Uruguay.[13] En virtud de ello, podemos aseverar entonces que, entre las nuevas formas de interacción social, además de comunicarnos, comerciar, contratar y vincularnos, también existen nuevas formas de delinquir, y por lo tanto, también de investigar[14].

En consecuencia, toda actividad policial o de patrullaje en la red tendiente a la investigación para la prevención de delitos o a la "recolección, uso y análisis de información que estas nuevas formas de interacción social ofrecen"[15] en el marco de una investigación criminal, es conocida por su nombre en inglés como open source intelligence (OSINT) o, en español, como actividad de inteligencia de fuentes abiertas. Esta actividad es la que, hoy en día, a la luz de los derechos fundamentales, presenta fuertes tensiones constitucionales, especialmente si se la intenta armonizar con el derecho a la intimidad que mencionábamos más arriba.

Pero antes de avanzar en la definición del concepto de inteligencia de fuentes abiertas y sus alcances, nos parece pertinente definir en primer lugar, al ámbito en el que se realiza este tipo de actividad: el ciber-espacio. Para introducirnos en el concepto, Candiotto y Argibay Molina nos señalan que durante el último medio siglo, y a raíz del desarrollo de las tecnologías de la información y la comunicación, todos hemos sido

[12] Candiotto, M., & Argibay Molina, J. (2019). Investigación con fuentes abiertas de información en el proceso penal (OSINT). In M. Riquert & C. Sueiro, *Sistema penal e Informática* (1st ed., pp. 154-175). CABA: Jose Luis Depalma – Hammurabi; p. 154. Véase también: South America Internet Usage Stats and Population Statistics, 2017

[13] *Ibid*, p. 154. Véase también: South America Internet, Mobile Cellular Subscriptions and Facebook Users - Population 2020 Statistics, 2020

[14] Candiotto, M., & Argibay Molina, J. (2019). Investigación con fuentes abiertas de información en el proceso penal (OSINT). In M. Riquert & C. Sueiro, *Sistema penal e Informática* (1st ed., pp. 154-175). CABA: Jose Luis Depalma – Hammurabi; p. 154. Véase también: South America Internet Usage Stats and Population Statistics, 2017, p. 154.

[15] *Ibid*, p. 155.

testigos de la aparición de la virtualidad como una "nueva plaza de convivencia social" e interacción entre las personas.[16]

Esto ha sido posible, indudablemente gracias al diseño de "incontables mecanismos, herramientas y aplicaciones (…) [que han facilitado] la integración e interrelación de las personas, sin limitaciones espacio-temporales."[17]. Sin embargo, esta particularidad de no responder a las clásicas fronteras estaduales, convierte al ciber-espacio en una cuestión compleja para el derecho, que no ha avanzado a la par del desarrollo de las nuevas tecnologías.

Este es el caso de nuestro ordenamiento jurídico que, a pesar de no definir concretamente al ciberespacio como tal, define a las tecnologías de la información y las comunicaciones y a los recursos asociados a ella en la Ley 27.078 de "Argentina Digital". Así, el inciso i) del artículo 6 define a las primeras como "el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permitan la compilación, procesamiento, almacenamiento y transmisión de información", y el inciso d) a las segundas como "las infraestructuras físicas, los sistemas, los dispositivos, los servicios asociados u otros recursos o elementos asociados con una red de telecomunicaciones o con un Servicio de TIC que permitan o apoyen la prestación de servicios a través de dicha red o servicio, o tengan potencial para ello".

Además de estas dos últimas cuestiones – relacionadas a la inexistencia de una definición jurídica concreta sobre ciberespacio y la imposibilidad de su delimitación territorial-, otro de los elementos que caracterizan al espacio cibernético es el hecho de que toda interacción que se de en dicho ámbito, independientemente de su intensidad o frecuencia, "deja huelas digitales".[18] Estas "huellas", señalan los autores, "contienen información que queda, de alguna manera, registrada "sin importar quién sea el que, en definitiva, la comparte o ingresa. Sea el propio usuario o un tercero, lo relevante es que, al interactuar en el ciberespacio, ciertos datos quedarán disponibles para el público en general, a un solo clic de distancia".[19]

Esta última cuestión reviste de especial importancia a la hora de discutir acerca de los límites que hay entre los derechos a la privacidad y a la publicidad de lo privado de

[16] *Ibid*, p. 155.

[17] *Ibid*, p. 155.

[18] *Ibid*, p. 155.

[19] *Ibid*, p. 155-156.

los que hablábamos antes. Esto es así, debido a que la disponibilidad de las huellas digitales, pone bajo la lupa la discusión acerca del carácter público o privado de los datos, y por ende, de la información de las personas que se encuentra disponible en la red.

En este marco, la utilización de las técnicas de investigación OSINT para propósitos de inteligencia criminal resulta particularmente problemático toda vez que se exista este halo de duda en torno al carácter de la información obtenida, y por lo tanto, en torno a la construcción de nuevos estándares sobre mínima sospecha razonable que, en la era cibernética, justifiquen la intervención punitiva del Estado.[20] Esto inmediatamente nos lleva a preguntarnos acerca de si la información obtenida a través de estas técnicas es de carácter confidencial o si, por el contrario, ciertas garantías constitucionales se ven vulneradas para acceder a ella.

Por lo tanto, el problema central en este debate estriba en poder establecer de manera clara las fronteras entre la información privada, íntima y la de libre acceso público disponible en la web. Con el objetivo de contribuir a una solución para este problema, Candiotto y Argibay Molina realizaron un aporte que puede ser de gran utilidad a la hora de establecer el carácter de la fuente de la información obtenida, a partir de su clasificación en tres niveles.

De este modo, el primer nivel quedaría constituido por aquellas fuentes de información de "acceso libre", en el que no existen restricciones de ningún tipo para acceder a los datos allí alojados, como por ejemplo, señalan los autores, el Boletín

[20] Para las comunicaciones telefónicas, ya en el consabido fallo Quaranta de la CSJN, se estableció la necesidad de la existencia de una "mínima sospecha razonable" que funcione como criterio habilitante para el inicio de una investigación criminal y para la potencial injerencia estatal que pudiera sufrir la privacidad de una persona, en atención al interés público comprometido en la prevención y persecución del delito. Sin embargo, en el contexto planteado por este artículo, cabe interrogarse si todo rastro informático es pasible de ser instrumentalizado por las autoridades, sin más, con el objetivo de fundar una intervención estatal, o bien, si acceder a ese tipo de información requiere de una orden judicial previa, que permita primero localizarla, y después analizarla.

A nuestro entender, este último criterio es el que más se ajusta a una interpretación respetuosa de los derechos y garantías del implicado en el proceso. En este sentido, es necesario que el análisis de la información no sea realizado ex post facto, ya que de este modo, se vería deteriorado el carácter "inviolable" de las garantías en el marco de un proceso penal.

Para complementar este análisis, recomendamos la lectura del voto disidente del Dr. Petracchi en el fallo CSJN "Torres, Oscar Claudio y Rasuk, Eduardo Marcelo s/ ley 20.771 -Causa N° 37.252-", 19/05/1992" (citado en Quaranta).

Oficial.[21] Un segundo nivel de accesibilidad, quedaría configurado por aquellas fuentes de información de carácter "semi-público y no pago", en la cual se le exige al usuario de la plataforma que se registre como requisito previo a poder acceder a la información allí disponible, como por ejemplo sucede con la red social de búsqueda de empleo LinkedIn.[22]

Por último, existe un tercer nivel, que los autores denominan como "semi-público y pago", en el que el usuario debe, además de registrarse, abonar un importe, derecho o membresía para poder acceder a los datos que dicha fuente de información contiene. Tal es el caso, por ejemplo, de la plataforma Nosis.[23] Sin embargo, a pesar de lo útil que pueda resultar hacer esta clasificación de las fuentes de información, es necesario tener presente la ambigüedad que existe en los alcances de lo que puede considerarse como "información pública" o "privada", ya que dentro de cada uno de estos niveles, también pueden discriminarse datos de carácter tanto público como privado, y que puedan dar origen a confusión.[24]

Decíamos entonces, que a pesar de estas precauciones, existen cantidades ingentes de información en las redes, no pasibles de ser catalogadas como estrictamente confidencial (que potencialmente no hayan sido, bajo ningún modo, obtenida por medios ilegales), y que, sin embargo, resultarían difícilmente clasificables como información pública. De este modo se concluye que si bien, el carácter de la fuente de información (de acceso libre, semi- pública y no paga y semi- pública y paga) es un criterio necesario, no resulta suficiente para asegurar el carácter público o privado de la información que se encuentra alojada en la red.

En consecuencia, se plantea el problema relacionado a la posibilidad de establecer pautas o criterios explícitos que habiliten y fundamenten el relevamiento y almacenaje estatal de dicha información por parte del Estado. Esta problemática se intentará indagar

[21] *Op. Cit*, p. 158.

[22] *Ibid*, p. 158.

[23] *Ibid*, p. 159.

[24] Indudablemente, esta cuestión trae consigo muchos otros debates en torno a la privacidad de los datos personales, como lo son -por ejemplo- aquellos en relación a lo cuestionable que resulta el hecho de que las empresas lucren con la información personal de las personas sin su consentimiento, o el hecho de que para acceder a un mínimo de privacidad en la web deba pagarse un canon. Sin embargo, adentrarnos en temas como éstos, nos exigiría desviarnos del tema principal del presente trabajo.

en la siguiente sección, a la luz de la reciente resolución ministerial sobre "ciberpatrullaje".

II.B. El Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas

A partir de la resolución 144/2020, el Ministerio de Seguridad de la Nación aprobó un nuevo Protocolo en materia de prevención de cibercriminalidad. El contexto es el de la actual pandemia de Covid-19 y el decreto del P.E.N que dispone el Aislamiento Social Preventivo y Obligatorio (ASPO), en consonancia con la emergencia pública en materia sanitaria, establecida por la ley 27.541.

Sin embargo, el Protocolo no resulta absolutamente novedoso: su antecedente se encuentra en resoluciones del Ministerio de Seguridad, que datan de 2018, en donde se instruía a las fuerzas de seguridad a efectuar tareas de prevención en lo referido a la venta ilegal de armas, artículos que provengan de un delito, drogas, mensajes o imágenes que provengan de la explotación sexual, la trata y el tráfico de personas, etc. Según el documento transcripto en los considerandos de la resolución 144/2020: "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".[25]

En este sentido, tal como se hiciera referencia más arriba -al tratar las técnicas OSINT-, un aspecto problemático, sobre el que se centrará este análisis, estriba en la automática asociación entre el tipo de acceso a los sitios y el carácter de la información allí alojada. Si bien el Protocolo, en sus considerandos, tiene en cuenta la normativa internacional que define y protege privacidad e intimidad (PIDCP, CADH, Convenio de Budapest), a la vez que las objeciones realizadas por ONG de distinta índole, por otra parte, reafirma la necesidad de que, en el actual contexto, se refuercen las actividades de prevención policial.

Respecto de este punto, en la Res. 144/2020 se puede leer: "…las tareas que realizan los cuerpos policiales y fuerzas de seguridad en cumplimiento de su función preventora del delito no requieren autorización judicial, porque ello es parte de su tarea

[25] Poder Ejecutivo Nacional. Ministerio de Seguridad de la Nación. Resolución 144/2020, 31/05/2020, BORA N° 21811/20, publicado 02/06/2020.

específica como cuerpos policiales, y sus leyes orgánicas, según se ha visto, les imponen desarrollar y sustanciar la prevención del delito, mediante despliegues adecuados a la naturaleza y modalidad de cada delito o grupo de delitos."[26] Si bien resulta obvio que la actividad de prevención es facultad de las fuerzas de seguridad, la referencia a la posibilidad de desplegarla sin autorización judicial, resulta un segundo eje problemático.

En especial, es necesario distinguir aquí el tipo de actividad de prevención que se realiza: desde el punto de vista jurídico, es difícilmente equiparable una investigación con base en datos fehacientes, que permitan identificar a individuos concretos como posibles autores de un hecho delictivo determinado, con las tareas de vigilancia generalizada sobre la base de la compulsa masiva de información digital. En este segundo caso, podría existir un avance sobre información disponible en sitios de acceso abierto, pero que, en muchas ocasiones, pertenecen a una esfera privada que la persona tiene el interés de mantener en reserva.[27]

Para darle sostén a las tareas de vigilancia que se habilitan, en los considerandos del Protocolo se afirma: "esta labor de prevención del delito, para el caso de obtenerse, como resultado de ella, elementos que permitan sospechar o presumir la comisión de actividades delictivas, concluye con la puesta en conocimiento de la notitia críminis a los magistrados competentes del poder judicial o del ministerio público, según corresponda".[28] Luego, esas nociones se refuerzan mediante la cita del artículo 183 del Código Procesal Penal de la Nación.

Sin embargo, según ese artículo, las investigaciones de las fuerzas de seguridad, por iniciativa propia, deben estar basadas en denuncias o "en orden de autoridad competente", de manera que, de no mediar ninguno de esos dos supuestos, la existencia de una actividad delictiva hallada a partir del control general de la información virtual

[26] *Ibid,* párr. 13.

[27] Para pensar un ejemplo análogo, aquello sería semejante al seguimiento físico indiscriminado de las prácticas cotidianas de las personas (por ejemplo, concurrir a determinados lugares o espacios), y reconstruirlas como objeto de inteligencia. No caben dudas, en este último caso, que la investigación y vigilancia de una persona es una actividad que puede ser legítimamente llevada a cabo por las fuerzas de seguridad, pero nadie dudaría de que en esas circunstancias una autorización judicial sea un prerrequisito indispensable.

[28] Poder Ejecutivo Nacional, Ministerio de Seguridad de la Nación, Resolución 144/2020, 31/05/2020, BORA N° 21811/20, publicado 02/06/2020.

de las personas vendría a operar como una fundamentación ex post facto, similar a la que la CSJN considera como inadmisible en su famoso fallo "Quaranta."[29]

La Resolución 144/2020 menciona, más adelante, principios generales que serán rectores en la actividad de prevención: "sólo podrán efectuarse tareas de prevención del delito con uso de fuentes digitales abiertas en los casos en que ello sea el medio más adecuado para el objetivo buscado —principio de necesidad—. Que las tareas de prevención deberán ser idóneas y necesarias para evitar el peligro que se pretende repeler, ajustándose al logro de ese objetivo —principio de proporcionalidad—. Que la judicialización de las conductas prevenidas requerirá de un análisis en función de las características comunicacionales propias del medio en que se realizan —principio de razonabilidad—".[30]

Si bien estos principios pueden entenderse como garantías de las personas frente a la actividad de prevención, no existe en el Protocolo una definición previa de la medida de lo "necesario", "proporcional" o "razonable". El fundamento más sólido aparece al comienzo de la norma, cuando se citan explícitamente delitos que serán objeto de persecución y prevención, de donde pueden deducirse parámetros que delimitan el control estatal.

A pesar de ello, resulta complejo imaginar indicadores claros acerca de qué tipo de actividad de las personas en sitios de fuente abierta habilitan la intervención estatal, y –como se afirmó más arriba-, que el ingreso al ámbito de reserva individual no permita ser justificado ex post. En ese sentido, por ejemplo, la normativa bajo análisis menciona de manera expresa que "la protesta a través de redes sociales no formará parte de ningún indicador delictivo"[31], y luego se agrega que estará vedado obtener información, producir inteligencia o almacenar datos sobre personas o usuarios "por el sólo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales."[32]

Es arduo imaginar el modo en que esas categorías puedan ser excluidas del objeto de investigación por la propia criminalización que realizan las agencias del derecho

[29] CSJN, "Quaranta, José Carlos s/ inf. ley 23.737, causa n1 763C", 31/08/2010.

[30] Poder Ejecutivo Nacional, Ministerio de Seguridad de la Nación, Resolución 144/2020, 31/05/2020, BORA N° 21811/20, publicado 02/06/2020.

[31] *Ibid*, párr. 29.

[32] *Ibid*, párr. 36.

penal. Resurge, entonces, la cuestión de la distinción entre ámbito de reserva e información pública, y lo problemático de construir criterios/parámetros de "sospecha", que habiliten la prevención estatal.

Conclusiones

A lo largo del trabajo, se trató de reflexionar sobre la manera en que las nuevas formas de comunicación han producido una **matización de los conceptos clásicos de publicidad, privacidad e intimidad**, y se procuró recalcar que los **criterios** que tradicionalmente, a partir jurisprudencia y doctrina, se elaboraron para dar fundamento a la **intervención del estado** en ciertos ámbitos, sufrieron transformaciones. Con ese fin, se introdujeron las nociones de **"investigación de fuentes abiertas" y "huella digital"**.

Así, se pudo apreciar que el carácter de fuente abierta de cierta información, no obsta a que ésta pueda corresponder a esferas privadas, que necesiten de un fundamento legal para ser indagadas por las autoridades. Ese fundamento legal, puede decirse, significa nada menos que la construcción de **criterios claros y objetivos que justifiquen la recolección e indagación** de la información disponible en el ciberespacio.

Ese último problema condujo el análisis hacia otros interrogantes relacionados, esto es, los parámetros de que se dispone en la actualidad para construir lo que en la jurisprudencia se denominó "*mínima sospecha razonable*". Para ello, se tomó un análisis de caso: el Protocolo del Ministerio de Seguridad para el control de las fuentes abiertas de información. A partir del análisis concreto, se intentaron mostrar las dificultades en torno a la construcción de criterios objetivos de intervención.

A su vez, como problema relacionado, se dejaron sugeridas algunas derivaciones lógicas de lo anterior: la complejidad de la traducción jurídica de los principios de proporcionalidad y legalidad en la construcción de los parámetros de control y prevención en los espacios de fuentes abiertas. Este último aspecto resulta sumamente relevante, ya que el Protocolo se trata de una resolución ministerial, y aún no hay ley emanada del Poder Legislativo Nacional que regule la cuestión.

En este sentido, la construcción de estándares y criterios claros, aparece como una cuestión fundamental para evitar que, en la necesidad de indagar la información en espacios de fuentes abiertas, se comprometan garantías de orden constitucional.

Referencias

Arévalo Mutiz, M; Navarro Hoyos, J; García Leguizamón, F; Casas Gómez, C. (2011). Modelos de regulación jurídica de las redes sociales virtuales, en: *Revista Via Iuris*, ISSN 1909-5759, Nº. 11, 2011, págs. 109-136. Disponible online en: https://dialnet.unirioja.es/servlet/articulo?codigo=3956735 (consultado 13/6/2020).

Candiotto, M., & Argibay Molina, J. (2019). Investigación con fuentes abiertas de información en el proceso penal (OSINT). In M. Riquert & C. Sueiro, *Sistema Penal e Informática. Ciberdelitos. Evidencia Digital. TICS.* (1st ed., pp. 153-176). Buenos Aires: Hammurabi.

Carrió, A. (1994). Garantías constitucionales en el proceso penal, Buenos Aires, Ed. Hammurabi.

Garzón Valdés, E. (1999). Privacidad y publicidad. *Revista Jurídica de la Universidad de Palermo*.

Garibaldi, Gustavo (2010); Las modernas tecnologías de control y de investigación del delito: su incidencia en el derecho penal y los principios constitucionales, Buenos Aires, Ad-Hoc.

Nino, C. (2005). Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional, Buenos Aires, Ed. Astrea, 2005

Ruiz, M. (2018). Ciberterritorialidad: ¿Un nuevo principio de aplicación espacial de la ley penal?, MJ-DOC-13562-AR | MJD13562, en: *Revista MicroIuris.com Inteligencia Jurídica*, 5 de Julio de 2018. Disponible online en: https://aldiaargentina.microjuris.com/2018/11/06/ciberterritorialidad-un-nuevo-principio-de-aplicacion-espacial-de-la-ley-penal/

South America Internet Usage Stats and Population Statistics (2017). Consultado por última vez el 30 enero del 2021, en: https://www.internetworldstats.com/stats15.htm

South America Internet, Mobile Cellular Subscriptions and Facebook Users - Population 2020 Statistics. (2020). Consultado por última vez el 30 de Enero del 2021 en: https://www.internetworldstats.com/south.htm

Uciferri, Leandro (2018), Seguidores que no vemos – Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT). CABA: Asociación por los Derechos Civiles. Disponible en: https://adc.org.ar/informes/seguidores-que-no-vemos/

Vaninetti, Hugo Alfredo (2020); Derecho a la intimidad en la era digital. 1. Derechos Personalísimos; Buenos Aires, Ed. Hammurabi.

Yoshino, Kenji (1999), *El Derecho a la publicidad*, en: Revista Jurídica de la Universidad de Palermo.