ANUARIO DE DERECHO CONSTITUCIONAL LATINOAMERICANO
AÑO XXVI, BOGOTÁ, 2020, PP. 793-823, ISSN 2346-0849

Andrés López Cabello* **(Chile)**
Tomás I. Griffa** **(Argentina)**

Privacidad en redes sociales y vigilancia estatal: un desafío pendiente de la práctica constitucional argentina

RESUMEN

El monitoreo y análisis estatal de la información que circula en redes sociales ha ganado terreno en la Argentina. Presentado como la simple traslación de las tareas de prevención policial al ámbito digital, se alega que no afecta derechos fundamentales porque solo se vigila la actividad pública y, si es público, no hay privacidad. En este artículo exploramos lo engañoso de este supuesto dado que, así como en el espacio público "analógico" las personas tienen una razonable expectativa de privacidad, esto es igualmente aplicable en internet y, especialmente, en las redes sociales. Las actividades y expresiones en esos espacios abiertos son esferas de privacidad protegidas por el derecho internacional de los derechos humanos. Para gozar de este derecho en la era digital no es necesario el ocultamiento deliberado de nuestras acciones y expresiones.

Palabras clave: privacidad en línea; redes sociales; vigilancia.

* Abogado, Universidad de Chile; magíster en Relaciones Internacionales, Facultad Latinoamericana de Ciencias Sociales (Flacso, Argentina). Equipo de Litigio y Defensa Legal del Centro de Estudios Legales y Sociales (CELS), Argentina. andres.lopezc@gmail.com. https://orcid.org/0000-0002-9508-6884.

** Abogado, Universidad de Buenos Aires. Docente, Facultad de Derecho, Universidad de Buenos Aires. Equipo de Litigio y Defensa Legal del Centro de Estudios Legales y Sociales (CELS, Argentina). tomasgriffa12@gmail.com. https://orcid.org/0000-0001-9095-3355.

VOLVER A TABLA DE CONTENIDO

Privacy on social media and state surveillance.
A pending challenge for Argentine constitutional practice

ABSTRACT

State monitoring and analysis of information that circulates on social media has gained ground in Argentina. Presented as the simple transition of police prevention activities to the digital sphere, it is alleged that it does not affect fundamental rights because only public activity is monitored and, if it is public, there is no privacy. In this article we explore the deceptiveness of this assumption, since just as in the "analog" public space people have a reasonable expectation of privacy, this is equally applicable on the Internet and, especially, on social media. Activities and expressions in these open spaces are spheres of privacy protected by international human rights law. In order to enjoy this right in the digital age, it is not necessary to deliberately conceal our actions and expressions.

Keywords: Online privacy; social media; surveillance.

Schutz der Privatsphäre in sozialen Netzwerken und staatliche Überwachung: eine ungelöste Herausforderung für die argentinische Verfassungspraxis

ZUSAMMENFASSUNG

Die staatliche Beobachtung und Analyse der in sozialen Netzwerken verbreiteten Informationen hat in Argentinien an Bedeutung gewonnen. Indem sie als einfache Übertragung der vorbeugenden Tätigkeit der Polizei auf den digitalen Raum dargestellt wird, wird behauptet, dass hierdurch keine Grundrechte betroffen seien, weil diese Tätigkeit sich auf die Überwachung öffentlicher Aktivitäten beschränke und es daher keine Privatsphäre gebe. Im vorliegenden Beitrag soll dargelegt werden, dass diese Annahme insofern irreführend ist, als die Personen im „analogen" öffentlichen Raum eine angemessene Beachtung ihrer Privatsphäre erwarten können und diese Erwartung auch für das Internet und insbesondere für die sozialen Netzwerke gilt. Handlungen und Äußerungen in solchen offenen Räumen sind somit Teil der Privatsphäre, die unter den Schutz des internationalen Rechts der Menschenrechte fällt. Um im digitalen Zeitalter in den Genuss dieses Rechts zu gelangen, bedarf es keiner ausdrücklichen Verschleierung von Handlungen und Äußerungen.

Schlagwörter: Privatsphäre online; soziale Netzwerke; Überwachung.

Introducción

Luego de que en la Argentina se declaró la emergencia sanitaria por la pandemia del SARS-CoV-2 en marzo de 2020, en distintas provincias del país y con la intervención de diversas fuerzas policiales, una decena de personas fueron sometidas a procesos penales por expresiones en sus redes sociales.

Estos procesos se dirigían principalmente contra individuos que habían hecho alguna broma en sus redes sociales sobre la posibilidad de aprovechar la cuarentena para realizar saqueos y contra quienes habían compartido o elaborado piezas de desinformación. La mayoría de estas investigaciones se iniciaron por actuaciones autónomas de las fuerzas de seguridad. Realizando tareas de monitoreo en redes sociales, las divisiones de cibercrimen identificaron expresiones que, en su criterio, podrían constituir el delito de intimidación pública o el de incitación a cometer delitos. Así lo denunciaron a las autoridades del Ministerio Público correspondiente quienes impulsaron la acción penal.[1]

Esta práctica de monitoreo policial en las redes sociales, alegan los funcionarios, no es una extravagancia solo justificada en el contexto excepcional de la pandemia. En realidad, sería parte de las funciones tradicionales de prevención policial de las fuerzas de seguridad, pero en el ámbito digital. Asimilándola con las tareas de patrullaje policial en la vía pública, las autoridades han bautizado esta práctica de monitoreo de redes sociales como "ciberpatrullaje".

Estas formas de vigilancia han sido utilizadas, desde hace años, para impulsar procesos penales y en otros ámbitos. Por ejemplo, a raíz de tareas de inteligencia realizadas en redes sociales, en 2017 a decenas de activistas de organizaciones de la sociedad civil se les prohibió participar en la Conferencia Ministerial de la Organización Mundial del Comercio (OMC) que se celebraría en Buenos Aires. El Gobierno explicó que los activistas "habían hecho explícitos llamamientos a manifestaciones de violencia a través de las redes sociales, expresando su vocación de generar esquemas de intimidación y caos". Diversos afectados iniciaron acciones judiciales de *habeas data* contra el Ministerio de Relaciones Exteriores y la Agencia Federal de Inteligencia para conocer qué información se había recogido de sus redes sociales, qué autoridad recopiló esa información y en virtud de qué norma legal. En los procesos, el Gobierno se negó a proveer la información requerida, lo que ha sido convalidado por algunos tribunales y se encuentra bajo conocimiento de la Corte Suprema.[2]

Esta actividad de monitoreo y análisis del discurso público en las redes sociales es lo que se conoce como inteligencia de redes sociales (*Social media intelligence*, Socmint), que es un elemento dentro del más amplio ámbito de la inteligencia de

[1] Para una revisión de algunos casos de "ciberpatrullaje" durante la emergencia sanitaria, consultar Centro de Estudios Legales y Sociales (CELS), "Observaciones del CELS a la Resolución 31/2018 y al Proyecto de protocolo de ciberpatrullaje", *Sobre el Proyecto de protocolo de ciberpatrullaje* (Buenos Aires: CELS, 2020), https://www.cels.org.ar/web/publicaciones/sobre-el-proyecto-de-protocolo-de-ciberpatrullaje/.

[2] Véase Paula Litvachky *et al.,* "El secreto. La seguridad nacional como coartada para un Estado sin controles", en *Derechos humanos en la Argentina. Informe 2019* 9, ed. por CELS (Buenos Aires: Siglo XXI, 2019), 104 y ss.; Leandro Ucciferri, "Seguidores que no vemos. Una primera aproximación al uso estatal del Open-source intelligence (Osint) y Social media intelligence (Socmint)", Buenos Aires, ADC, 2018, https://adc.org.ar/informes/seguidores-que-no-vemos/.

fuentes abiertas (*Open source intelligence,* Osint). Como se verá, esta práctica sin control ni límites claros avanza sobre esferas del derecho a la privacidad que se encuentran protegidas por el derecho internacional de los derechos humanos (DIDH).

1. Aclaraciones previas

En este artículo, el foco de atención estará en el análisis del alcance y contenido del derecho a la privacidad en el derecho internacional de los derechos humanos, a la luz de los intereses humanos actuales, en que internet y la expresión e interacción pública en las redes sociales es parte esencial de la vida de millones.

Si bien no vamos a explorar los elementos del discurso "peligroso" perseguido con el "ciberpatrullaje", sí corresponde hacer algunas prevenciones, en tanto dichas expresiones están protegidas por el DIDH. Sobre este punto vale recordar que la libertad de expresión es "la piedra angular de todas las sociedades libres y democráticas",[3] y que conforme el derecho internacional, toda limitación debe ser legal, necesaria, razonable, proporcional y perseguir un interés legítimo.[4] El concepto de "restricción necesaria", huelga señalar, implica la existencia de una "necesidad social imperiosa"; no es suficiente que la limitación sea "útil", "razonable" u "oportuna".[5]

Estas exigencias, por cierto, se agudizan cuando la responsabilidad jurídica que se pretende es de naturaleza penal.[6] Los efectos represivos y disuasorios de la persecución criminal son, en principio, más intensos que en el ámbito civil, que puede habilitar mecanismos proporcionales para la reparación de daños.

En la Argentina hay jurisprudencia interesante en la que se ha acotado la aplicación de los delitos "contra el orden público". En línea con los precedentes Noto,

---

[3] Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos (PIDCP), Comité de Derechos Humanos, Observación General n.° 34, artículo 19, Libertad de opinión y libertad de expresión, CCPR/C/GC/34, 12 septiembre 2011, párr. 2; Opinión Consultiva OC-5 de 13 de noviembre de 1985, "La colegiación obligatoria de periodistas" (arts. 13 y 29 Convención Americana sobre Derechos Humanos), solicitada por el Gobierno de Costa Rica, Serie A, núm. 05, párr. 70.

[4] Entre muchos, Comité de Derechos Humanos, Observación General n.° 34, cit.; Corte IDH, Opinión Consultiva OC-5/85, cit., párr. 46; Caso Herrera Ulloa *vs*. Costa Rica, Sentencia de 2 de julio de 2004, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, núm. 107, párrs. 121 y 123; Caso Ricardo Canese *vs.* Paraguay, Sentencia de 31 de agosto de 2004, Fondo, Reparaciones y Costas, Serie C No. 111, párr. 96.

[5] Véase Corte IDH, Opinión Consultiva OC-5/85, cit., párr. 46; Caso Herrera Ulloa *vs*. Costa Rica, cit., párr. 122; Caso Fontevecchia y D'Amico *vs.* Argentina, Sentencia de 29 de noviembre de 2011, Fondo, Reparaciones y Costas, Serie C, núm. 238, párr. 54.

[6] Corte IDH, Caso Kimel *vs.* Argentina, Sentencia del 2 mayo de 2008, Fondo, Reparaciones y Costas, Serie C, núm. 177, párr. 78; Caso Álvarez Ramos *vs.* Venezuela, Sentencia de 30 de agosto de 2019, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C, núm. 380, párr. 119; Caso Usón Ramírez *vs*. Venezuela, Sentencia de 20 de noviembre de 2009, párr. 55.

Brandenburg y Watts de la Suprema Corte estadounidense,[7] en Argentina se ha aclarado que, por ejemplo, la reivindicación de las "puebladas" y el enfrentamiento con la policía, o de la ocupación y quema de comisarías y tribunales es un ejercicio legítimo de la libertad de expresión.[8]

Sobre la protección, o no, del discurso falso, nos limitaremos a notar que la preocupación por la circulación de información falsa, engañosa o de "mala calidad", no es un fenómeno nuevo ni limitado a las redes sociales. Precisamente esa era la preocupación que subyacía tras la intención de exigir una colegiatura obligatoria para ejercer el periodismo a mediados de los años ochenta. Frente a eso, la Corte Interamericana de Derechos Humanos (Corte IDH) dejó en claro que "no sería lícito invocar el derecho de la sociedad a estar informada verazmente para fundamentar un régimen de censura previa supuestamente destinado a eliminar las informaciones que serían falsas a criterio del censor".[9] La Corte advirtió que "un sistema de control al derecho de expresión en nombre de una supuesta garantía de la corrección y veracidad de la información que la sociedad recibe puede ser fuente de grandes abusos y, en el fondo, viola el derecho a la información que tiene esa misma sociedad".[10]

Del mismo modo, es un hecho generalmente aceptado que el simple carácter de falsedad de una expresión no es motivo suficiente para que esa expresión sea restringida. En particular, el estándar de real malicia exige un análisis cuidadoso para evaluar la legitimidad de alguna sanción por el daño generado por una expresión falsa, solo cuando fuera hecha con conocimiento de su falsedad o con una despreocupación temeraria al respecto. Este estándar desarrollado por la Corte Suprema estadounidense[11] ha sido recogido por la Corte Suprema de Justicia argentina[12] y el sistema interamericano de derechos humanos.[13]

---

[7] Scotus, Noto v. United States, 367 U.S. 290 (1961), Sentencia de 5 de junio de 1961; Watts v. United States, 394 U.S. 705 (1969), Sentencia de 21 de abril de 1969 y Brandenburg v. Ohio, 395 U.S. 444 (1969), Sentencia de 9 de junio de 1969.

[8] Cámara Criminal y Correccional Federal (CCCF), Sala I, Causa N.° 25.212, "Ortiz, S. s/ procesamiento", Sentencia de 8 de julio de 1994; Sala I, Causa N.° 37.733, "Bonafini, Hebe s/ sobreseimiento", Sentencia de 27 de abril de 2006; Sala I, Causa N.° 40.687, "Bignone, Reynaldo s/rechazo falta de acción", Sentencia de 29 de agosto de 2007; Sala II, Causa N.° 20.336, "Vita, Leonardo G. y otro s/procesamiento", Sentencia de 29 de agosto de 2003.

[9] Corte IDH, Opinión Consultiva OC-5/85, cit., párr. 33.

[10] Corte IDH, Opinión Consultiva OC-5/85, cit., párr. 77.

[11] Scotus, New York Times Co. v. Sullivan, 376 U.S. 254 (1964), Sentencia de 9 de marzo de 1964; Garrison v. Louisiana, 379 U.S. 64 (1964), Sentencia de 23 de noviembre de 1964.

[12] CSJN, "Vago, Jorge Antonio c/ Ediciones de La Urraca SA. y otros", Sentencia de 19 de noviembre de 1991, *Fallos*: 314:1517; "Pandolfi, Oscar Raúl c/ Rajneri, Julio Raúl", Sentencia 1 julio 1997, *Fallos*: 320:1272; "Patitó, Jose Ángel y otro c/ Diario La Nacion y otros s/daños y perjuicios", Sentencia 24 junio 2008, *Fallos*: 331:1530.

[13] CIDH, Declaración de Principios sobre Libertad de Expresión, adoptada en su 108° periodo ordinario de sesiones celebrado del 2 al 20 octubre del 2000; CIDH, Marco jurídico interamericano sobre el derecho a la libertad de expresión, 2009, par. 109; Corte IDH, Caso Tristán Donoso *vs*. Panamá, Sentencia de 27 de enero de 2009, Excepción Preliminar, Fondo,

La doctrina de la real malicia está dirigida a resguardar la libertad de expresión, de forma que no es admisible su aplicación artificiosa como una herramienta para socavar el discurso, con la pretensión, sin más, de privar de protección al discurso deliberadamente falso. En este punto, en 2012 la Corte estadounidense declaró la inconstitucionalidad de una ley que penalizaba a quien se presentara como condecorado por una medalla militar sin serlo, que el Gobierno impulsaba con el argumento de que no era más que la aplicación de la doctrina de real malicia. Sin embargo, la Corte advirtió que esta doctrina existe "para permitir más discurso, no menos" y que "una regla diseñada para tolerar cierto discurso no debería florecer para convertirse en la justificación de una regla que lo restringe".[14] Según la Corte, que la Constitución provea menor protección a las declaraciones deliberadamente falsas "no puede interpretarse en el sentido de 'ninguna protección en absoluto'".[15] La prohibición del discurso falso no es la solución, sostuvo, sino que es la propia dinámica de la libertad de expresión lo que permite superar la mentira. La "verdad", argumentó, "no necesita esposas ni una placa para su reivindicación".[16]

En el mismo sentido se expresaron en su Declaración Conjunta de 2017 los relatores especiales para la Libertad de Expresión cuando recordaron que "el derecho humano a difundir información e ideas no se limita a declaraciones 'correctas'" y que "las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluidos 'noticias falsas' (*fake news*) o 'información no objetiva', son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión".[17]

Reparaciones y Costas, Serie C, núm. 193, párr. 125. En este último caso, aunque no refirió expresamente a la doctrina de "real malicia", el estándar que aplicó la Corte para evaluar la responsabilidad de Tristán Donoso es, en esencia, muy similar. Allí explicó que en el momento en que Tristán Donoso convocó a la conferencia de prensa y afirmó los hechos que resultaron ser inexactos, "existían diversos e importantes elementos de información y de apreciación que permitían considerar que su afirmación no estaba desprovista de fundamento" (párrs. 124 y 125). Sobre la relación entre la doctrina de real malicia y la jurisprudencia de la Corte IDH, véase Hernán Gullco, "La doctrina de la 'real malicia' y la reciente jurisprudencia de la Corte Interamericana de Derechos Humanos sobre libertad de expresión", *Revista de Derecho y Ciencias Penales*, n.° 13 (2009): 127-138.

[14] Scotus, United States v. Alvarez, 567 U.S. 709 (2012), Sentencia de 28 de junio de 2012, voto de los jueces Kennedy y Roberts y de las juezas Ginsburg y Sotomayor.

[15] Scotus, United States v. Alvarez, 567 U.S. 709 (2012), Sentencia de 28 de junio de 2012, voto de los jueces Breyer y Kagan.

[16] Scotus, United States v. Alvarez, 567 U.S. 709 (2012), Sentencia de 28 de junio de 2012, voto de los jueces Kennedy y Roberts y de las juezas Ginsburg y Sotomayor.

[17] Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relator Especial de la Organización de los Estados Americanos (OEA) para la Libertad de Expresión, Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), "Declaración Conjunta sobre Libertad de Expresión y 'Noticias Falsas'

Dicho lo anterior, en lo que sigue revisaremos brevemente algunas particularidades de las prácticas de inteligencia en fuentes abiertas y la especial implicancia en los derechos humanos de la inteligencia sobre redes sociales. Luego, analizaremos de qué forma el DIDH protege las acciones y expresiones de las personas en el espacio público y cómo se aplica esto en el contexto de las tecnologías de la información y las redes sociales. Veremos también cómo estas políticas tienen un efecto concreto en el ejercicio pleno de la libertad de expresión y generan un efecto de autocensura. Por último, analizaremos estas prácticas a la luz de los principios constitucionales de legalidad y razonabilidad en el contexto argentino, y explicaremos por qué su uso indiscriminado resulta incompatible con los derechos a la privacidad y a la libertad de expresión y no puede ser válidamente empleado como sustento de un proceso penal.

Para cerrar, reafirmaremos la necesidad de repensar los límites y las garantías que deben guiar las políticas de privacidad y vigilancia en el presente, considerando las necesidades y los intereses humanos actuales, en una época de intensa actividad en línea, en general, y de las redes sociales, en particular.

2. Nuevos desafíos de la inteligencia en fuentes abiertas y redes sociales

Más allá de que en la Argentina se le ha llamado "ciberpatrullaje" o "prevención policial digital", la actividad de agentes estatales de monitoreo, recolección y análisis de información hecha pública en redes sociales constituye lo que en el ámbito de inteligencia se conoce como Socmint. Esta inteligencia en redes sociales es una forma particular de la inteligencia de fuentes abiertas (Osint), que es la búsqueda, la recolección y el análisis de información que se encuentra disponible públicamente. Esta consiste en datos para cuyo acceso no se requiere una autorización o credencial específica y que no se encuentran protegidos por ninguna capa o sistema de seguridad que se deba eludir.

La Osint no es una práctica nueva en el ámbito de la inteligencia, pero la expansión de internet tuvo profundos efectos en su desarrollo. Internet no solo cambió la vida de las personas, sino que afectó las capacidades y metodologías de los organismos de inteligencia. En 2001, el director del Consejo Nacional de Inteligencia, que coordina los organismos militares y civiles de la comunidad de inteligencia estadounidense, distribuyó internamente un artículo en el que destacaba que la Osint ya no es lo que solía ser hace diez años. Las fuentes abiertas, explicó, solían ser el "glaseado en el pastel", eran accesorias al material recogido por la inteligencia de señales (*Signals Intelligence* Sigint), de imágenes (*Imagery Intelligence* Imint) y la colección clandestina de origen humano (*Human Intelligence* Humint). Con la expansión de internet,

('Fake News'), Desinformación y Propaganda", Estándares sobre desinformación y propaganda, 2.a), 2017.

señalaba, la inteligencia de fuentes abiertas (Osint) "se ha expandido mucho más allá del 'glaseado' y comprende una gran parte del pastel".[18]

De la mano de la expansión de la Osint, facilitada por el amplio uso de internet, también ha florecido un nuevo campo específico para las actividades de inteligencia destinado a recopilar y analizar la información que las personas vuelcan en sus redes sociales: Socmint. Quien fuera por años director del servicio de inteligencia británico invitaba, en 2012, a que la comunidad de inteligencia internacional reconociera la potencialidad de las redes sociales. Las oportunidades que ofrece la explosión del uso de las redes sociales, decía, son notables, y la Socmint "debe convertirse en miembro de pleno derecho de la familia de inteligencia y aplicación de la ley".[19] En el mismo sentido, un reciente informe de la Corporación RAND explicaba que "la creciente omnipresencia de internet y el auge de las redes sociales y el análisis de *big data* en las últimas dos décadas han revolucionado la inteligencia de fuente abierta", lo que exigía, entonces, hablar de una Osint de "segunda generación".[20]

Las redes sociales son elementos cada vez más esenciales en la vida de millones de personas. Esto ha generado nuevas posibilidades para las autoridades policiales y las ha convertido, por cierto, en fuentes significativas de información para las agencias de inteligencia y seguridad pública.[21]

Al no traspasar barreras de seguridad ni realizarse por métodos encubiertos, algunos pretenden igualar las prácticas de Socmint con las fuentes abiertas.[22] Sin embargo, lo cierto es que la naturaleza de las plataformas de redes sociales y el tipo de información e interacción que allí acontece exige una mayor protección en ese ámbito. En ellas, las fronteras entre lo público y lo privado se presentan como especialmente difíciles de delinear. En general, con el advenimiento de la "era digital", la naturaleza de los espacios públicos y privados ha cambiado y se ha vuelto aún más difícil establecer distinciones tajantes entre estos ámbitos. Esto es especialmente cierto en el caso de las redes sociales. Al respecto se ha alertado que estas se caracterizan por encontrarse en una "zona gris" entre lo público y lo privado, con una naturaleza dual en tanto "son públicas, pero a menudo se sienten privadas" por los usuarios, pudiendo entenderse como espacios de internet cuasipúblicos.[23]

---

[18] John Gannon, "The strategic use of open-source information", *Studies in Intelligence* 45, n.° 3 (2001): 67.

[19] David Omand, Jaime Bartlett y Carl Miller, "Introducing social media intelligence (Socmint)", *Intelligence and National Security* 27, n.° 6 (2012): 801-823.

[20] Heather Williams e Ilana Blum, *Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise* (Santa Mónica: RAND Corporation, 2018), 1.

[21] Kira Vrist Rrønn y Sille Obelitz Søe, "Is social media intelligence private? Privacy in public and the nature of social media intelligence", *Intelligence and National Security* 34, n.° 3 (2019): 362-378.

[22] Omand, Bartlett y Miller, "Introducing Social Media Intelligence (Socmint)", 801-823.

[23] Rrønn y Søe, "Is social media intelligence private?" 362-378.

En este punto, vale advertir que las técnicas de Osint y Socmint no solo involucran la recopilación y el análisis de lo que expresamente decimos en nuestras redes sociales, sino que abarca otro conjunto de información relacionada. Con quién interactuamos y de qué forma, dónde nos encontramos geográficamente, desde qué dispositivo y con qué red nos conectamos, en qué horarios y otros "datos sobre los datos" (metadatos) que se puedan extraer de esa información.

Pues bien, como es conocido, las prácticas de inteligencia y vigilancia de las acciones en línea de las personas pueden implicar un grado de injerencia sobre su derecho a la privacidad y el pleno ejercicio de otros derechos.

Al respecto, el DIDH nos dice que las injerencias en el derecho a la privacidad solo están permitidas si no son arbitrarias ni ilegales y en este punto "los mecanismos de derechos humanos han interpretado sistemáticamente que esas palabras apuntan a los principios generales de legalidad, necesidad y proporcionalidad".[24] Desde hace años, el Comité de Derechos Humanos ha dicho que estas injerencias solo pueden tener lugar en virtud de la ley, que a su vez debe alinearse con los propósitos y objetivos del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Además, la injerencia no puede ser arbitraria, lo que exige que la restricción, además de estar prevista en la ley, sea siempre razonable en las circunstancias particulares del caso concreto.[25] Este concepto de razonabilidad se refiere a que "cualquier injerencia en la vida privada debe ser proporcional al propósito perseguido y necesaria en las circunstancias particulares del caso".[26] De esta forma, una limitación "solo puede ser legal y no arbitraria si persigue un fin legítimo", si esa restricción es "necesaria y proporcional a ese fin legítimo" y si es "la menos intrusiva de las opciones disponibles", sin comprometer la esencia del derecho.[27]

Como se explicará más adelante, en el caso de la Argentina, la práctica de monitoreo de redes sociales para fines de prevención policial no tiene respaldo legal. La ley de inteligencia nacional 25.520 solo habilita la producción de inteligencia criminal atada a hipótesis delictivas concretas y excluye de la legalidad las prácticas de vigilancia masiva que "salen de pesca" preventivamente. Ahora bien, más allá de los problemas de legalidad, lo que nos interesa poner en discusión en este artículo es la engañosa noción de que todo lo que voluntariamente hacemos público en

---

[24] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 3 de agosto de 2018, A/HRC/39/29, par. 10.

[25] Naciones Unidas, Asamblea General, Consejo de Derechos Humanos, Observación General n.º 16, artículo 17, Derecho a la intimidad, 1988, HRI/GEN/1/Rev.7, p. 162, párrs. 3 y 4.

[26] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, par. 21.

[27] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 3 de agosto de 2018, A/HRC/39/29, par. 10.

nuestras redes sociales está ahí disponible para que el Estado lo recolecte, analice y almacene para los fines que estime convenientes.

Esta es una discusión en torno al contenido y alcance del derecho a la privacidad en el espacio público, su aplicación al ámbito digital, las facultades del Estado para recolectar, analizar y almacenar esa información hecha pública y los impactos de esta actividad en otros derechos, como la libertad de expresión.

3. La policía sentada a la mesa

Cuando se discute sobre el monitoreo de redes sociales es común escuchar que como sociedad no podemos reclamar algún tipo de protección de nuestra privacidad en este ámbito, porque todo lo que decimos allí lo hacemos en realidad de manera pública. Y, si lo que hacemos es público y cualquier persona que ingresa a una red social puede ver lo que allí estamos diciendo y con quién interactuamos, pues por qué entonces el Estado no podría hacer lo mismo. Además, se alega, el Estado lo hace precisamente para cumplir sus funciones de prevención policial y, en definitiva, cuidarnos a los usuarios de esas redes.

Pero este es un razonamiento engañoso, en el que los argumentos de seguridad pública eluden las garantías constitucionales de las personas.

Así como cuando estamos sentados en un café conversando con un amigo no esperaríamos que un policía estuviera sentado a la mesa escuchando lo que públicamente conversamos, tampoco sería razonable esperar que cuando interactuamos públicamente en las redes sociales ese mismo policía esté sentado en una oficina revisando sistemáticamente qué decimos y con quién interactuamos. Del mismo modo, tampoco sería admisible que, aunque fueran públicas, la policía se infiltre en asambleas o manifestaciones políticas, para ver y escuchar qué, quiénes y cómo interactúan en ese espacio. Tampoco sería aceptable, por ejemplo, que agentes estatales se instalaran en las salas de espera de los centros de salud, por muy públicas que fueran, para registrar lo que allí acontece.

No porque actuemos y hablemos sin escondernos, sin establecer capas de protección a nuestras interacciones, significa que no gocemos de algún grado de derecho a la privacidad. Para gozar de este derecho no es necesario el ocultamiento deliberado de nuestras acciones y expresiones.

Por cierto, puede ser entendible que existan diversos grados en la expectativa de privacidad que tengamos dependiendo del tipo de comunicación de que se trate y el medio que se utilice. Es razonable pensar que no gozamos del mismo grado de protección cuando mantenemos una conversación por teléfono o correo electrónico sobre un tema sensible con nuestro abogado o médico, que cuando damos un discurso arriba de un escenario o interactuamos en las redes sociales.

Aunque es lógico pensar en distintos grados en la expectativa de privacidad, esto no implica que la actividad realizada "a la vista de todos" esté desprovista de toda

protección. Que hablemos sin escondernos no quiere decir que, como sociedad, estemos de acuerdo con que el Estado implemente políticas de monitoreo y vigilancia masiva para ver y escuchar –y almacenar– todo lo que se dice en un foro público, sea analógico, en "la vida real", o en el ámbito digital.

La protección de la vida privada no solo alcanza a las comunicaciones privadas y deliberadamente excluidas del conocimiento de terceros. También irradia a las actividades que las personas realizamos en lugares o foros públicos de comunicación, como las redes sociales u otros espacios abiertos de internet.

En definitiva, como no vivimos en un Estado de sospecha constante, en los espacios públicos las personas mantenemos una legítima expectativa de que nuestras acciones, aun las públicas, no están sometidas a vigilancia.

La policía sentada a la mesa de la conversación pública no es admisible en un Estado democrático de derecho.

4. Una razonable expectativa de privacidad en el espacio público

La protección de la vida privada, entonces, no se encuentra delimitada exclusivamente a lo que ocurre dentro del domicilio o a las cuestiones deliberadamente excluidas del conocimiento de terceros. Aun en el espacio público y a la vista de todos, conservamos una razonable expectativa de privacidad de que no se nos someta a políticas de vigilancia en las que se recopile, analice y almacene todo lo que hacemos o dejamos de hacer.

Los intereses de privacidad en el espacio público son moral y políticamente importantes en la misma medida. Esto, advierte Lever, es sobre todo cierto si se atiende a que es, precisamente, el espacio público el que "nos ofrece algunas de nuestras mejores oportunidades para la paz y la tranquilidad, para una relación sincera con amigos o para relajarnos y divertirnos".[28] Es en la interacción con otros que nuestras vidas se desarrollan plenamente. Sería un error suponer que las personas carecen de intereses legítimos en la privacidad una vez que dejan la intimidad de sus casas.

Al respecto, el Tribunal Europeo de Derechos Humanos (TEDH) ha advertido de manera consistente que no por aventurarse en la esfera pública las personas pierden toda protección a su derecho a la vida privada. Por el contrario, señala, existe "una zona de interacción de una persona con otras, incluso en un contexto público, que puede caer dentro del alcance de la 'vida privada'".[29] El TEDH ha reconocido una "vi-

[28] Annabelle Lever, "Democracy, Privacy and Security", en *Privacy, Security and Accountability: Ethics, Law and Policy*, ed. por Adam Moore (London: Routledge, 2016), 105-124.

[29] TEDH, Gran Sala, Caso von Hannover v. Germany (n.° 40660/08 y 60641/08), Sentencia de 7 de febrero de 2012, párr. 95; Caso Benedik v. Slovenia (n.° 62357/14), Sentencia de 28 de abril de 2018, párr. 100; Caso P.G. y J.H. v. The United Kingdom (n.° 44787/98), Sentencia de

da social privada" y ha expresado, entonces, que el derecho a la vida privada "abarca el derecho de cada individuo a acercarse a los demás para establecer y desarrollar relaciones con ellos y con el mundo exterior".[30] Las relaciones interpersonales, no por ser compartidas con terceros y realizadas en espacios no vedados al público, dejan de ser parte de la vida privada de las personas.

Así, ha señalado también que "la información pública puede caer en el ámbito de la vida privada, cuando se recopila y almacena sistemáticamente en archivos en poder de las autoridades".[31] Esta interferencia es tal aun si las autoridades no consultan o utilizan los registros creados con información pública e incluso si esos registros no incluyen información sensible.[32] La Gran Sala del TEDH aclaró que la Convención garantiza "una forma de autodeterminación informativa, permitiendo a las personas confiar en su derecho a la privacidad en lo que respecta a los datos que, aunque neutrales, se recopilan, procesan y difunden de manera colectiva".[33] Y, además, alertó a los Estados respecto de que "el hecho de que la información ya sea de dominio público no elimina necesariamente la protección del artículo 8 de la Convención".[34]

En esta línea son de especial interés los desarrollos de la Suprema Corte estadounidense sobre las expectativas de privacidad de las personas en el espacio público y la información que deliberadamente comparten con otras.

En 1967, la Corte resolvió el caso Katz en el que se impugnaban las pruebas producidas por el Estado mediante la instalación de un micrófono en una cabina telefónica pública que, aunque no grababa ni interceptaba la conversación, sí permitía escuchar lo que la persona decía en la cabina. El Estado argumentaba que como no interceptó la llamada ni ingresó en el domicilio del imputado, no necesitaba orden judicial. La Corte rechazó esta postura y explicó que el derecho a la vida privada de la Cuarta Enmienda "protege personas, no lugares". Aquí la Corte elaboró el principio de que existe una "razonable expectativa de privacidad en el espacio público" que está protegida constitucionalmente.[35]

---

25 de septiembre de 2001, párr. 56; CEDH, Caso Peck v. The United Kingdom (n.° 44647/98), Sentencia de 28 de enero de 2003, párr. 57; Caso Uzun v. Germany, (n.° 35623/05), Sentencia de 2 de septiembre de 2002, párr. 43.

[30] TEDH, Caso Bărbulescu v. Romania (n°61496/08), Sentencia de 5 de septiembre de 2017, párr. 70.

[31] TEDH, Caso Rotaru v. Romania (n.° 28341/95), Sentencia de 4 de mayo de 2000.

[32] TEDH, Caso Amann v. Switzerland (n.° 27798/95), Sentencia de 16 de febrero de 2000, párrs. 65-67; Caso P.G. y J.H. v. The United Kingdom (n.° 44787/98), Sentencia de 25 de septiembre de 2001, párr. 57 *in fine*; Caso Uzun v. Germany (n.° 35623/05), Sentencia de 2 de septiembre de 2002, párr. 46.

[33] TEDH, Gran Sala, Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finland (n.° 931/13), Sentencia de 27 de junio de 2017, párr. 137; Caso Benedik v. Slovenia (n.° 62357/14), Sentencia de 28 de abril de 2018, párr. 103.

[34] TEDH, Gran Sala, Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finland, (n.° 931/13), Sentencia de 27 de junio de 2017, párr. 134.

[35] Scotus, Katz v. United States, 389 U.S. 347 (1967), Sentencia de 18 de diciembre de 1967.

También, en 2012, en el caso Jones, la Corte declaró inconstitucional el seguimiento por GPS del vehículo de un imputado sin orden judicial previa, aunque el seguimiento se limitara a calles y espacios públicos. La decisión final de la Corte se centró en que la instalación del GPS había afectado el derecho de propiedad sobre el vehículo, pero cinco de los nueve jueces también explicaron que este tipo de seguimiento por espacios públicos sin autorización judicial no era constitucional porque violaba el derecho a la privacidad. En su voto, al que adhirieron tres jueces, el juez Alito explicó que "las expectativas de la sociedad han sido que ni los agentes de seguridad ni otros deberían –y, de hecho, en muchos casos no podrían– monitorear secretamente y catalogar cada uno de los movimientos de los vehículos de los individuos por un periodo extendido de tiempo".[36] Este tipo de vigilancia continua de las actividades de las personas, aun en el espacio público y sin guardar secreto alguno, solo sería admisible cuando fuera habilitada por una autoridad judicial en un caso concreto con "causa probable". La jueza Sotomayor agregó también que era necesario terminar con el entendido de que "el secreto es un prerrequisito de la privacidad". Así, explicó, "no asumiré que toda la información que es voluntariamente revelada para algún fin determinado se encuentra, por ese simple motivo, desprovista de la protección de la Cuarta Enmienda".[37]

Después, más recientemente, en el caso Carpenter de 2018, la Corte estadounidense dejó sin efecto una condena en la que se había utilizado como prueba la ubicación del celular del imputado en el lugar de los hechos. Esta información había sido obtenida de las celdas de telefonía celular, sin autorización judicial. El Estado argumentaba que esta información no era privada, porque el imputado ya la había compartido con un tercero, con su compañía de teléfono, y que el seguimiento se había limitado a espacios públicos. Esto fue desechado por la Corte, quien explicó que "una persona no claudica toda su protección de la Cuarta Enmienda por aventurarse en la esfera pública", y que "los individuos mantienen una legítima expectativa de privacidad respecto del registro de sus movimientos capturados por las señales de su celular".[38]

Además, los jueces alertaron sobre los especiales riesgos de este tipo de rastreo, por su cualidad retrospectiva. Con estas formas de vigilancia, dijo, "el gobierno ahora puede viajar atrás en el tiempo", sujeto solo a las políticas de retención de las compañías telefónicas. De esta forma, alertó,

> … quien sea que resulte ser el sospechoso, este habrá sido efectivamente seguido cada momento, de cada día, durante cinco años, y la policía podrá

[36] Scotus, United States v. Jones, 565 U.S. 400 (2012), Sentencia de 23 de enero de 2012, voto del juez Alito, al que concurren las juezas Ginsburg y Kagan y el juez Breyer.

[37] Scotus, United States v. Jones, 565 U.S. 400 (2012), Sentencia de 23 de enero de 2012, voto de la jueza Sotomayor.

[38] Scotus, Carpenter v. United States, 585 U.S. __ (2018), Sentencia de 22 de junio de 2018.

> –según la postura el gobierno– utilizar los resultados de esa vigilancia sin considerar las restricciones de la Cuarta Enmienda. Solo los pocos sin celular podrán escapar de esta incansable y absoluta vigilancia.[39]

Es decir, solo los que se rehúsen a utilizar una tecnología o prestación determinada (como un celular, la internet o las redes sociales) podrán escapar de la vigilancia total que esa tecnología permite y que las autoridades están dispuestas a explotar, sin ningún control judicial. Esta posibilidad, entendió la Corte, era inadmisible a la luz de la protección constitucional del derecho a la privacidad. Esto es especialmente cierto si se repara en que la utilización de un celular "es indispensable para participar en la sociedad moderna".[40]

Al resolver en el caso Carpenter la Corte estadounidense recuperó lo que había dicho en 1948 respecto de que "nuestros antepasados, después de consultar las lecciones de la historia, diseñaron nuestra Constitución para colocar obstáculos en el camino de una vigilancia policial demasiado penetrante, que aparentemente consideraban era un mayor peligro para un pueblo libre, que el escape del castigo de algunos criminales".[41]

Efectivamente, las lecciones de la historia y la actual expansión de los límites de lo permisible en materia de vigilancia aconsejan prudencia a la hora de abrazar paradigmas de control social y avalar restricciones cada vez mayores a nuestra privacidad.

5. Intereses humanos actuales y privacidad en espacios abiertos de internet

El contenido y alcance del derecho a la privacidad debe ser analizado a la luz de las necesidades y los intereses humanos en la vida actual, donde internet y las redes sociales son parte central de la vida de millones de personas. Es en el contexto de la globalización informativa y la ubicuidad de internet en la vida cotidiana, donde los Estados están llamados a garantizar y respetar los derechos de las personas y no explotar ilegítimamente los mayores riesgos que estas tecnologías generan.

La Corte Interamericana de Derechos Humanos (CIDH) ha aclarado que cuando la Convención Americana sobre Derechos Humanos (CADH) protege la vida privada frente a injerencias arbitrarias o abusivas no lo hace de forma restrictiva. El artículo 11 de la CADH en realidad solo habla del domicilio, la correspondencia y la vida privada y familiar de las personas, pero la Corte dijo que esto no debe

---

[39] Scotus, Carpenter v. United States, 585 U.S. __ (2018), Sentencia de 22 de junio de 2018.

[40] Scotus, Carpenter v. United States, 585 U.S. __ (2018), Sentencia de 22 de junio de 2018; Riley v. California, 573 U.S. 373 (2014), Sentencia de 25 de junio de 2014.

[41] Scotus United States v. Di Re, 332 U.S. 581 (1948), Sentencia de 5 de enero de 1948.

entenderse como una lista cerrada de las esferas de privacidad.[42] Así, por ejemplo, advirtió que "aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación incluida dentro del ámbito de protección de la vida privada", sea que fueran "realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla".[43]

Además, esta protección se refiere no solo al contenido de la conversación, sino que alcanza a "cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas", todos ellos aspectos "que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones".[44]

En este mismo sentido, el TEDH también ha aclarado en más de una ocasión que la "vida privada" que protege el artículo 8 del Convenio Europeo, cuando garantiza la vida privada y familiar, la residencia y la correspondencia de las personas, "es un concepto amplio no susceptible de una definición exhaustiva",[45] que puede "abarcar múltiples aspectos de la identidad física y social de las personas".[46] En este respecto, el TEDH advirtió también que se debe prestar especial atención a la hora de implementar nuevas tecnologías de investigación que, si bien pueden ayudar a la lucha contra el delito, también pueden implicar importantes avances sobre algunos derechos, como la privacidad. Sobre este punto señaló:

> … la protección que brinda el artículo 8 de la Convención se vería inaceptablemente debilitada si se permitiera el uso de técnicas científicas modernas en el sistema de justicia penal a cualquier costo y sin equilibrar cuidadosamente los beneficios potenciales del uso extensivo de tales técnicas con importantes intereses de la vida privada.[47]

---

[42] Corte IDH, Caso Escher y Otros *vs*. Brasil, Sentencia de 6 de julio de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, núm. 200, párrs. 114 y 115.

[43] Corte IDH, Caso Escher y Otros *vs*. Brasil, Sentencia de 6 de julio de 2009, párr. 114.

[44] Corte IDH, Caso Escher y Otros *vs*. Brasil, Sentencia de 6 de julio de 2009, párr. 114.

[45] TEDH, Caso Peck v. The United Kingdom (n.° 44647/98), Sentencia de 28 de enero de 2003, párr. 58; Caso Retty v. The United Kingdom (n.° 2346/02), Sentencia de 29 de abril de 2002, párr. 61; Caso Niemietz v. Germany (n.° 13710/88), Sentencia de 16 de diciembre de 1992, párr. 29.

[46] TEDH, Caso S. y Marper v. The United Kingdom (n.° 30562/04 y 30566/04), Sentencia de 4 de diciembre de 2008, párr. 66; Caso Mikulić v. Croatia (n° 53176/99), Sentencia de 7 de febrero de 2002, párr. 53.

[47] TEDH, Caso S. y Marper v. The United Kingdom (n.° 30562/04 y 30566/04), Sentencia de 4 de diciembre de 2008, párr. 112.

Asimismo, la Corte IDH adelantó que "la fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente". Así, advirtió que este progreso científico "no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares". Por el contrario, los Estados deben "asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada".[48]

Pues bien, en el contexto actual de desarrollo tecnológico en el que las posibilidades técnicas de implementar políticas de vigilancia masiva son cada vez mayores, los Estados deben prestar especial atención para asegurar su adecuación al DIDH.

Luego de la revelación de las políticas de vigilancia masiva conjunta del Reino Unido y Estados Unidos, la Asamblea General de las Naciones Unidas aprobó en 2013 la Resolución 68/167 sobre la privacidad en la era digital. Allí expresó su profunda inquietud por estas políticas de vigilancia y recordó que los derechos de las personas también deben protegerse en línea. En particular, exhortó a los Estados a proteger la privacidad en línea y revisar sus procedimientos, prácticas y leyes sobre vigilancia y archivo de datos personales, de forma que se garantice el cumplimiento pleno y efectivo de sus obligaciones internacionales.[49]

También, le encomendó a la Alta Comisionada para los Derechos Humanos que se aboque al estudio y elabore un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales, así como la recopilación de datos personales en los planos nacional y extraterritorial. En su informe de 2014, la Alta Comisionada recordó que las tecnologías de la comunicación aumentaron la capacidad de gobiernos y empresas para realizar actividades de vigilancia de forma que "las plataformas tecnológicas de las que depende crecientemente la vida política, económica y social a nivel mundial no solo son vulnerables a la vigilancia en masa, sino que en realidad pueden facilitarla".[50]

Además, señaló que no es correcto pensar que solo la información sustantiva en la comunicación está protegida y que la recopilación de datos acerca de una comunicación (metadatos) no constituye en sí misma una injerencia en la vida privada. La Alta Comisionada aclaró que la distinción entre información sustantiva protegida y metadatos desprotegidos no es admisible desde el punto de vista del derecho a la privacidad, pues "la agregación de la información comúnmente conocida como

---

[48] Corte IDH, Caso Escher y Otros *vs.* Brasil, Sentencia de 6 de julio de 2009, párr. 115.

[49] Naciones Unidas, Asamblea General, Resolución 68/167. El derecho a la privacidad en la era digital, aprobada el 18 de diciembre de 2013, A/RES/68/167.

[50] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, párr. 2.

'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada".[51]

Por su parte, en su segundo informe temático sobre la privacidad en la era digital, el nuevo Alto Comisionado reforzó estas consideraciones y recordó que el derecho a la privacidad es fundamental "para el goce y el ejercicio de los derechos humanos dentro y fuera de internet". La privacidad, explicó, es "uno de los fundamentos de la sociedad democrática y tiene un papel clave en la realización de una amplia gama de derechos humanos".[52]

En particular, y atendiendo a la gran cantidad de información personal que circula en internet y que es de "libre acceso", el Alto Comisionado reafirmó que "la protección del derecho a la privacidad no se limita a los espacios privados, aislados, como el domicilio de una persona, sino que se extiende a los espacios públicos y a la información de acceso público".[53] Así les recordó a los Estados que "el derecho a la vida privada también se ve afectado cuando se reúne y analiza la información sobre una persona que se ha hecho pública en las redes sociales". Al respecto explicó que, conforme el DIDH, "el intercambio público de información no implica que la información sustantiva quede desprotegida".[54]

Que los usuarios consientan las políticas de privacidad de cada plataforma (en la medida de lo posible y con las dificultades de abordar los siempre confusos términos y condiciones) no implica que hayan consentido también el acceso y tratamiento de su información personal en esa plataforma por parte de las autoridades gubernamentales.[55] Aceptar, por ejemplo, que el resto de los millones de usuarios de Facebook pueda ver mis fotos y con quién interactúo, no es lo mismo que aceptar que los organismos de inteligencia utilicen la información allí publicada y los metadatos que de ella puedan recuperar, para fines de seguridad, de forma indiscriminada y sin control ni límites claros.

En este punto vale recuperar el concepto de "vigilancia participativa", utilizado por primera vez por Mark Poster en los años noventa, y que se refiere a la vigilancia que es consensual, en la que "la población ha sido disciplinada para la vigilancia y

---

[51] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, párr. 19.

[52] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 3 de agosto de 2018, A/HRC/39/29, párr. 11.

[53] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 3 de agosto de 2018, A/HRC/39/29, párr. 6.

[54] Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 3 de agosto de 2018, A/HRC/39/29, párr. 6.

[55] Rrønn y Søe, "Is social media intelligence private?", 370.

para participar en el proceso".[56] En relación con las prácticas de monitoreo estatal de redes sociales, se ha advertido que allí la vigilancia participativa surge de la propia lógica de participación en estas plataformas, en la que compartir información personal significa ser parte de una comunidad. En esta, los costos sociales percibidos de no participar y compartir información personal son más altos que las eventuales preocupaciones sobre privacidad e intrusión de terceros.[57] Esto agrega una nueva capa de complejidad al asunto e interroga fuertemente sobre la legitimidad del monitoreo estatal de esa interacción en línea, que explota los legítimos intereses de las personas en utilizar estas redes.

El tratamiento masivo y sistemático de esta información socava el derecho a la privacidad de los usuarios y genera un efecto disuasorio de tal magnitud que da cuenta de una práctica desproporcionada y, por cierto, moralmente problemática. El hecho de que se pueda acceder con facilidad a esa información no significa que deba considerársela como una práctica moralmente permisible, no intrusiva en la privacidad de las personas y no sujeta a restricciones. Esta vigilancia oficial tiene efectos negativos en la forma en que interactuamos y usamos las redes sociales, de forma que, en definitiva, "es la sociedad en su conjunto y la democracia la que paga el precio".[58]

Aunque la información esté públicamente expuesta, al alcance de la mano de las autoridades estatales, la pregunta que interesa no gravita en torno a la factibilidad técnica ni a la idoneidad de esa práctica para los fines de seguridad pública. La pregunta apremiante es, más bien, si en un Estado de derecho es admisible que las autoridades gubernamentales accedan a cuentas personales de redes sociales y exploten la información allí expuesta, y si pueden hacerlo, bajo qué circunstancias, con qué límites y restricciones.[59]

Y entendemos que la vigilancia de las plataformas de redes sociales cuando no hay evidencia o sospecha razonable respecto de individuos y conductas específicas, cuando no está sujeta a hipótesis criminales concretas que se pretenda investigar, resulta injustificable a la luz de los requisitos de legalidad, y la necesidad de proteger y garantizar el derecho a la privacidad y libertad de expresión. El DIDH no lo permite.

---

[56] Mark Poster, *The Mode of Information: Post-structuralism and Social Context* (Chicago: University of Chicago Press, 1990), 93.

[57] Fernanda Bruno, "Surveillance and Participation on Web 2.0", en *Routledge Handbook of Surveillance Studies*, ed. por Kristie Ball, Kevin Haggerty y David Lyon (London, New York: Routledge, 2014).

[58] Rrønn y Søe, "Is social media intelligence private?", 374.

[59] Rrønn y Søe, "Is social media intelligence private?, 363.

6. Autocensura y privacidad en los espacios abiertos de internet

La protección y vigencia efectiva del derecho a la privacidad tiene, ciertamente, efectos en el goce y ejercicio de otros derechos, como la libertad de expresión, la libertad de asociación, el derecho a la identidad, el derecho a la autonomía informativa, el derecho a la igualdad, etc. En este punto, el Relator Especial para la Libertad de Expresión de las Naciones Unidas ha manifestado en más de una ocasión que "la intimidad y la libertad de expresión se relacionan entre sí y son mutuamente dependientes; la vulneración de una de estas puede ser tanto la causa como la consecuencia de la vulneración de la otra".[60] Respecto del ejercicio pleno de estos derechos en internet, en 2019 el Relator señaló que "la privacidad y la libertad de expresión están entrelazadas en la era digital, y la privacidad en línea es el punto clave para garantizar el ejercicio de la libertad de opinión y de expresión".[61]

Es que si una persona se sabe vigilada y registrada en sus acciones y expresiones, es muy posible que esto genere algún tipo de efecto disuasorio en lo que esa persona dirá o dejará de decir en la discusión pública, sea en el ámbito analógico (como participar en una protesta social) o en el digital (expresando una opinión en un foro o relacionándose con otros en las redes sociales).[62] Los efectos disuasorios de la vigilancia de la actividad en línea han sido extensamente estudiados de manera empírica en Estados Unidos, donde se ha advertido del impacto en la libertad de expresión en línea de los propios estadounidenses. Allí se encontró que la posibilidad de ser vigilado afectaba la actividad en línea de las personas de forma que incluso aquellas "que decían no tener nada que ocultar, eran altamente propensas a autocensurarse en línea cuando tomaban conocimiento de que el Gobierno las vigilaba".[63]

---

[60] Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, 17 de abril de 2013, A/HRC/23/40, párr. 79.

[61] Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, La vigilancia y los derechos humanos, 2019, A/HRC/41/35, párr. 24.

[62] La Corte estadounidense se refirió por primera vez a este efecto en el caso Wieman, donde explicó que la inhibición del discurso no solo afecta a quien se persigue puntualmente ante la Justicia, sino que se genera una inconfundible disuasión (*an unmistakeable tendency to chill*) en el resto de las personas (Wieman v. Updegraff, 344 U.S. 183 (1952), Sentencia de 15 de diciembre de 1952). La Corte IDH explicó también que las sanciones penales y civiles, así como otras restricciones indirectas, pueden generar este efecto disuasorio en el ejercicio de la libertad de expresión, que puede llevar a la autocensura (Corte IDH, Caso Herrera Ulloa *vs*. Costa Rica, Sentencia de 2 de julio de 2004, párr. 133; Caso Tristán Donoso *vs*. Panamá, Sentencia de 27 de enero de 2009, párr. 129; Caso Granier y otros *vs*. Venezuela, Sentencia de 22 de junio de 2015, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C No. 293, párr. 164, entre otros).

[63] Brennan Center for Justice, New York University School of Law, "Social Media Monitoring. How the Department of Homeland Security Uses Digital Data in the Name of National

Así, por ejemplo, un estudio en 2014 reveló que el 86% de los estadounidenses estaría dispuesto a tener una conversación sobre Snowden y el programa de vigilancia masiva de la National Security Agency, pero solo el 42% tendría esa conversación en sus redes sociales. La posibilidad de que el Gobierno monitoree lo que allí se dice hacía que las personas no estuvieran dispuestas a discutir algunos temas en línea y los reserven solo a las conversaciones cara a cara, donde es menos probable que el Gobierno esté escuchando.[64]

En un estudio de 2016 se encontró que aunque varios participantes estaban de acuerdo con las políticas de vigilancia para proteger la seguridad nacional y señalaban no tener nada que esconder, sin embargo, "cuando estos individuos perciben que están siendo monitoreados adaptan fácilmente su comportamiento, expresando sus opiniones cuando son mayoría y suprimiéndolas cuando no lo son".[65]

Del mismo modo, en 2017 se encontró que el principal disuasorio para una actividad *online* es una amenaza directa de acción legal por parte de un tercero (como una acción penal por tuitear una broma sobre saqueos) y que la segunda actividad más disuasoria era la vigilancia gubernamental. El estudio mostró que el 62% de los usuarios estaría menos dispuesto (o no dispuesto en absoluto) a discutir ciertos tópicos en línea, si supiera que lo que dice en esos foros en línea está siendo monitoreado por el Estado.[66]

La vigilancia de la actividad en línea, aunque no se tenga nada qué ocultar, tiene un efecto disuasorio sobre el libre ejercicio de nuestros derechos. Esto es especialmente cierto cuando esas actividades se llevan a cabo sin control judicial y con criterios excesivamente laxos y ambiguos. Este efecto disuasorio se agrava aún más cuando la sociedad deja de confiar en las autoridades al notar la aplicación absurda que hacen de sus potestades persecutorias, como cuando se impulsan acciones penales por chistes de adolescentes en las redes sociales.

7. Un desafío pendiente para la práctica constitucional de los tribunales argentinos

A pesar de sus graves implicancias, las autoridades argentinas parecen no albergar duda alguna respecto de que la inteligencia sobre fuentes digitales abiertas (redes

Security", New York, 2020, 3, https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf.

[64] Keith Hampton *et al.*, "Social media and the 'Spiral of Silence'", Washington, D. C., Pew Research Center, 2014, https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/.

[65] Elizabeth Stoycheff, "Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring", *Journalism & Mass Communication Quarterly* 93, n.° 2 (2016): 296-311.

[66] Jonathon W. Penney, "Internet surveillance, regulation, and chilling effects online: A comparative case study", *Internet Policy Review* 6, n.° 2 (2017): 1-39.

sociales incluidas), el "ciberpatrullaje", resulta perfectamente legal y compatible con los derechos consagrados por la Constitución Nacional. Las fuerzas de seguridad recurren a este tipo de prácticas de forma habitual, contando para ello con reparticiones especializadas; el Poder Ejecutivo Nacional ha dictado normas reglamentarias para avalar las tareas de "prevención digital" y los tribunales argentinos han convalidado estos procedimientos sin siquiera interrogarse sobre su constitucionalidad.

7.1. Según el marco jurídico local, el monitoreo de redes sociales es una actividad de inteligencia

Desde el punto de vista conceptual, la recopilación y el análisis de información en las redes sociales por parte de las fuerzas de seguridad constituye una actividad de inteligencia, lo que coincide con la legislación argentina en la materia y las definiciones allí contenidas. El artículo 2, inciso 1º, de la Ley 25.520 define a la inteligencia nacional como "la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación". Mientras, el inciso tercero de la norma conceptualiza la inteligencia criminal en los siguientes términos: "la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional".

Entonces, si hablamos de una práctica que consiste en la obtención y el análisis de información respecto de la actividad de las personas en las redes sociales, a cargo de funcionarios de inteligencia del Estado y con la finalidad de detectar hechos que puedan configurar delitos, para la ley argentina se trata de tareas de inteligencia.

Esto en nada se modifica por la circunstancia de que se trate de información de "fuentes abiertas". La Estructura Orgánica y Funcional de la Agencia Federal de Inteligencia, aprobada por el Decreto 1311 de 2015, refiere expresamente que la información de inteligencia "comprende las observaciones y mediciones obtenidas o reunidas de fuentes públicas o reservadas", por lo que difícilmente se podría argumentar que, por tratarse de datos públicos, su recopilación y análisis no constituye inteligencia. El tratamiento de información sobre la actividad de los particulares en las redes sociales constituye una práctica de inteligencia en función de la legislación aplicable, aunque se trate de "información pública". En todo caso, la diferencia con la obtención de información "no pública" o reservada radica en la protección agravada que la Constitución y la ley le acuerdan a ese tipo de datos, y no en la naturaleza de la práctica y su regulación legal.[67]

[67] CELS, "Observaciones del CELS a la Resolución 31/2018 y al Proyecto de protocolo de 'ciberpatrullaje'"(Buenos Aires: CELS, 2020), https://www.cels.org.ar/web/wp-content/

El punto no es menor, porque gran parte de la fundamentación esgrimida por las autoridades para justificar prácticas como las aquí analizadas consiste en la negación de que se trata de actividades de inteligencia, argumentando que estamos frente a meras actividades de prevención policial, realizadas en el ámbito digital, eufemísticamente llamadas "ciberpatrullaje". De esta forma, argumentan, no es necesario ajustarse a las especiales salvaguardas que deben guiar las actividades de inteligencia estatal.

7.2. Una excursión de pesca. Los principios de legalidad y razonabilidad y la regla de exclusión probatoria

No obstante, a la luz de los principios de legalidad y razonabilidad, las tareas de inteligencia masiva en redes sociales presentan serios problemas de constitucionalidad, lo que exige la aplicación del principio de exclusión probatoria en el proceso penal, cuando de ellas deriven causas judiciales.

Cierto es que los funcionarios de seguridad cuentan con facultades legales en materia de inteligencia criminal, pero sus competencias en ese ámbito se encuentran limitadas por la definición legal de este concepto: la Ley de Inteligencia Nacional solo habilita la realización de inteligencia de este tipo en relación con "actividades criminales específicas" que afecten determinados bienes jurídicos (la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías, etc.; art. 2, inc. 3º, de la norma citada).

Esta expresión implica la introducción de un requisito legal para toda práctica de inteligencia criminal: la exigencia de un mínimo grado de motivación, de sospecha razonable, respecto de la existencia de determinada conducta criminal (nótese que el legislador emplea la palabra "específica"), con cierta delimitación espacial, temporal o personal, y en relación con la probabilidad de encontrar datos relevantes en la fuente abierta de que se trate. Resulta claro, entonces, que la ley no consagra una facultad amplia de reunir información masivamente, para luego analizar si alguno de los datos así obtenidos se vincula con alguna actividad delictiva.[68]

La terminología legal no deja lugar a dudas respecto de que solo se puede efectuar "inteligencia criminal" en relación con supuestos delictivos específicos bien delimitados. La consulta de fuentes abiertas para su análisis por parte de funcionarios policiales solo resulta admisible frente a un delito (o conjunto de delitos) en concreto, respecto del cual se cuente con cierto grado de sospecha que habilite la actividad, y se encuentra prohibido su uso masivo para simplemente salir de pesca.

Tal interpretación es la más compatible con la protección de los derechos a la privacidad y a la libertad de expresión de los ciudadanos que, como anticipamos, se verían gravemente afectados si los funcionarios estatales pudieran recopilar

uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf.

[68] CELS, "Observaciones del CELS".

información de manera masiva sobre la actividad de las personas en las redes sociales, sin ningún tipo de fundamento concreto para tal proceder y con el único objetivo de detectar la eventual comisión de delitos.

Si bien la Corte Suprema argentina no se ha pronunciado todavía sobre este tipo de prácticas, sí ha advertido que una intrusión por parte de funcionarios estatales en el derecho a la privacidad de las personas, respecto de su domicilio o comunicaciones, solo resulta admisible "cuando median elementos objetivos idóneos para fundar una mínima sospecha razonable".[69] De esta manera, la CSJN ha señalado que "es exigible la existencia de elementos objetivos para evaluar la razonabilidad de la sospecha necesaria para el dictado de una medida que pueda afectar garantías fundamentales".[70] Solo así resulta posible evitar la discrecionalidad de los funcionarios de seguridad, puesto que "la necesidad de la motivación en supuestos en que están en juego garantías constitucionales encuentra su respaldo en la necesidad de controlar la coacción estatal y evitar la arbitrariedad de sus órganos administrativos".[71]

A su vez, el criterio de interpretación restrictiva que rige en materia de reglamentación de derechos demanda que, incluso si hubiera dudas respecto de la extensión de la habilitación legal, estas deberían resolverse en favor de la menor restricción posible de los derechos fundamentales.[72] Esto no es más que la aplicación del principio *pro homine*, criterio hermenéutico que informa todo el derecho de los derechos humanos en virtud del cual "se debe acudir a la norma más amplia, o a la interpretación más extensiva, cuando se trata de reconocer derechos protegidos e, inversamente, a la norma o a la interpretación más restringida cuando se trata de establecer restricciones".[73]

En 2018, la Secretaría de Seguridad dictó una resolución, no publicada en el *Boletín Oficial*, que pretende dar sustento normativo a la inteligencia sobre fuentes digitales abiertas y que, en la práctica, habilita que la policía rastrille toda la red en una excursión de pesca. La Resolución 31 de 2018 instruye a las áreas de ciberdelitos de las fuerzas de seguridad a realizar tareas de prevención policial en sitios de internet de acceso público sobre diversos supuestos criminales, sin exigir para ello

---

[69] CSJN, "Quaranta, José Carlos s/ inf. Ley 23.737 –causa n.º 763–", Sentencia de 31 de agosto de 2010, *Fallos*: 333:1674.

[70] CSJN, "Recurso de hecho. Stancatti, Oscar s/ causa n.º 462/2013", Sentencia de 24 de mayo de 2016, *Fallos*: 339:697.

[71] CSJN, "Recurso de Hecho. Matte, Domingo Luis; Irigoin, Néstor Félix y otros s/ tenencia de estupefacientes con fines de comercialización –causa n.º 2246–", *Fallos* 325:1845. Dictamen del procurador general al que remitió la Corte Suprema.

[72] Germán Bidart Campos, *Manual de la Constitución Reformada*, tomo II (Buenos Aires: Ediar, 2000), 344.

[73] Mónica Pinto, "El principio *pro homine*. Criterios de hermenéutica y pautas para la regulación de los derechos humanos", en *La aplicación de los tratados sobre derechos humanos por los tribunales locales*, coord. por Martín Abregú (Buenos Aires: CELS - Editores del Puerto, 2004), 163.

ningún tipo de motivo o sospecha previa.[74] Esta resolución implica un notorio exceso respecto de las facultades del Poder Ejecutivo, al pretender introducir un supuesto de actividad de inteligencia que implica serias restricciones de los derechos de los particulares, por fuera de los habilitados por el legislador.[75]

Además, de conformidad con el principio de razonabilidad, una restricción de derechos es admisible solo si los medios empleados son adecuados para los objetivos perseguidos, y media entre ambos una relación de proporcionalidad.[76] La razonabilidad exige evaluar "si las restricciones a la libertad individual son indispensables y proporcionales para alcanzar los fines de interés general".[77] Así es también, como se dijo, la forma en que los organismos de derechos humanos lo han entendido respecto de las limitaciones a la privacidad, advirtiendo que "cualquier injerencia en la vida privada debe ser proporcional al propósito perseguido y necesaria en las circunstancias particulares del caso".[78]

La práctica consistente en monitorear y recopilar de manera indiscriminada información disponible en las redes sociales con la finalidad de analizarla posteriormente en busca de indicios de la eventual comisión de delitos implica una restricción de los derechos a la privacidad y a la libertad de expresión decididamente incompatible con tales estándares. No existe proporcionalidad alguna entre el fin (legítimo) de descubrir posibles delitos y el medio elegido, que restringe y condiciona de forma masiva la privacidad y la expresión de la totalidad de las personas que participan en redes sociales. Esta afectación, en tanto indiscriminada, es totalmente inmotivada respecto de cada uno de estos sujetos en concreto, pues se realiza sin ningún tipo de justificativo particular. Todos los usuarios serán eventuales sospechosos, cuyas interacciones en línea serán vigiladas y analizadas.

De admitirse tareas de inteligencia como las aquí analizadas, los funcionarios estatales podrán inmiscuirse indiscriminada y masivamente en todo espacio de expresión que tenga lugar en medios digitales abiertos, sin que se les exija tan siquiera una justificación para tal proceder, lo que desnaturaliza y altera los derechos constitucionales en juego.

---

74 Entre los "tópicos" que enumera incluye la venta o permuta ilegal de armas y de artículos cuyo origen presumiblemente provenga de la comisión de un hecho ilícito, actividades de narcotráfico, explotación sexual o laboral, hostigamiento sexual a menores de edad y delitos "ciber" de la Ley 26388, entre otros.

75 En 2020, el Ministerio de Seguridad anunció su intención de dictar una nueva resolución. El borrador presentado replica la falta de motivación en las actividades de inteligencia de modo que le caben las mismas críticas (CELS, "Observaciones del CELS").

76 Néstor P. Sagüés, *Manual de derecho constitucional* (Buenos Aires: Astrea, 2007), 918 y ss.; CSJN, *Fallos* 156:290; 294:434; 328:690, entre muchos otros.

77 Gregorio Badeni, *Instituciones de derecho constitucional* (Buenos Aires: Ad-Hoc, 1997), 246.

78 Naciones Unidas, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, párr. 21.

Lo irrazonable del procedimiento en cuestión surge con evidencia al compararlo con el equivalente "analógico" del "ciberpatrullaje": atendida su cualidad de vigilancia total y omnipresente, consistiría en nada menos que el seguimiento y la vigilancia continua de todos los movimientos y las expresiones de las personas en calles y lugares de acceso público, o la grabación de toda conversación que tenga lugar fuera de sus domicilios.

En función de las graves afectaciones de derechos constitucionales y el notorio exceso en las facultades legales de inteligencia, es evidente que estas prácticas no resultan aptas para sustentar un proceso penal respetuoso del Estado de derecho, lo que exige la aplicación del principio de exclusión probatoria. De conformidad con este principio, los indicios obtenidos ilegalmente, en violación de garantías constitucionales, son inadmisibles como prueba de cargo.[79] Este criterio ha sido receptado en una reiterada y uniforme línea jurisprudencial de la CSJN en punto a que admitir esta prueba "compromete la buena administración de justicia al pretender constituirla en beneficiaria del hecho ilícito".[80] A su vez, si el procedimiento inicial es violatorio de garantías constitucionales, esa ilegalidad se proyecta sobre los actos subsiguientes que sean su consecuencia, de modo que las evidencias que son "fruto" de la ilegalidad originaria son igualmente inadmisibles.[81]

Como se explicó, las actividades de inteligencia sobre redes sociales exigen la preexistencia de un mínimo de elementos justificantes, de cierto grado de sospecha razonable. En ausencia de esta motivación previa, la recopilación de información de las redes sociales, o de fuentes digitales abiertas en general, es ilegal y no es apta para sustentar el inicio de un proceso penal.

7.3. Un análisis ausente

A pesar de todas estas consideraciones, hasta donde tenemos conocimiento ningún tribunal argentino ha puesto en duda la validez de las tareas de inteligencia sobre fuentes abiertas de internet. Su aptitud para dar sustento a un proceso penal es dada por sentado, a pesar de las graves implicancias que implica para los derechos individuales.

Así, por ejemplo, existen precedentes en los que jueces federales entienden el "ciberpatrullaje" como un simple procedimiento más, en virtud del cual los funcionarios policiales "se abocan a la prevención de delitos, contravenciones y faltas

---

[79] Alejandro Carrió, *Garantías constitucionales en el proceso penal* (Buenos Aires: Hammurabi, 2012), 305; Julio B. J. Maier, *Derecho procesal penal*, tomo III (Buenos Aires: Del Puerto, 2011), 126.

[80] CSJN, "Montenegro, Luciano Bernardino", Sentencia de 10 de diciembre de 1981, *Fallos* 303:1938; "Fiorentino, Diego Enrique", Sentencia de 27 de noviembre de 1984, *Fallos* 306:1752, entre muchos otros.

[81] Carrió, *Garantías constitucionales en el proceso penal*, 316; CSJN, "Rayford, Reginald y otros", Sentencia de 13 de mayo de 1986, *Fallos* 308:733.

realizados en la red de internet".[82] Esto pone el foco en la prevención, soslayando que se trata de inteligencia criminal, con especiales afectaciones en el pleno ejercicio de los derechos a la privacidad y libertad de expresión.

Del mismo modo, se ha insinuado que como en las tareas de Osint y Socmint la información es accesible a cualquier persona, no hay una intromisión ilegítima en la privacidad. En un precedente reciente, la Cámara Criminal y Correccional Federal convalidó un proceso iniciado a raíz de "tareas de relevamiento en la web" efectuadas por funcionarios policiales, en una página de acceso público de compraventa de bienes y servicios. En el caso, vale notar, no se trató de inteligencia en redes sociales que, como se dijo, merecen una protección acentuada por las más graves implicancias de las injerencias estatales en este ámbito.

De cualquier modo, frente al planteo de nulidad de la defensa, que cuestionó la constitucionalidad de lo actuado por la policía, la Cámara sostuvo que el relevamiento realizado por esta "en modo alguno puede considerarse como una intromisión indebida dentro del ámbito privado de las personas a poco que se repare en que fue realizada en derredor de un sitio de acceso público que opera como una plataforma para el intercambio de bienes y servicios entre los usuarios".[83]

Esta postura naturaliza la práctica policial en cuestión con el único argumento de que la información es "de acceso público", sin considerar mínimamente las implicancias para la privacidad y la libertad de expresión, que aquí se han desarrollado. El DIDH impide una admisión irrestricta del "ciberpatrullaje" con la mera mención de que se trata de información pública, como lo hizo la Cámara.

8. Consideraciones finales

A la luz del DIDH, la inteligencia sobre fuentes abiertas y, en especial, sobre redes sociales, es una actividad que condiciona el pleno goce y ejercicio de los derechos a la privacidad y a la libertad de expresión. En un Estado de derecho resulta imprescindible evitar la naturalización de tales actividades estatales, desprovistas de todo control y límite, y sin someterse a exigencias mínimas de sospecha razonable.

Que se trate de fuentes de acceso público a las que las autoridades pueden acceder sin eludir medidas de seguridad no elimina la legítima expectativa de no ser sometidos a políticas de monitoreo y vigilancia estatal en todas nuestras acciones y expresiones en espacios abiertos de internet. Como sociedad estamos llamados a repensar el contenido y alcance del derecho a la privacidad en línea, así como

[82] Juzgado Criminal y Correccional Federal n.° 4, resolución en el expediente CFP 2398/2016, de 23 de mayo de 2016. En el caso, el juez ordenó el procesamiento de una mujer por amenazas en redes sociales sin interrogar siquiera sobre la legalidad del "ciberpatrullaje de rutina" que dio inicio al proceso.

[83] Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, "D.C.N., F.F.X. s/ procesamiento", CFP 889/2018/3/CA1, Sala 2, Sentencia de 3 de febrero de 2020.

los límites y las garantías que deben guiar las actividades de inteligencia estatales sobre fuentes abiertas.

Salvo que estemos dispuestos a vivir en una sociedad de control y vigilancia sin límites, no es admisible que la única forma de ejercer plenamente nuestros derechos sea a escondidas.

Bibliografía

Badeni, Gregorio. *Instituciones de derecho constitucional*. Buenos Aires: Ad-Hoc, 1997.

Bidart Campos, Germán J. *Manual de la Constitución Reformada*. Tomo II. Buenos Aires: Ediar, 2000.

Brennan Center for Justice, New York University School of Law. "Social Media Monitoring. How the Department of Homeland Security Uses Digital Data in the Name of National Security". 2020. Acceso 30 de mayo de 2020. https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf.

Bruno, Fernanda. "Surveillance and Participation on Web 2.0". En *Routledge Handbook of Surveillance Studies*, editado por Kristie Ball, Kevin Haggerty y David Lyon. London - New York: Routledge, 2014.

Carrió, Alejandro D. *Garantías constitucionales en el proceso penal*. Buenos Aires: Hammurabi, 2012.

CELS. "Observaciones del CELS a la Resolución 31/2018 y al Proyecto de protocolo de 'ciberpatrullaje'". 2020. Acceso 30 de mayo 2020. https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf.

Gannon, John. "The Strategic Use of Open-Source Information". *Studies in Intelligence* 45, n.° 3 (2001): 67-71.

Gullco, Hernán. "La doctrina de la 'real malicia' y la reciente jurisprudencia de la Corte Interamericana de Derechos Humanos sobre libertad de expresión", *Revista de Derecho y Ciencias Penales*, n.° 13 (2009): 127-138.

Hampton, Keith *et al.* "Social Media and the 'Spiral of Silence'". Washington, D. C., Pew Research Center, 2014. Acceso 30 de mayo 2020. https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/.

Lever, Annabelle. "Democracy, Privacy and Security". En *Privacy, Security and Accountability: Ethics, Law and Policy*, editado por Adam Moore. London: Routledge, 2016.

Litvachky, Paula *et al.* "El secreto. La seguridad nacional como coartada para un Estado sin controles", editado por CELS, *Derechos humanos en la Argentina. Informe 2019*. Buenos Aires: Siglo XXI, 2019.

Maier, Julio B. J. *Derecho procesal penal*. Tomo III. Buenos Aires: Del Puerto, 2011.

Omand, David, Jaime Bartlett y Carl Miller. "Introducing social media intelligence (Socmint)". *Intelligence and National Security* 27, n.° 6 (2012): 801-823.

Penney, Jonathon W. "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study". *Internet Policy Review* 6, n.° 2 (2017): 1-39.

Pinto, Mónica. "El principio pro homine. Criterios de hermenéutica y pautas para la regulación de los derechos humanos". *La aplicación de los tratados sobre derechos humanos por los tribunales locales*, coordinado por Martín Abregú. Buenos Aires: CELS - Editores del Puerto, 2004.

Poster, Mark. *The Mode of Information: Post-structuralism and Social Context*. Chicago: University of Chicago Press, 1990.

Rrønn, Kira Vrist y Sille Obelitz *Søe*. "Is social media intelligence private? Privacy in public and the nature of social media intelligence". *Intelligence and National Security* 34, n.° 3 (2019): 362-378.

Sagüés, Néstor P. *Manual de derecho constitucional*. Buenos Aires: Astrea, 2007.

Stoycheff, Elizabeth. "Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring". *Journalism & Mass Communication Quarterly* 93, n.° 2 (2016): 296-311.

Ucciferri, Leandro. "Seguidores que no vemos. Una primera aproximación al uso estatal del Open-source intelligence (Osint) y Social media intelligence (Socmint)". Buenos Aires: ADC, 2018. https://adc.org.ar/informes/seguidores-que-no-vemos/.

Williams, Heather e Ilana Blum. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica: RAND Corporation, 2018.

Normas jurídicas y jurisprudencia

Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal (CCCF). Sala I, Causa N.° 25.212, "Ortiz, S. s/ procesamiento", Reg. N° 414, Sentencia de 8 de julio de 1994.

CCCF. Sala II, Causa N.° 20.336, *"Vita, Leonardo G. y otro s/procesamiento"*, Sentencia de 29 de agosto de 2003.

CCCF. Sala I, Causa N.° 37.733, *"Bonafini, Hebe s/sobreseimiento"*, Sentencia de 27 de abril de 2006.

CCCF. Sala I, Causa N.° 40.687, *"Bignone, Reynaldo s/rechazo falta de acción"*, Sentencia de 29 de agosto de 2007.

CCCF. Sala II, "D.C.N., F.F.X. s/ procesamiento", CFP 889/2018/3/CA1, Sentencia de 3 de febrero de 2020.

Comisión Interamericana de Derechos Humanos (CIDH). Declaración de Principios sobre Libertad de Expresión, adoptada en su 108° periodo ordinario de sesiones, 2 al 20 octubre de 2000.

CIDH. Marco jurídico interamericano sobre el derecho a la libertad de expresión, 2009.

Comité de Derechos Humanos. Observación General n.° 16, artículo 17, Derecho a la intimidad, 1988, HRI/GEN/1/Rev.7.

CDH. Observación General n.º 34, Artículo 19, Libertad de opinión y libertad de expresión, 12 septiembre 2011, CCPR/C/GC/34.

Corte Interamericana de Derechos Humanos (Corte IDH). Opinión Consultiva OC-5/85, del 13 de noviembre de 1985. La colegiación obligatoria de periodistas (arts. 13 y 29, Convención Americana sobre Derechos Humanos) solicitada por el gobierno de Costa Rica, Serie A, núm. 05.

Corte IDH. Caso Herrera Ulloa *vs.* Costa Rica, Sentencia de 2 de julio de 2004. Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C No. 107.

Corte IDH. Caso Ricardo Canese *vs.* Paraguay, Sentencia de 31 de agosto de 2004, Fondo, Reparaciones y Costas, Serie C No. 111.

Corte IDH. Caso Kimel *vs.* Argentina, Sentencia de 2 mayo de 2008, Fondo, Reparaciones y Costas, Serie C No. 177.

Corte IDH. Caso Tristán Donoso *vs.* Panamá, Sentencia de 27 de enero de 2009. Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C No. 193.

Corte IDH. Caso Escher y Otros *vs.* Brasil, Sentencia de 6 de julio de 2009. Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C No. 200.

Corte IDH. Caso Usón Ramírez *vs.* Venezuela, Sentencia de 20 de noviembre de 2009. Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C No. 207.

Corte IDH. Caso Fontevecchia y D'Amico *vs.* Argentina, Sentencia de 29 de noviembre de 2011, Fondo, Reparaciones y Costas, Serie C No. 238.

Corte IDH. Caso Granier y otros *vs.* Venezuela, Sentencia de 22 de junio de 2015. Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C No. 293.

Corte IDH. Caso Álvarez Ramos *vs.* Venezuela, Sentencia del 30 de agosto de 2019. Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C No. 380.

Corte Suprema de Justicia de la Nación (CSJN). "Montenegro, Luciano Bernardino", Sentencia de 10 de diciembre de 1981, *Fallos* 303:1938.

CSJN. "Fiorentino, Diego Enrique", Sentencia de 27 de noviembre de 1984, *Fallos* 306:1752.

CSJN. "Rayford, Reginald y otros", Sentencia de 13 de mayo de 1986, *Fallos* 308:733.

CSJN. "Vago, Jorge Antonio c/ Ediciones de La Urraca SA. y otros», Sentencia de 19 de noviembre de 1991, *Fallos*: 314:1517.

CSJN. "Pandolfi, Oscar Raúl c/ Rajneri, Julio Raúl", Sentencia de 1 de julio de 1997, *Fallos*: 320:1272.

CSJN. "Recurso de Hecho. Matte, Domingo Luis; Irigoin, Néstor Félix y otros s/ tenencia de estupefacientes con fines de comercialización –causa n.° 2246–", Sentencia de 18 de julio de 2002, *Fallos* 325:1845.

CSJN. "Patitó José Ángel y otro c/ Diario La Nación y otros y otro s/Daños y perjuicios", Sentencia de 24 de junio de 2008, *Fallos*: 331:1530.

CSJN. "Quaranta, José Carlos s/ inf. ley 23.737 –causa n.º *763*–", Sentencia de 31 de agosto de 2010, *Fallos*: 333:1674.

CSJN. "Recurso de Hecho. Stancatti, Oscar s/ causa n.° 462/2013". Sentencia de 24 de mayo de 2016, *Fallos*: 339:697.

Juzgado Criminal y Correccional Federal n.° 4. Resolución en el Expediente CFP 2398/2016, de 23 de mayo de 2016.

Naciones Unidas. Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Informe 17 de abril de 2013, Frank La Rue, A/HRC/23/40.

Naciones Unidas. Informe La vigilancia y los derechos humanos, 28 de mayo de 2019, David Kaye, A/HRC/41/35.

Naciones Unidas. Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Informe El derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37.

Naciones Unidas. Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Informe El derecho a la privacidad en la era digital, 3 de agosto de 2018, A/HRC/39/29.

Naciones Unidas. Asamblea General. Resolución 68/167. El derecho a la privacidad en la era digital, aprobada el 18 de diciembre de 2013, A/RES/68/167.

Scotus. United States v. Di Re, 332 U.S. 581 (1948), Sentencia de 5 de enero de 1948.

Scotus. Wieman v. Updegraff, 344 U.S. 183 (1952), Sentencia de 15 de diciembre de 1952.

Scotus. Noto v. United States, 367 U.S. 290 (1961), Sentencia de 5 de junio de 1961.

Scotus. New York Times Co. v. Sullivan, 376 U.S. 254 (1964), Sentencia de 9 de marzo de 1964.

Scotus. Garrison v. Louisiana, 379 U.S. 64 (1964), Sentencia de 23 de noviembre de 1964.

Scotus. Katz v. United States, 389 U.S. 347 (1967), Sentencia de 18 de diciembre de 1967.

Scotus. Watts v. United States, 394 U.S. 705 (1969), Sentencia de 21 de abril de 1969.

Scotus. Brandenburg v. Ohio, 395 U.S. 444 (1969), Sentencia de 9 de junio de 1969.

Scotus. United States v. Jones, 565 U.S. 400 (2012), Sentencia de 23 de enero de 2012.

Scotus. United States v. Alvarez, 567 U.S. 709 (2012), Sentencia de 28 de junio de 2012.

Scotus. Riley v. California, 573 U.S. 373 (2014), Sentencia de 25 de junio de 2014.

Scotus. Carpenter v. United States, 585 U.S. (2018), Sentencia de 22 de junio de 2018.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Niemietz V. Germany (n.° 13710/88), Sentencia de 16 de diciembre de 1992.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Amann V. Switzerland (n.° 27798/95), Sentencia de 16 de febrero de 2000.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Rotaru V. Romania (n° 28341/95), Sentencia de 4 de mayo de 2000.

Tribunal Europeo de Derechos Humanos (TEDH). Caso P.G. y J.H. V. The United Kingdom (n.° 44787/98), Sentencia de 25 de septiembre de 2001.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Mikulić V. Croatia (n.° 53176/99), Sentencia de 7 de febrero de 2002.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Retty V. The United Kingdom (n.° 2346/02), Sentencia de 29 de abril de 2002.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Uzun V. Germany (n.° 35623/05), Sentencia de 2 de septiembre de 2002.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Peck V. The United Kingdom (n.° 44647/98), Sentencia de 28 de enero de 2003.

Tribunal Europeo de Derechos Humanos (TEDH). Caso S. y Marper V. The United Kingdom (n.° 30562/04 y 30566/04), Sentencia de 4 de diciembre de 2008.

Tribunal Europeo de Derechos Humanos (TEDH). Gran Sala del TEDH Caso Von Hannover V. Germany (n.° 40660/08 y 60641/08), Sentencia de 7 de febrero de 2012.

Tribunal Europeo de Derechos Humanos (TEDH). Gran Sala del TEDH, Satakunnan Markkinapörssi Oy y Satamedia Oy V. Finland (n.° 931/13), Sentencia de 27 de junio de 2017.

Tribunal Europeo de Derechos Humanos (TEDH). Caso Bărbulescu V. Romania (n.° 61496/08). Sentencia de 5 de septiembre de 2017.

Tribunal Europeo de Derechos Humanos (TEDH). Gran Sala del TEDH, Caso Benedik V. Slovenia (n.° 62357/14), Sentencia de 28 de abril de 2018.