Seguidores que no vemos

Una primera aproximación al uso estatal del *Open-source intelligence* (OSINT) y *Social media intelligence* (SOCMINT)

por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

Con el apoyo de

PRIVACY INTERNATIONAL

Octubre 2018
https://adc.org.ar | https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por el International Development Research Centre (IDRC), el mismo es publicado bajo una licencia Creative Commons Atribución–No Comercial–Compartir Igual.

Índice

Seguidores que no vemos

Una primera aproximación al uso estatal del Open-source intelligence (OSINT) y Social media intelligence (SOCMINT)*

I. Introducción

Se estima que en solo 60 segundos en internet se envían 187 millones de emails, se realizan 3,7 millones de consultas en buscadores, se envían 38 millones de mensajes por WhatsApp, se publican 481 mil *tweets*, se miran 4,3 millones de videos en YouTube, se descargan 375 mil aplicaciones, se comparten 174 mil fotos en Instagram y se gastan unos 862 mil dólares en compras online. Basta con multiplicar estas cifras por horas, días, meses y años, para poner en evidencia la magnitud que ha cobrado internet a lo largo de la última década.[1]

El auge de las diversas iteraciones de la web trajo, con cada instancia de innovación y desarrollo tecnológico, una serie de servicios que permearon la vida diaria en sociedad, modificando la forma en que nos comunicamos con nuestros seres queridos, hacemos negocios, compartimos información, buscamos y consumimos entretenimiento o aprendemos algo nuevo.

Con el advenimiento de plataformas que fomentaron una web más social, se dio inicio a una nueva era de servicios, acompañada por cambios en los modelos de negocios y los patrones de conducta en el consumo de contenido y la interacción de las personas online.

Paralelamente, la necesidad de investigar conductas contrarias a la ley, ya sea que transcurran en el ámbito digital o no, debido a la omnipresencia de la tecnología en la sociedad moderna, ha llevado a que se preste cada vez mayor atención a las relaciones que las personas mantienen con la tecnología y particularmente las actividades que realizan o los servicios que utilizan en internet. Hoy en día,

*El presente documento fue elaborado por **Leandro Ucciferri,** abogado, analista de políticas públicas e investigador del Área Digital de la Asociación por los Derechos Civiles (ADC). https://adcdigital.org.ar | https://adc.org.ar

[1] "What Happens in an Internet Minute in 2018?", Visual Capitalist, mayo 2018, disponible en: http://www.visualcapitalist.com/internet-minute-2018/

los perfiles online que las personas mantienen en las redes sociales sirven como una ventana hacia sus pensamientos, conductas, preferencias, rutinas, vínculos íntimos y profesionales, en definitiva, algunas de las características más esenciales que hacen a la formación de su identidad.

El objetivo de este informe es realizar un aporte a una discusión que actualmente no está teniendo lugar en la agenda de la sociedad ni en los espacios democráticos de construcción de políticas públicas. Bajo la excusa de la libre disponibilidad y publicidad de la información que es compartida en internet, los Estados alrededor del mundo se han aprovechado silenciosamente de su explotación para los más diversos fines. Este documento no pretende ser comprensivo de todas las particularidades intrínsecas a esta temática, sino más bien ser un puntapié inicial que colabore en el impulso del debate público que, desde una perspectiva de protección a los derechos fundamentales, la cuestión merece.

En tal sentido, en los capítulos sucesivos realizamos una primera exploración analizando el creciente uso de técnicas de investigación de información en fuentes abiertas de datos y en redes sociales, por parte de diversos organismos gubernamentales en Argentina, poniendo el foco particularmente desde el punto de vista de la persecución de delitos.

De esta manera, en la **segunda sección** explicamos qué es el *Open-source Intelligence* (OSINT) y el *Social media Intelligence* (SOCMINT), por qué tienen cada vez mayor relevancia en la era digital y cuál es el potencial impacto en los derechos fundamentales. En la **tercera sección** nos abocamos al caso de estudio elegido para nuestra investigación, el uso de estas técnicas con fines de seguridad pública y combate del delito, adentrándonos en el análisis de algunos casos relevantes de los últimos dos años y el creciente rol del Ministerio de Seguridad junto a otras fuerzas de cumplimiento de la ley. Por último, en la **cuarta sección**, brindamos una serie de recomendaciones preliminares para el perfeccionamiento de políticas públicas que sean respetuosas de un abordaje desde los derechos humanos.

II. La investigación en fuentes abiertas: internet y redes sociales ¿Qué es OSINT y SOCMINT?

La investigación de información en fuentes abiertas de datos, conocido en inglés como *Open-source intelligence* (bajo las siglas OSINT), es la práctica que conlleva el uso de un conjunto de técnicas y tecnologías que facilitan la recolección de información que se encuentra disponible públicamente[2], como pueden ser textos, imágenes, videos, audios, e incluso datos geoespaciales. Recién en el momento que a dicha información se le encuentra una utilidad o propósito, y es asignada a una acción concreta, pasa entonces a convertirse en inteligencia propiamente dicha.

[2] Disponible públicamente implica que es accesible para cualquier persona sin necesidad de contar con credenciales especiales de acceso de ningún tipo, en contraposición a información que se encuentra detrás de una capa de protección, por ejemplo usuario y contraseña.

El surgimiento del OSINT puede ser rastreado hasta los inicios de los servicios de inteligencia alrededor del mundo. A medida que el desarrollo tecnológico ha traído novedosas maneras de comunicarnos y compartir información, la investigación en fuentes abiertas fue adaptándose a las nuevas circunstancias. Es así como el nacimiento de la prensa, la radio, la televisión e internet, fueron marcando hitos que impactaron en la cantidad de datos e información disponibles a una inconmensurable multitud de personas a lo largo del mundo.

El desarrollo de internet trazó un antes y un después en las posibilidades de explotación de información mediante herramientas de OSINT, teniendo como resultado su fusión con el resto de las disciplinas de recolección de inteligencia. Si bien el acceso a fuentes abiertas como periódicos, revistas, programas de radio y televisión, o trabajos académicos, es de fácil acceso y de un costo relativamente bajo, con la llegada de internet, y en particular con el crecimiento de la web, los límites que frenaban el crecimiento exponencial del OSINT como una de las principales disciplinas de investigación se fueron reduciendo. Sin embargo, esta situación también presenta desventajas. La cantidad de información generada por minuto en internet se muestra como una navaja de doble filo, ya que poder acceder a prácticamente todo el repositorio de conocimiento producido por la humanidad puede llegar a ser abrumador, desalentador o intimidante, sin mencionar también la cantidad de recursos –de tiempo, humanos, económicos, o una combinación de estos factores– que pueden ser necesarios para procesarla y analizarla efectivamente.[3]

Es al respecto de esto último que se presenta como urgente un debate público sobre la implicancia de estas técnicas de investigación en derechos fundamentales, en particular los derechos a la privacidad y la libertad de expresión. El uso que hacemos de internet hoy en día puede ser explotado con consecuencias en la manera en que llevamos adelante nuestras vidas, toda vez que las fuerzas de seguridad y otros organismos estatales han aprovechado la apertura y publicidad de internet al perpetuar un *status quo* que les permite acceder a la información allí disponible sin necesariamente rendir cuentas sobre cómo, cuándo y por qué. De esta forma se alienta la falacia de que no existe expectativa de privacidad alguna en lo que se publica en internet.

Gracias a este *status quo* se ha popularizado una concepción laxa sobre cuál es el alcance del OSINT, en particular respecto a la inclusión en esta disciplina de la recolección de información en redes sociales. Sin embargo, corresponde trazar una separación incisiva que permita dar cuenta de las particularidades de cada una.

El análisis de redes sociales, denominado en inglés *Social media intelligence* o SOCMINT, implica básicamente la recolección y procesamiento de información en las diversas plataformas (Twitter, Instagram, Facebook, YouTube, Snapchat, por nombrar tan solo algunas de las más populares)

[3] "The Strategic Use of Open-Source Information", John Gannon, Intelligence Community Perspective, disponible en: https://www.cia.gov/library/readingroom/docs/DOC_0006122487.pdf Más información en: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

donde las personas usuarias publican expresiones, fotos, videos, participan de conversaciones o tan solo se informan de los hechos que ocurren en el mundo.

El uso de SOCMINT para llevar a cabo una investigación puede implicar diversas técnicas, como son: la revisión manual del contenido publicado; la revisión de búsquedas específicas de usuarios, *hashtags*, grupos, entre otras; la revisión de las actividades o tipos de contenido publicado por usuarios; el uso de herramientas de scraping para extraer contenido en una página web; e incluso la sistematización de alguna o varias de las técnicas anteriores mediante distintos tipos de software.

La clara separación que merece hacerse entre OSINT y SOCMINT, cuando hablamos del uso que realiza el estado –particularmente para la prevención e investigación del delito–, obedece a que las plataformas de las redes sociales desafían una concepción tajante entre lo público y lo privado, pues, en su mayoría, son ámbitos gobernados por empresas privadas que mantienen sus propias reglas de juego, como son los términos y condiciones y las políticas de privacidad.

Afirmar, por lo tanto, que no hay expectativa de privacidad en el uso que se hace de una red social sería, cuanto menos, incierto, restringiendo el debate que debemos promover como sociedad sobre la regulación de este tipo de técnicas por parte del Estado y el sector privado.

Sostener que vivimos en una sociedad hiperconectada no es novedad. En la última década, la fusión entre nuestras vidas online y offline se ha dado en forma exponencial, ubicua y sigilosa. Con cada avance tecnológico y nuevo producto que sale al mercado, comenzamos a naturalizar la manera en que nos relacionamos con nuestros dispositivos, convirtiéndolos finalmente en una extensión de nuestro cuerpo y mente. De la misma forma es que nuestras interacciones con las personas que nos rodean se han ido digitalizando, al punto en que es más común enterarse en qué andan nuestros familiares y amigos a partir de sus publicaciones en las redes sociales.

Estos fenómenos comenzaron a ser explorados por las ciencias sociales buscando darle un marco teórico a la evolución del comportamiento humano en la era digital. Así, el sociólogo español Manuel Castells lo denomina la “sociedad red”, en referencia a la estructura social en la era de la información, dominada por redes centralizadas bajo un nuevo paradigma de tiempo y espacio que no se encuentra atado a los límites geográficos.

El análisis de este fenómeno no puede evitar traer a colación el factor económico. El desarrollo de la economía digital por las principales empresas tecnológicas, basadas en su mayoría en Silicon Valley, California, ha moldeado la relación que sostienen las personas con la tecnología. A nivel individual, las personas participan voluntaria y alegremente auto-exponiéndose, argumenta el filósofo Byung-Chul Han, convirtiéndose la exposición en una coerción sistémica alimentado por las mismas plataformas. Han denomina a este nuevo fenómeno "sociedad de la exhibición", en donde todo debe ser mostrado para existir, produciendo así valor de exposición, el cual tiene por fin generar atención –o *Likes*, en el mundo de las redes sociales–, pues cada persona es también su propio objeto publicitario.[4]

[4] La sociedad de la Transparencia (Transparenzgesellschaft), Byung-Chul Han, Herder, 2013.

El mercado digital ideado y profundizado por empresas como Facebook y Google, ponen en el eje de sus negocios a la explotación masiva de los datos obtenidos de sus usuarios con fines de monetizar la atención de las personas para vender publicidad. Esto es lo que Han denomina el "mercado panóptico", donde el capitalismo de la vigilancia somete todo a una exposición obligatoria, a la vez que el exceso de visualización convierte todo en una mercancía. Mientras tanto, los habitantes del panóptico[5] digital piensan que son libres.

Habiendo brindado un marco de análisis sobre cómo las redes sociales están diseñadas para que las personas faciliten una ventana hacia su vida íntima, avancemos con otros dos aspectos íntimamente vinculados a SOCMINT: en primer lugar, su utilidad y confiabilidad y, en segundo lugar, su impacto en la privacidad.

En primer lugar, lo que las personas expresan en internet, y en particular en las redes sociales, no necesariamente se condice con lo que ellas crean, intentan o piensan en realidad. En el campo de la psicología denominan efecto de desinhibición online al fenómeno que busca explicar el comportamiento que tienen las personas cuando interactúan en el mundo digital en contraposición a sus interacciones con otras personas cara a cara.

En tal sentido, las personas pueden mostrar comportamientos sustancialmente distintos sea que se trate del mundo físico o del digital. Algunas de las causas que estudian el origen de estos comportamientos son: la sensación de protección obtenida por factores como la distancia y la temporalidad; la igualdad o monotonía que recubre a los perfiles online resultando en cierta minimización del estatus o autoridad; o el producto de una imaginación disociativa que lleva a creer que lo ocurrido en el mundo online es ficticio dentro de una realidad separada del mundo físico.[6]

Las plataformas de redes sociales introducen una capa de complejidad al estudio sobre las expresiones online toda vez que ciertas herramientas o funciones hacen más difusa la comprensión sobre el alcance de lo que una persona expresa en sus publicaciones, como puede ser la amplificación del mensaje fuera de los círculos sociales propios.

En segundo lugar, el control que tienen las personas usuarias de qué información sobre sí mismas es publicada en las redes sociales (en otras palabras, la denominada autodeterminación informativa) no siempre es una simple cuestión de elección voluntaria y predeterminada, entrando en juego diversos factores, como son:

- los metadatos que acompañan a las publicaciones (geolocalización, fecha, idioma, dispositivos

[5] El término panóptico fue ideado por Jeremy Bentham, filósofo inglés fundador del movimiento utilitarista, a fines del siglo XVIII, refiriéndose al diseño estructural de una cárcel en la cual todos los prisioneros pueden ser observados al mismo tiempo en sus celdas individuales, pero sin que ellos puedan saber si efectivamente son observados por los guardias, produciendo así la sensación de encontrarse bajo vigilancia a toda hora del día. Este concepto fue luego estudiado por el filósofo francés Michel Foucault en su obra "Vigilar y castigar" (1975).

[6] "The Online Disinhibition Effect", Suler, J. (2004). CyberPsychology and Behavior, 7, 321-326. Disponible en: https://pdfs.semanticscholar.org/c70a/ae3be9d370ca1520db5edb2b326e3c2f91b0.pdf

utilizados, etc.)[7];

- las publicaciones realizadas por terceros que contienen información personal;
- las configuraciones de privacidad, que van actualizándose a medida que las plataformas evolucionan, teniendo en cuenta que las mismas no son siempre las más protectoras por defecto, ya que en general la norma es la publicidad. Por otra parte, la inclusión de nuevas funciones en la plataforma conlleva la recolección de nuevos tipos de información y con ello una nueva curva de aprendizaje al respecto.

En tal sentido, la expectativa de privacidad que una persona puede tener en una red social tiene directa relación con el conocimiento que esta tiene sobre el funcionamiento de dicha plataforma.

La jurisprudencia europea determinó que las personas cuentan con una expectativa de privacidad incluso en espacios públicos. Así lo sostuvo el Tribunal Europeo de Derechos Humanos (TEDH) en el caso *Peck v. United Kingdom* (2003), donde reconoció la existencia de una zona de interacción de la persona con los demás, incluso en un contexto público, que puede entrar en el ámbito de la vida privada y ser susceptible de protección.[8]

El análisis de perfiles online no se encuentra relegado exclusivamente a los comentarios, opiniones y otros diversos tipos de expresiones publicadas en las plataformas web, como mencionamos brevemente en los párrafos anteriores, generalmente las publicaciones pueden estar acompañadas de otro tipo de información igual o más valiosa y que en ocasiones no se le da mayor atención. Cuando datos como la geolocalización, el sentimiento detrás de las expresiones, la red de contactos que interactúan con ese perfil o en base a un contenido específico, son recolectados por días, semanas, meses o años y analizada en conjunto, pueden darnos una visión increíblemente detallada de los

[7] Por ejemplo, un solo tweet de 140 caracteres puede ir acompañado de metadatos que representan unas 20 veces el tamaño de lo publicado. Una descripción detallada sobre los metadatos que acompañan a tus tweets y cómo analizarlos puede leerse en el siguiente enlace: https://blog.0day.rocks/you-will-be-surprised-by-what-your-tweets-may-reveal-about-you-and-your-habits-3bc907688bc8

[8] En el caso de Peck contra el Reino Unido, el demandante se quejó de la divulgación a los medios de comunicación del material grabado por el circuito cerrado de televisión (CCTV), que dio lugar a la publicación y difusión de imágenes que lo mostraban en un intento de suicidio. La autoridad local que operaba el sistema CCTV, el Brentwood Borough Council, había dado las imágenes a los medios de comunicación con el objetivo de promover la eficacia del sistema en la detección y prevención de delitos. La Comisión de Televisión Independiente (ITC) y la Comisión de Normas de Radiodifusión (BSC) consideraron que el enmascaramiento era inadecuado ya que vecinos, colegas, amigos y familiares que veían los programas reconocían al demandante. El Tribunal Europeo de Derechos Humanos determinó que la divulgación de las imágenes a los medios de comunicación resultó en una infracción del artículo 8 de la Convención Europea. La Corte hace hincapié en que el solicitante estaba en una calle pública pero que no estaba allí para participar en ningún evento público, ni era una figura pública, y que la divulgación de las imágenes no era necesaria en una sociedad democrática. Case of Peck v. United Kingdom, Tribunal Europeo de Derechos Humanos, enero 2003, http://merlin.obs.coe.int/iris/2003/6/article2.en.html Más información disponible en: "CCTV and Human Rights: the Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41", Caoilfhionn Gallagher, Surveillance & Society, 2004, http://www.surveillance-and-society.org/articles2(2)/humanrights.pdf

hábitos y costumbres de una persona a lo largo de su vida.[9]

El análisis sistemático de lo que ocurre en los perfiles de redes sociales por organismos estatales no dista sustancialmente de una realidad bajo la cual todas las conversaciones en los espacios públicos urbanos son grabadas con micrófonos.

Además de la clara injerencia sobre la privacidad de las personas, el monitoreo y análisis de la información publicada en redes sociales conlleva efectos claros sobre la libertad de expresión. Las personas ajustan o modifican su comportamiento cuando saben o sienten, aún en una remota posibilidad, que están siendo observadas y juzgadas. El uso de técnicas de SOCMINT alimenta un efecto inhibitorio, *chilling effect* en el derecho anglosajón, sobre la expresión de las personas en internet, llevando en muchos casos al ajuste incremental de sus propios niveles de autocensura.[10]

1. Una problemática global con injerencias reales en nuestros derechos fundamentales

Diversos casos reportados en los últimos años dan cuenta de la magnitud global de esta temática, lejos de ser un problema enfrentado por un puñado de países, varios gobiernos al rededor del mundo viraron hacia la implementación de técnicas de OSINT y SOCMINT en sus labores, reflejando una nueva realidad para la vida digital moderna: nuestra actividad en internet, y particularmente en las redes sociales, está siendo mirada fijamente con ojos lujuriosos sobre su potencial para la investigación de conductas contrarias a la ley.

En Boston, Estados Unidos, la American Civil Liberties Union (ACLU) reportó preocupaciones sobre discriminación racial por parte del departamento de policía al utilizar una herramienta para monitorear redes sociales enfocándose injustamente en personas que utilizaban el hashtag *#MuslimLivesMatter* en Twitter.[11] Este mismo comportamiento por parte del gobierno estadounidense

[9] Siguiendo este argumento, encontramos en el derecho anglosajón la denominada "Teoría del mosaico", desarrollada por Orin Kerr, según la cual mediante la recolección y agregación exhaustiva de datos producto de la vigilancia, incluso cuando en principio los mismos puedan parecer inocuos, se logra un conocimiento más detallado que al analizar cada pieza de información de manera aislada, de esta forma, a través del paso del tiempo se puede construir un mosaico de hábitos, relaciones y más precisiones sobre la vida privada de las personas vigiladas, lo que implica una violación a la protección de la Cuarta Enmienda de la Constitución estadounidense. "The Mosaic Theory of the Fourth Amendment", Orin Kerr, 111 MICH. L. REV. 311, 312 (2012): https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1079&context=mlr; "How Long is Too Long? The 4th Amendment and The Mosaic Theory", 2014: http://lawandlibertyblog.com/nyujll/2014/6/3/how-long-is-too-long-the-4th-amendment-and-the-mosaic-theory

[10] Una lectura recomendada al respecto de los efectos inhibitorios de la vigilancia en la libertad de expresión online puede consultarse en: "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", Jon Penney, Internet Policy Review, 27 de mayo de 2017, disponible en: https://ssrn.com/abstract=2959611

[11] "Boston police's social media surveillance unfairly targeted Muslims, ACLU says", Alanna Durkin Richer, Associated Press / Boston Globe, 7 de febrero de 2018, disponible en: https://www.bostonglobe.com/metro/2018/02/07/boston-police-social-media-surveillance-unfairly-targeted-muslims-aclu-says/9JUpzPmy8Tsr5RLxvCm61M/story.html

había sido reportado previamente en el caso del movimiento *#BlackLivesMatter*.[12]

En Canadá, múltiples agencias y entidades gubernamentales utilizan herramientas y prácticas para monitorear diversas redes sociales en forma proactiva,[13] llegando incluso a prestar ayuda y recursos en el desarrollo de un software que facilita la recolección y el procesamiento de la información.[14]

En Egipto, a mediados de 2014, se reportó el plan del gobierno para comprar tecnologías que faciliten el monitoreo de las publicaciones en las redes sociales, justificándolo en la necesidad de identificar "riegos de seguridad" y "personas que representen un peligro para la sociedad" mediante la recolección y análisis de expresiones que constituyen "ideas destructivas". En el documento filtrado a la prensa con la licitación para la compra, el Ministerio del Interior aclara a qué se refiere con "ideas destructivas", mediante un extenso listado, en donde menciona: blasfemia y escepticismo en las religiones, tomar declaraciones fuera de contexto, pornografía y falta de moralidad, sarcasmo, entre otras situaciones.[15]

A mediados de 2018, el presidente egipcio ratificó una ley que habilita al Consejo Supremo de Reglamentos de Medios a poner bajo supervisión aquellas personas que tengan más de cinco mil seguidores en alguna red social o posean un blog o sitio web personal, incluyendo la facultad de suspender o bloquear cuentas que difundan noticias falsa o cualquier información incitando al odio, violencia o violación de la ley.[16]

En Venezuela, desde el año 2014 se han reportado al menos dos docenas de personas encarceladas, generalmente sin juicio previo, por expresiones publicadas en sus perfiles de la red social Twitter, en oposición al gobierno actual o incluso por mensajes con información financiera como la cotización del dólar.[17]

En Chile, se ha reportado que la fuerza de seguridad federal, Carabineros, realiza actividades de "ciberpatrullaje" en las redes sociales con un equipo específicamente destinado a dichas tareas.[18]

[12] "The Government Is Watching #BlackLivesMatter, And It's Not Okay", Nusrat Choudhury, ACLU, 4 de agosto de 2015, disponible en: https://www.aclu.org/blog/racial-justice/government-watching-blacklivesmatter-and-its-not-okay

[13] "The Canadian Government Told Us It's Down With Social Media Monitoring", Ben Makuch, Motherboard, 14 de noviembre de 2014, disponible en: https://motherboard.vice.com/en_us/article/vvbpb9/the-canadian-government-told-us-its-down-with-social-media-monitoring

[14] "Monitoring your memes: The government has helped develop software to monitor your social media for threats", Justin Ling, VICE News, 9 de marzo de 2017, disponible en: https://news.vice.com/en_ca/article/nedxez/the-canadian-government-developed-software-to-monitor-your-social-media-for-threats

[15] "Egyptian Government Wants Surveillance System To Monitor 'Destructive Ideas' On Social Networks", Privacy International, 13 de junio de 2014, disponible en: https://privacyinternational.org/blog/1252/egyptian-government-wants-surveillance-system-monitor-destructive-ideas-social-networks

[16] "Egypt's President el-Sissi ratifies law to monitor social media users", DW, 2 de septiembre de 2018, disponible en: https://p.dw.com/p/34Aak

[17] "Encarcelado por tuitear", Luis Carlos Díaz, Derechos Digitales, 18 de junio de 2018, disponible en: https://www.derechosdigitales.org/12273/encarcelado-por-tuitear/

[18] "El desconocido 'ciberpatrullaje' de Carabineros en las redes sociales", Víctor Rivera, La Tercera, 28 de agosto

III. "Ciberpatrullando" internet: El rol de la investigación en fuentes abiertas en Argentina

La aplicación de técnicas y herramientas de investigación en fuentes abiertas comenzó a permear en el Estado desde hace al menos una década. A lo largo de estos años, varios organismos gubernamentales han explorado el uso de diversas plataformas y tecnologías que permiten aprovechar los datos e información publicada en internet para perseguir los fines y objetivos propios a sus roles. En tal sentido, podemos encontrar iniciativas desde el ámbito fiscal, el educativo y el de seguridad pública, por nombrar tan solo aquellas que han cobrado relevancia pública.

A comienzos de 2007, el entonces director de la Agencia de Recaudación de la Provincia de Buenos Aires (ARBA) anunciaba la reciente incursión del organismo en tareas de inteligencia fiscal mediante el uso de imágenes satelitales. En diálogo con el diario La Nación, el funcionario declaró que llevaban trabajando cuatro años en la digitalización de los planos de las parcelas y propiedades del territorio bonaerense, a partir de los cuales comenzaron a entrecruzar la información con imágenes satelitales de Google Earth Pro (una licencia que en su momento costaba 400 dólares anuales, pero en 2015 Google lo convirtió en un servicio gratuito), así se facilitaba el posterior envío de inspectores para constatar la información previamente recolectada.[19]

En junio de 2008, ARBA daba a conocer los resultados de una investigación de cuatro años que tuvo por objetivo la identificación de evasores en el rubro agrario. Para comprobar las declaraciones impositivas efectuadas por los propietarios de terrenos mayores a las 50 hectáreas, el equipo de inteligencia de ARBA utilizó imágenes satelitales para analizar la existencia de construcciones y mejoras realizadas en los terrenos, lo que les permitió descubrir, por ejemplo, cultivos no declarados.[20]

En igual sentido, en 2012, la Agencia de Recaudación Municipal de la ciudad de Mar del Plata anunciaba operaciones en las cuales –a los fines de detectar inconsistencias en las declaraciones impositivas– había entrecruzado información de la base de datos del municipio, la cartografía de ARBA y las imágenes satelitales actualizadas en Google Maps.[21]

La incursión de ARBA en la explotación de imágenes satelitales pasó a un mayor nivel tecnológico luego de la presentación del programa "Monitoreo Estratégico Satelital Integrado" en 2014, el cual le facilita al organismo el cruzamiento de información entre 18 satélites y diversas bases de datos

de 2018, disponible en: https://www.latercera.com/nacional/noticia/desconocido-ciberpatrullaje-carabineros-las-redes-sociales/299027/

[19] "Montoya busca evasores con el Google", La Nación, 21 de febrero de 2007, disponible en: https://www.lanacion.com.ar/885329-montoya-busca-evasores-con-el-google

[20] "Con satélites, detectaron 10.000 silos sin declarar en Buenos Aires", Clarín, 22 de junio de 2008, disponible en: https://www.clarin.com/ediciones-anteriores/satelites-detectaron-10000-silos-declarar-buenos-aires_0_HyKze0nATKe.html

[21] "ARBA y la Municipalidad detectan grandes empresas y constructores evasores", La Capital, 25 de julio de 2012, disponible en: http://www.lacapitalmdp.com/noticias/La-Ciudad/2012/07/25/225280.htm?ref=ar

con información tributaria,[22] así como también del acuerdo con la Comisión Nacional de Actividades Espaciales (CONAE) y el uso de satélites más precisos para la captura de imágenes.[23]

A mediados de 2016, nuevamente en la Provincia de Buenos Aires, el gobierno llamó a licitación privada para la contratación de un servicio "de implementación de un observatorio analítico, actualizado en tiempo real, sobre las diversas problemáticas de la educación (...) que son expresadas por los distintos actores de la comunidad educativa, incluyendo al propio Estado y sus políticas públicas, a través de las redes sociales", con un presupuesto estimado en $1.597.200.[24]

A comienzos de septiembre de 2017, el Ministerio de Economía y Finanzas de la Ciudad Autónoma de Buenos Aires autorizó el procedimiento de licitación pública para la provisión de una "Solución De Analítica para Datos Estructurados y Big Data", por un total de $17.500.000, con el objetivo de equipar con herramientas a la Administración Gubernamental de Ingresos Públicos (AGIP) para poder identificar y gestionar riesgos que lleven a la eventual evasión impositiva, citando como ejemplo en el pliego la posibilidad de predecir el comportamiento de los contribuyentes a partir del seguimiento de los *tweets* publicados y así identificar conversaciones que den indicios sobre la intención de cometer fraude.[25]

Dos semanas después, a mediados del mismo mes, se prorrogó la apertura de ofertas para la licitación, habiéndose recibido "numerosas consultas y solicitudes de prórroga".[26] Finalmente, a fines de diciembre de 2017, se dejó sin efecto la licitación,[27] "con el objeto de contemplar las necesidades de la Dirección General de Estadísticas y Censos, y garantizar una mayor participación". Según consta en el Boletín Oficial, se habían recibido las ofertas de las firmas "Avanzit Tecnología S.A."[28], "Consenit S.A."[29] y "Grupo Net S.A."[30].

1. Todo lo que *tuitees* podrá ser utilizado en tu contra

Adentrémonos a continuación al ámbito de la seguridad pública, el cual elegimos como caso de estudio para el enfoque de esta temática y así poder analizar en detalle algunos de los principales sucesos ocurridos en los últimos dos años, a partir del cambio en la administración pública, así como

[22] "MESI: Arba optimiza el monitoreo satelital", ARBA, https://bit.ly/2z14U7w

[23] "Tecnología satelital para combatir la evasión", ARBA: https://bit.ly/2q9ct83

[24] Licitación Privada N° 9/16, Boletín Oficial de la Provincia de Buenos Aires, 11 de julio de 2016, disponible en: http://www.gob.gba.gov.ar/Bole/pdfs/2016-07-11/OFICIAL2016-07-111467923140.pdf

[25] Licitación Pública 8618-1261-LPU17, página 184 y 185, disponible en: https://bit.ly/2qb6dNg

[26] Boletín Oficial, página 202, disponible en: https://bit.ly/2PRWrdV

[27] Boletín Oficial CABA, página 247, disponible en: https://bit.ly/2PjfGA3

[28] www.avanzit.com.ar

[29] www.consenit.com

[30] www.gruponet.com.ar

también las tendencias que se han ido originando y que entendemos se irán profundizando en un futuro cercano.

La llegada de una nueva cara al Poder Ejecutivo, tras las elecciones presidenciales de fines de 2015, implicó un giro de ciento ochenta grados en las prioridades de las políticas públicas impulsadas por el Estado. La nueva administración, empoderada ante la victoria electoral a nivel nacional, en la provincia de Buenos Aires y en la Ciudad Autónoma de Buenos Aires, se encargó de promover una nueva relación del Estado con la tecnología, impulsando una impronta de modernidad, no solamente en la forma de hacer política, sino también en la relación de los organismos estatales con los ciudadanos.

Entre 2016 y 2017, en medio de un contexto de repentinos cambios en las políticas económicas y sociales que incluyeron la revisión de los contratos de empleados en la administración pública, una serie de casos que involucraban a distintos usuarios de redes sociales tomaron estado mediático, al encontrarse como sujetos de investigaciones judiciales tras la imputación de la comisión de distintos delitos originados por las expresiones que habían publicado en sus cuentas.

En mayo de 2016, una mujer fue procesada por el delito de amenazas contemplado en el Art. 149 bis del Código Penal de la Nación[31], reprimido con una pena de 6 meses a 2 años de prisión (y agravado cuando las amenazas fueren anónimas), en forma conjunta al delito de actos discriminatorios previstos por el Art. 3 de la Ley 23.592[32] que contempla a quienes por cualquier medio "alentaren o iniciaren a la persecución o el odio contra una persona o grupos de personas a causa de su raza, religión, nacionalidad o ideas políticas", acción reprimida con una pena de 1 mes a 3 años de cárcel.[33]

Los fundamentos para el procesamiento se basaron en la publicación de diversos *tweets* publicados a principios de marzo de 2016 en los cuales la persona amenazó al Presidente recién electo, Mauricio Macri, y a su entorno familiar, en particular a su hija menor. El juez de primera instancia, Ariel Lijo, destacó en la resolución que "gran cantidad de usuarios de la red se vieron alarmados por aquellas publicaciones, haciéndose eco de estas, incluso, en diversos medios virtuales".[34] Al momento de efectuarse las publicaciones, los *tweets* con las amenazas habían llegado apenas a 8 *retweets* y a 2 *likes*, sin embargo, los *tweets* fueron rápidamente capturados por una multiplicidad de usuarios, en su mayoría afines al nuevo gobierno, que lograron difundir dichas expresiones a miles de usuarios de la plataforma, principalmente mediante capturas de pantalla.[35] Basta con realizar una simple búsqueda

[31] El texto completo actualizado del Código Penal de la Nación se encuentra disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

[32] El texto completo de la Ley 25.592 se encuentra disponible en: https://bit.ly/2rcZdRP

[33] "El juez Lijo procesó a una mujer por amenazar a Mauricio Macri y a su familia", Centro de Información Judicial, 23 de mayo de 2016, disponible en: http://cij.gov.ar/nota-21585-El-juez-Lijo-proces–a-una-mujer-por-amenazar-a-Mauricio-Macri-y-a-su-familia.html

[34] Poder Judicial de la Nación, Juzgado Criminal y Correccional Federal 4, 2398/2016, Página 2.

[35] En tal sentido, puede consultarse un ejemplo en: https://bit.ly/2qbn5Dk (Recuperado el 13 de septiembre de 2018)

en Twitter con el nombre de usuario utilizado por la persona que realizó las amenazas para revisar la evolución de los intercambios, la información compartida y el tono de las publicaciones.[36]

Esta fue una de las primeras causas a partir de la cual se comenzó a popularizar el término "ciberpatrullaje", definido por el juez Lijo como aquel mediante el cual "los efectivos [de la Policía] se abocan a la prevención de delitos, contravenciones y faltas realizados en la red de internet". Es así como surge de la resolución que el Área de Cibercrimen de la Policía Metropolitana (Policía de la Ciudad de Buenos Aires) llevó a cabo "un rastrillaje en fuentes abiertas de la red internet". Asimismo, la Policía realizó búsquedas en Facebook para identificar el perfil asociado a la misma persona detrás de la cuenta de Twitter.

Antes de continuar con la reseña del caso, cabe mencionar otro fenómeno que se ha vuelto cada vez más común en los últimos años y que podemos identificar al observar los numerosos tweets de varios usuarios que se originaron con motivo de las amenazas publicadas: la difusión de información personal con fines de intimidación o el comúnmente llamado "escrache".

Luego de que las amenazas cobraron relevancia mediática, diversos usuarios de Twitter comenzaron a difundir datos personales de quien luego sería procesada, como son el número de su DNI y CUIT, su domicilio, su nombre completo y fecha de nacimiento. De esta forma, los usuarios pasan de ser simples participantes en la conversación o intercambios generados, a convertirse en policías, fiscales y jueces al mismo tiempo. Esta situación fue evaluada por el juez al único efecto de justificar la configuración de los delitos que le son imputados a la usuaria de Twitter, por haber provocado un estado de conmoción incitando a la violencia en la conversación mantenida en la red social. Sin perjuicio de ello, el juez aprovechó para remarcar que si en cambio la persona hubiere expresado críticas en la actuación del gobierno –incluso bajo un tono hostil o agraviante–, las publicaciones habrían estado enmarcadas dentro de la protección constitucional a la libre expresión.

Según consta en la resolución, al momento de realizar la declaración indagatoria, la usuaria de Twitter imputada justificó la motivación de sus expresiones en un exabrupto por haber perdido recientemente su trabajo en el Ministerio de Desarrollo Social de la Nación. Sin embargo, el juez determinó que se configuró el delito de amenaza ya que la imputada realizó diversas publicaciones que fueron acompañadas con la modificación de la información personal de su perfil en Twitter (nombre, avatar y biografía) acorde a dichas expresiones, excediendo el concepto de "exabrupto".

En la sección VII de la resolución, el juez analizó el impacto que su decisión podía tener en el derecho a la libertad de expresión. En primer lugar, el juez determinó que los mensajes de la usuaria de Twitter se encontraban enmarcados en el concepto de "expresiones de odio", por ende encuadraban en las expresiones prohibidas por los diversos instrumentos de derechos humanos. En segundo lugar, evaluó el potencial efecto inhibitorio o disuasivo –*chilling effect*–, reconociendo que el mismo puede convertirse en una mecanismo internalizado de censura que afecta a toda la sociedad.

[36] Ver por ejemplo: https://twitter.com/search?f=tweets&vertical=default&q=%40lamarikaos&src=typd

Según el razonamiento seguido por el juez, "la sanción que pudiera corresponder a la imputada no producirá que quienes se ven involucrados en el debate democrático de la nación, restrinjan, consciente o inconscientemente, sus dichos constitucionalmente protegidos por temor a una pena que pudiera recaerles de idéntica índole".[37] Esto es así, explicó el juez, pues el caso examinado gravitaba en torno a las mencionadas "expresiones prohibidas".

Sin embargo, hay otra situación que incumbe al análisis de potenciales efectos inhibitorios en la libertad de expresión, con el posible efecto adverso de la autocensura, y que fue omitida por el juez probablemente por no encontrarse directamente vinculado al objeto de la causa –las amenazas y expresiones de odio publicadas–, la misma se encuentra directamente vinculada a la problemática que buscamos dilucidar en el presente informe. La acción de "ciberpatrullar" las redes sociales, e internet en general, es algo que puede provocar una injerencia negativa en el modo en el que utilizamos la web, ya sea para comunicarnos, para intercambiar y formar ideas o encontrar información, por nombrar tan solo los fines más elementales. Todo ello puede verse socavado cuando se utilizan herramientas, tecnologías y prácticas basadas en políticas sobre las cuales hay poca o nula transparencia, tanto respecto a su alcance como a su rendición de cuentas y control.

En los meses subsiguientes fueron apareciendo otras causas judiciales iniciadas a partir de amenazas, dirigidas a funcionarios públicos, expresadas en las redes sociales. En diciembre de 2016, un hombre fue procesado por publicar mensajes amenazantes contra el presidente y la vicepresidenta de la Nación, la ministra de Seguridad de la Nación y la gobernadora de la Provincia de Buenos Aires.[38] Finalmente, el caso fue elevado a juicio en mayo de 2017, imputándosele los delitos de amenazas anónimas, intimidación pública y actos de propaganda basada en ideas con el objeto de la justificación o promoción de la discriminación racial o religiosa (Arts. 45, 55, 149 bis, 211 del Código Penal y art. 3º de la Ley 23.592).[39] En igual sentido, una mujer fue procesada en julio de 2018 por una serie de amenazas expresadas contra diversos funcionarios de los poderes Ejecutivo y Judicial efectuadas en septiembre de 2016, los delitos imputados fueron los mismos analizados en las reseñas de los casos anteriores.[40] En este último caso, el primer *tweet* que originó la causa tiene solamente 6 *likes*,[41] mientras que el segundo *tweet* tiene 8 *retweets* y 10 *likes*,[42] al momento de la elaboración del presente informe.

[37] Poder Judicial de la Nación, Juzgado Criminal y Correccional Federal 4, 2398/2016, Página 34.

[38] "Detuvieron a un hombre que amenazó a Mauricio Macri por Twitter", Infobae, 20 de diciembre de 2016, disponible en: https://www.infobae.com/politica/2016/12/20/detuvieron-a-un-hombre-que-amenazo-a-mauricio-macri-por-twitter/

[39] "Elevan a juicio oral una causa por intimidación y amenazas contra Mauricio Macri", Centro de Información Judicial, 16 de mayo de 2017, disponible en: http://cij.gov.ar/nota-25920-Elevan-a-juicio-oral-una-causa-por-intimidaci-n-y-amenazas-contra-Mauricio-Macri.html

[40] https://web.archive.org/web/20180914195133/https:/twitter.com/Albor_Adrian/status/1023962054678532096

[41] Recuperado el día 14 de septiembre de 2018, disponible en: https://bit.ly/2CDjh5k

[42] Recuperado el día 14 de septiembre de 2018, disponible en: https://bit.ly/2PVfu7o

A partir de los casos reseñados anteriormente, podemos remarcar algunos interrogantes que surgen en el análisis del impacto de estas técnicas de investigación en los derechos de las personas: ¿Para la configuración de delitos de intimidación pública, cómo se mide la relevancia de las expresiones online? ¿Acaso es suficiente medirla a través de la cantidad de *retweets*, *favs*, *likes* o interacciones? En igual sentido, si las expresiones son realizadas por una persona con pocos seguidores –como la mayoría de los casos mencionados en este capítulo– o contactos en su perfil, ¿es muy distinto a que realice las mismas expresiones en una plaza o parque? ¿El número y tipo de seguidores debería ser analizado para identificar si son cuentas de personas reales en contraposición a simples perfiles *spam* o *bots*?

En el caso de esta última pregunta, podemos argumentar que las amenazas investigadas en varias de las causas judiciales, cobraron mayor relevancia una vez que las mismas fueron identificadas por cuentas oficialistas –afines al actual gobierno–, promoviendo dichas expresiones hacia sus propios contactos con el objetivo de repudiarlas, pero logrando también como efecto adverso darle mayor notoriedad a algo que podría haber pasado desapercibido.

Si tuviésemos que definir el punto cúlmine a partir del cual el "ciberpatrullaje" comienza a tomar un rol más preponderante en la conversación pública con un Estado que empieza a mostrarse más proactivo en la persecución del delito, el mismo empieza a cobrar forma entre fines de enero y principios de febrero de 2017, fecha en la cual la cuenta de Twitter de la ministra de Seguridad, Patricia Bullrich, fue comprometida, víctima de un *phishing*[43] enviado a su email institucional haciéndose pasar por un mensaje oficial desde la Embajada de Bolivia, junto con varias direcciones de email institucionales del Ministerio. Este suceso se dio a conocer rápidamente en Twitter, en donde los usuarios se percataron de los mensajes publicados desde la cuenta de Bullrich, haciéndose eco de la noticia y comenzando a difundirla junto con detalles del presunto acceso ilegítimo.[44]

Recién a mediados de febrero del mismo año se detuvieron a dos personas como presuntos responsables del *phishing* y el consecuente acceso ilegítimo a la cuenta de Twitter de la ministra y los correos institucionales del Ministerio de Seguridad. En marzo, el juez de primera instancia dictó el procesamiento de una de las personas detenidas. En la resolución quedó asentado el rol que tuvo la División Delitos Tecnológicos de la Policía Federal mediante las tareas de "ciberpatrullaje" llevadas a cabo por el cabo Jorge Landajo.

De acuerdo con la descripción brindada por el juez, el informe de la Policía que desarrolló las tareas de "ciberpatrullaje" se basó en consultas en motores de búsqueda, Twitter e Instagram. Como parte de la investigación, el cabo de la Policía Federal recuperó diversos *tweets* publicados por un conocido experto de la comunidad técnica que difundió lo acontecido en su perfil personal de Twitter.[45]

[43] El Phishing es una técnica de ingeniería social utilizada generalmente para obtener información confidencial. Más información en: https://www.segu-info.com.ar/malware/phishing.htm

[44] Los tweets recuperados el día 26 de enero de 2017 se encuentran disponibles en: https://bit.ly/2yyLDL3

[45] "Patricia Bullrich y el 'ciberpatrullaje'", Javier Smaldone, 9 de marzo de 2017, disponible en:

Lo ocurrido con la cuenta de Twitter de la ministra y los correos institucionales del Ministerio de Seguridad sirvió de base para justificar una nueva impronta en la manera en que las fuerzas federales abordarían la persecución del delito. Tan solo tres meses después del incidente, la ministra anunció el re-lanzamiento de la Policía Federal, destacando que la misma pasará "de las comisarías a la investigación, de los agentes a los detectives, del territorio a un despliegue inteligente y sorpresivo, sin aviso", remarcando además que se abocará al "ciberpatrullaje" con el objetivo de encontrar bandas delictivas en el ámbito digital.[46]

Tan solo diez días antes de darse inicio a la XI Conferencia Ministerial de la Organización Mundial del Comercio (OMC), con sede en Buenos Aires, un nuevo suceso pondría a Argentina en el *spotlight* internacional. Sesenta y cuatro personas, en su mayoría defensores de derechos humanos y activistas, correspondientes a veintiún organizaciones de la sociedad civil, fueron noticiadas por la OMC que, si bien habían sido aceptadas y debidamente acreditadas para participar de la Conferencia, las autoridades argentinas encargadas de la seguridad habían decidido denegar su acreditación, con el riesgo de ser incluso denegadas entrada al país.[47]

En un comunicado a comienzos de diciembre de 2017, el Ministerio de Relaciones Exteriores buscaba justificar esta decisión al establecer que algunos de los inscriptos "habían hecho explícitos llamamientos a manifestaciones de violencia a través de las redes sociales, expresando su vocación de generar esquemas de intimidación y caos".[48] La noticia no tardó en generar polémica en las redes sociales y medios de comunicación a nivel internacional.[49] En medio de deportaciones y conflictos con la entrada de los participantes extranjeros a la Conferencia, las dudas sobre cómo había procedido el gobierno argentino para llegar a la conclusión del comunicado de Cancillería aún quedaban por ser dilucidadas, pues la selección de organizaciones desacreditadas no parecía responder a lógica alguna.

Varias dudas inundaban la discusión pública al respecto. ¿Cómo habían llegado a definir prestarle

https://blog.smaldone.com.ar/2017/03/09/patricia-bullrich-y-el-ciberpatrullaje/

[46] "Se relanzó la Policía Federal con su nueva función de 'ciberpatrullaje'", Clarín, 18 de abril de 2017, disponible en: https://www.clarin.com/policiales/relanzo-policia-federal-nueva-funcion-ciberpatrullaje_0_B1KKunQ0x.html

[47] "Preocupa la negación de acreditaciones a organizaciones de la sociedad civil a la reunión de OMC en Buenos Aires", ADC, 1 de diciembre de 2017, disponible en: https://adcdigital.org.ar/2017/12/01/preocupa-la-negacion-acreditaciones-organizaciones-la-sociedad-civil-la-reunion-omc-buenos-aires/

[48] "Sobre la acreditación de ONG's a la Conferencia Ministerial de la OMC en Buenos Aires", Información para la Prensa N°: 558/17, Ministerio de Relaciones Exteriores y Culto, 2 de diciembre de 2017, disponible en: https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos

[49] Ver: "Argentina blocks some activists from attending WTO meeting", Reuters, 30 de noviembre de 2017, disponible en: https://www.reuters.com/article/us-argentina-wto-protest/argentina-blocks-some-activists-from-attending-wto-meeting-idUSKBN1DU39V

"Fury as Argentina blacklists WTO attendees over 'calls for violence'", The Guardian, 11 de diciembre de 2017, disponible en: https://www.theguardian.com/world/2017/dec/11/argentina-social-media-ban-world-trade-organisation-conference

"Argentina bans activists from WTO meeting", Financial Times, 30 de noviembre de 2017, disponible en: https://www.ft.com/content/9dc1a640-d5ff-11e7-8c9a-d9c0a5c8d5c9

atención a las redes sociales para la búsqueda de expresiones sobre la Conferencia? ¿Cuáles habían sido las tareas realizadas por el Estado argentino para encontrar las expresiones de violencia? ¿Qué tipo de expresiones consideraban capaces de generar "intimidación y caos" por redes sociales?

Con el objetivo de encontrar respuestas a estas y otras inquietudes, presentamos dos solicitudes de acceso a la información pública, ante el Ministerio de Seguridad y el Ministerio de Relaciones Exteriores.

Ambos ministerios negaron categóricamente cada una de las preguntas formuladas respecto a la investigación de antecedentes y su intervención en el proceso de acreditación de los participantes. Si bien Cancillería cursó una notificación a la Agencia Federal de Inteligencia (AFI) para que también se expida al respecto de la solicitud, al tiempo de cierre del presente informe no se había recibido respuesta alguna. Sin embargo, de la solicitud realizada por el Centro de Estudios Legales y Sociales (CELS) al momento de ocurrido el suceso, la AFI determinó que tampoco había participado en las tareas de acreditación de los participantes.[50]

Es evidente la clara elusión de los organismos estatales para establecer precisiones sobre lo ocurrido realmente respecto a las actividades de inteligencia llevadas a cabo para determinar que existieron expresiones de violencia en redes sociales publicadas por los miembros de las organizaciones desacreditadas. Tanto la Cancillería, el Ministerio de Seguridad y la Agencia Federal de Inteligencia brindaron respuestas evasivas que solamente permiten realizar conjeturas respecto a su proceder en el marco del desarrollo de la organización de la Conferencia, sin quedar precisamente dilucidado cuáles fueron las expresiones que causaron alarma en los organismos encargados de la seguridad del evento y qué criterios se siguieron para calificarlas en tal sentido, quiénes llevaron a cabo las investigaciones en las redes sociales y cuáles fueron las plataformas elegidas para enfocar la investigación.

2. Ministerio de Seguridad de la Nación y las fuerzas federales de seguridad

Con vista en los distintos sucesos que trascendieron en los últimos dos años, con el objetivo de arrojar luz sobre la manera en que el Ministerio de Seguridad y las fuerzas federales bajo su órbita ven y utilizan la investigación en fuentes abiertas y en redes sociales, presentamos una solicitud de acceso a la información pública a principios de julio de 2018 para profundizar lo que hasta el momento se conocía exclusivamente a través de los medios de comunicación.

La solicitud presentada se enfocó en dos grandes puntos. Por un lado, las causas judiciales iniciadas por expresiones investigadas en internet, con el objetivo de esclarecer: si se utilizan protocolos para llevar a cabo dichas tareas, cuántos casos se investigaron hasta el momento vinculados a expresiones

[50] EX -2018-9330179-APN-AAIP_Reclamo CELS C/Ministerio de Relaciones Exteriores y Culto y Agencia Federal de Inteligencia https://www.argentina.gob.ar/sites/default/files/rs-2018-20-apn-aaip.pdf

online, cuáles son los criterios seguidos para determinar la procedencia de las investigaciones, cómo es el proceso de recolección y análisis de la información, qué tipo de autorizaciones se solicitan para llevar a cabo las investigaciones en internet, qué tipo de capacitación recibe el personal que desarrolla las tareas de investigación, y cuáles son los métodos, técnicas y herramientas tecnológicas utilizadas para las investigaciones en el ámbito digital.

Por otra parte, para dilucidar a qué se refieren el Ministerio y las fuerzas federales al momento de hablar de "ciberpatrullaje", requerimos información sobre el concepto utilizado para definir dichas tareas y qué tipo de actividades incumben, cuáles son los protocolos de procedimiento aplicados y la capacitación recibida por el personal que lleva a cabo dichas tareas.

En principio, la primera respuesta del Ministerio brindada a comienzos de agosto de 2018 no abordaba las inquietudes requeridas en los 13 puntos de nuestra solicitud en forma comprensiva, por el contrario, el Ministerio acotó su respuesta únicamente a realizar una breve descripción genérica sobre las funciones de la "Dirección de Investigaciones del Ciberdelito", creada en marzo de 2018; una transcripción literal de la Resolución 234/2016, la cual contiene el Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos; y finalmente, una oración de cierre estableciendo que "en lo que refiere al uso de fuentes abiertas se aplican políticas de policiamiento en general y no en particular".

Ante la disconformidad de tan básica respuesta, procedimos a presentar un reclamo ante la Agencia de Acceso a la Información Pública (AAIP), quien a mediados de septiembre de 2018 emitió su resolución final. A partir del ingreso del reclamo, la AAIP solicitó al Ministerio que remita toda la documentación pertinente al requerimiento presentado por ADC, luego de lo cual el Ministerio envió a la Agencia tres notas ampliando la información provista originalmente, además de cursar intervención a la Policía Federal Argentina y la Policía de Seguridad Aeroportuaria.

En su nueva respuesta, el Ministerio establece que se encuentran trabajando en la implementación de indicadores que midan el desempeño de la Dirección de Investigaciones del Ciberdelito y les permita producir estadísticas, a la vez que confirman la puesta en marcha de políticas de policiamiento para detectar la realización de delitos en las redes sociales. Aún así, no les fue posible brindar un número estimado de la cantidad de casos investigados online desde la asunción de la ministra Bullrich, basando su justificación en la poca antigüedad de la Dirección.

Respecto a la realización de una distinción entre OSINT y SOCMINT como dos conceptos que deben ser abordados por separado, el Ministerio aclaró que no hace tareas de inteligencia. Sin embargo, en otro apartado de su respuesta, afirman que utilizan fuentes abiertas, entendido según el ministerio como aquello "accesible a cualquier ciudadano", para llevar a cabo sus investigaciones. Asimismo, si bien la Dirección establece no realizar tareas de informática forense bajo las cuales necesite aplicar el Protocolo General de Actuación, las fuerzas federales de seguridad se encuentran trabajando en la implementación del mismo para las actividades posteriores al "ciberpatrullaje", en lo que respecta

a la recolección de pruebas.

Ante la pregunta sobre la definición de "ciberpatrullaje", el Ministerio aclaró que la Dirección no tiene formulado un concepto, el cual aún se encuentra analizando técnica y jurídicamente. Sin embargo, la nota cursada por la División Delitos Tecnológicos de la Policía Federal sí determina que "ciberpatrullaje" se refiere a la "forma coloquial de referirse a la búsqueda de información en fuentes abiertas y públicas relacionadas con el ciberespacio".

Las actividades de "ciberpatrullaje" son llevadas a cabo en forma manual, con intervención humana y sin ningún tipo de software para automatizarlas, mediante consultas en motores de búsqueda y utilizando herramientas disponibles en forma gratuita en internet, aunque las mismas no fueron detalladas en las respuestas recibidas por la ADC.

La Dirección General de Investigación del Delito Complejo y la División Delitos Tecnológicos de la PFA, confirmaron que las investigaciones online, es decir las actividades de "ciberpatrullaje", son iniciadas exclusivamente luego de recibir un oficio judicial que solicite dichas actuaciones. La Dirección de Investigaciones del Ciberdelito del MinSeg posee "facultades investigativas establecidas en la Decisión Administrativa que dio su origen, pudiendo realizar presentaciones judiciales, como solicitar las diferentes medidas de prueba establecidas en los códigos procesales".

Finalmente, las capacitaciones recibidas por el personal de las fuerzas de seguridad abocadas a la investigación en el ámbito digital son impartidas por funcionarios y agentes de las mismas fuerzas, el Ministerio de Seguridad y organismos internacionales como Interpol. Tanto la PFA como el Ministerio no brindaron mayores detalles respecto al entrenamiento de sus empleados. En el caso del Ministerio aclarando incluso que la información sobre las capacitaciones y el material utilizado para las mismas es información reservada en los términos del artículo 8 de la Ley 27.275.

3. Policía de la Ciudad de Buenos Aires

La situación de la Policía de la Ciudad de Buenos Aires (ex Policía Metropolitana) no dista mucho de la realidad que enfrentan el Ministerio de Seguridad y las fuerzas federales. En una entrevista con ADC, una persona cercana a la Policía brindó precisiones sobre el actuar del organismo en la investigación del delito en el ámbito digital. Por motivos profesionales, la persona entrevistada solicitó mantener en reserva su identidad, motivo por el cual en los siguientes párrafos se la identifica como "I.R" (identidad reservada).[51]

Si bien dentro de la Policía de la Ciudad se utiliza bastante las técnicas de investigación en fuentes abiertas, su explotación aún no se encuentra completamente implementada. Esto se debe principalmente a una cuestión de capacitación y recursos. **I.R**: "La falta de explotación tiene que ver con

[51] Entrevista con ADC el 16 de julio de 2018 en la Ciudad Autónoma de Buenos Aires, Argentina.

falta de personal capacitado: *data science*, analistas y especialistas en bases de datos. Todo lo que es la inversión que requiere montar la infraestructura que te permite montar un buen análisis."

En la Policía no se realiza una distinción entre los conceptos de OSINT y SOCMINT. **I.R**: "se mantiene como un único concepto que es el análisis o investigación de información en fuentes abiertas de datos. Ese es el término que se ven en sumarios o en causas. Legal y técnicamente hablando es el término que utilizan para evitar poner palabras en inglés en un reporte judicial."

I.R: "Como fuente abierta se considera todo lo que sea público, pero que no haya sido obtenido a través de un mecanismo que haya violado la ley. Por ejemplo, hay una diferencia entre que yo pueda sacar un Facebook de alguien poniendo un teléfono, a que encuentre un *leak* de una base de datos porque *hackearon* LinkedIn, encuentro el usuario y contraseña del usuario de ese perfil, y lo uso para obtener información. Es una fuente abierta, sí, estaba ahí. Desde el punto de vista de dónde provino esa información, lo podrían llegar a cuestionar. Si el [abogado] defensor se aviva, puede viciar de nulidad todas las cuestiones."

Respecto al procedimiento en las causas judiciales, la investigación en fuentes abiertas es tomada como una más de las etapas de investigación.

I.R: "Caso 1: te llaman de un juzgado, te dicen tengo un oficio para que retiren. Vas al juzgado, tomas vista de la causa, te sentás con el secretario, juez o fiscal –dependiendo la confianza que tengas–, y te va a ir diciendo 'mirá, es una causa que estamos investigando por tráfico de drogas, está relacionado a tal cosa, tenemos tal información', a veces te dicen qué se puede hacer o a veces ya tienen idea de qué necesitan, 'necesitamos que ustedes agarren estos perfiles de Facebook, estas cuentas de correo y hagan un análisis de fuentes abiertas'. Para eso te dan un oficio. Con eso vos haces un sumario en la Policía y empezás a hacer todas las tareas asociadas a ese sumario. Distribuís las tareas en el equipo, haces los informes, se confecciona todo, y después vas al juzgado a darles todo lo que encontraste. Si es lo único que te piden hacer, entonces se cierra el sumario y se eleva la causa. Sino, se profundiza la investigación a partir de la primer exploración. Siempre se hace con el respaldo de un brazo de la justicia."

Una vez que se termina, se hace un reporte y el caso sigue. **I.R**: "Esto [el producto de la investigación] queda como parte del expediente judicial. Vos cerras la etapa de investigación, elevas el sumario y listo. Se fue esa información. Lo único que queda en la Policía es un detalle con el título del sumario X, causa X, X tiempo. No queda una copia, ya que la misma es elevada al juzgado, pero sí tienen una copia de la recepción del juzgado."

La otra faceta de la investigación en fuentes abiertas se da cuando la Policía toma un rol proactivo en la persecución del delito. **I.R**: "[En ese caso] partís de una serie de selectores[52] vinculados [por

[52] La Policía denomina "selectores" a la categoría o tipo de información que se está utilizando para la investigación. Por ejemplo: la dirección de email, el teléfono, el número del Documento Nacional de Identidad, el nombre y apellido.

ejemplo] con el robo de autopartes. Si encontrás algo, vas a un juzgado, y ahí la diferencia es que vos le llevas la causa. Si te dice que sí, arrancas con el oficio y empezás a investigar. Sino queda ahí."

En el caso de grandes eventos públicos, como fue el caso de la XI Reunión Ministerial de la OMC, los Juegos Olímpicos de la Juventud o, próximamente, el G20, la situación varía, pues, según indica **I.R**: "hay una serie de acciones que se realizan para determinar si se está gestando la planificación de actividades delictivas".

I.R: "Este proceso se automatiza. Agarrás unas herramientas, en general lo que haces es un *scraping* de distintos medios (social media, páginas web, blogs, foros, etc.) con una serie de palabras clave, partís de esa premisa. [Se] *escrapea* todo el contenido y después se pasa a una base de datos, la cual se pasa a un informe gráfico donde podes decir [por ejemplo] cuál fue el tipo de hashtag que más surgió. Cuando llegás a un punto en el que podes individualizar a un usuario, ahí se hace todo manual. Esto se hace por casos específicos (. . .) de eventos que comúnmente tienen antecedentes de haber tenido algún problema. Ahora, si es por casos de decir 'bueno busquemos pedófilos', eso no existe."

¿Qué ocurre en el caso de necesitar realizar el seguimiento de una persona o grupos específicos? **I.R**: "En ese caso se utiliza [la figura del] agente encubierto. [El mismo] se mete en una organización, los sumarios se manejan en forma separada y confidencial, en comunicación directa con el juez; están incluso autorizados a la comisión de delitos siempre que no ponga en riesgo su persona o cometa delitos mayores. [También existen las figuras del agente] provocador o revelador, que se pueden usar en el ámbito de internet, y tienen la posibilidad de entrar a un lugar y mirar en forma pasiva."

En estos casos, se procede de la siguiente manera. I.R: "Por ejemplo, [se puede] hacer que alguien lo siga para ver el contenido de su perfil de Twitter o Instagram, pero debe autorizado bajo esa figura [agente encubierto, revelador o provocador], sino no puede. Todos los detalles quedan en el expediente: se creó el perfil @X, con tal avatar, para tal fin y todo lo que se genera para ese perfil debe haber sido previamente autorizado para el agente revelador que tiene que estar identificado, por un período de tiempo específico, el cual generalmente se va renovando, y con una función determinada. Cuando se cumple ese objetivo la figura ya no sirve. Lógicamente la autorización la brinda el juez. La plataforma [red social, foro, etc.] nunca está en conocimiento, es el 'enemigo' principal, porque puede eliminar los perfiles."

La implementación de técnicas de OSINT y SOCMINT por la Policía aún es muy incipiente. **I.R**: "Por una cuestión metodológica, tiene que haber un protocolo que hay que seguir. Hoy no lo hay, no hay personal capacitado ni herramientas. Hoy la gran mayoría de las cosas que se hacen están basadas en el sentido común y en el uso de herramientas manuales y *open-source*, [es un trabajo] artesanal, buscando, copiando, viendo."

4. Una breve mirada a las estadísticas de las plataformas de internet

Una forma de medir la importancia que le dan los gobiernos a la información proveniente de las redes sociales es mirando los informes publicados por las mismas plataformas que proveen los servicios.

Hoy en día, la publicación de informes de transparencia se ha convertido en un estándar para las empresas de internet. Gracias a ellos podemos analizar la evolución de los requerimientos de información personal proveniente de organismos gubernamentales en diversos países alrededor del mundo.

Si observamos la información provista por Twitter, según surge de la tabla 1, resulta evidente el incremento en la cantidad de solicitudes realizadas desde organismos Estatales argentinos en el período entre enero 2016 y diciembre 2017, en comparación con los cuatro años anteriores. Aunque no en todos los casos la empresa entregó la información requerida, esto puede deberse a distintos motivos como ser que no se haya identificado el perfil concreto, que la solicitud sea excesivamente amplia, que el usuario haya reclamado la solicitud luego de ser notificado o que la empresa haya solicitado mayor información contextual al requirente y no obtuvo respuesta, entre otras situaciones.[53]

Período	Solicitudes de información de cuentas	Porcentaje de información producida	Cuentas especificadas
Julio - diciembre 2012	2	0 %	13
Enero - junio 2013	2	0 %	2
Julio - diciembre 2013	1	0 %	1
Enero - junio 2014	7	0 %	8
Julio - diciembre 2014	3	33 %	4
Enero - junio 2015	3	0 %	3
Julio - diciembre 2015	4	0 %	14
Enero - junio 2016	18	22 %	33
Julio - diciembre 2016	76	26 %	87
Enero - junio 2017	57	12 %	64
Julio - diciembre 2017	80	10 %	100

En igual sentido, los informes publicados por Facebook muestran la misma tendencia respecto al aumento en la cantidad de solicitudes de información personal realizadas a la plataforma por parte del Estado argentino. A diferencia de Twitter, Facebook mantiene un nivel mayor en la cantidad de información que produce y entrega respecto a cada solicitud.[54]

[53] Una explicación detallada sobre las solicitudes de información personal en Twitter puede consultarse en el siguiente link: https://transparency.twitter.com/en/information-requests.html

[54] Una explicación detallada sobre las solicitudes de información personal en Facebook puede consultarse en el siguiente link: https://transparency.facebook.com/government-data-requests/country/AR

Período	Solicitudes totales	Porcentaje de información producida
Enero - junio 2013	152	27 %
Julio - diciembre 2013	278	18,40 %
Enero - junio 2014	254	31,90 %
Julio - diciembre 2014	482	48,50 %
Enero - junio 2015	568	46,10 %
Julio - diciembre 2015	892	71,30 %
Enero - junio 2016	829	74 %
Julio - diciembre 2016	995	75 %
Enero - junio 2017	984	76 %
Julio - diciembre 2017	1290	80 %

IV. Recomendaciones

De acuerdo con todo lo expuesto a lo largo del informe, podemos empezar por concluir que el uso de técnicas de OSINT y SOCMINT por parte de los organismos estatales, particularmente para la investigación del delito, es una problemática que presenta diversas complejidades.

Es necesario que las mismas sean debatidas en profundidad y con anterioridad a cualquier política pública que pueda implementar el Estado respecto a su explotación, dando cuenta de las particularidades que presentan, principalmente, la protección de derechos fundamentales como la privacidad y la libertad de expresión, reunión y asociación, las consideraciones sobre la protección de los datos personales derivados de las actuaciones, e incluso el rol del sector privado, tanto como facilitador de la tecnología utilizada para llevar a cabo las tareas de investigación, como de la información almacenada de los usuarios de las plataformas en sí.

En tal sentido, establecemos las siguientes recomendaciones preliminares con el objetivo de propiciar la discusión, elaboración y perfeccionamiento de políticas públicas abocadas al uso de OSINT y SOCMINT, que sean respetuosas de un abordaje desde los derechos humanos.

1. Los datos recolectados por las entidades estatales deben ser necesarios y proporcionales acorde a un fin legítimo perseguido, y solamente cuando sea estrictamente necesario se almacenará

la información en bases de datos. Las personas deben saber que la policía, y otros organismos gubernamentales, recolectan información suya proveniente de fuentes abiertas y redes sociales –incluyendo todas las inferencias realizadas a partir de dichos datos–, para ejercer plenamente los derechos reconocidos por la Ley de Protección de Datos Personales (acceso, rectificación, supresión y actualización). Cualquier denegación debe encontrarse fundada de manera precisa.

2. Es necesario establecer protocolos específicos que brinden un marco comprensivo de las particularidades de esta problemática. El uso que hagan las fuerzas de seguridad y otros organismos estatales debe encontrarse claramente delimitado, ser transparente y abierto de cara a la población, facilitando así la evaluación sobre su necesidad y proporcionalidad. Los criterios de actuación no pueden quedar libremente supeditados a interpretaciones de funcionarios públicos o miembros de fuerzas de seguridad.

3. Dichos protocolos deben contener un marco de rendición de cuentas, que incluya la publicación regular de reportes con información estadística objetiva, detallando minimamente datos como: la cantidad de casos y personas investigadas, junto con la duración de dichas actividades; las redes sociales –y sitios web en general– que fueron vigiladas; las herramientas y las metodologías utilizadas para cada caso investigado. Asimismo, también se deben establecer consecuencias claras ante la violación de sus políticas, con el objetivo de reducir el potencial abuso de las prácticas de vigilancia.

4. Además, los protocolos deben tener lineamientos claros que permitan dilucidar cómo se procederá en la determinación de la confiabilidad, veracidad y calidad de la información que es recolectada, procesada y almacenada, por ejemplo, para responder a interrogantes sobre ¿Cómo se distinguen e identifican expresiones que pueden ser delictivas en apariencia, pero son en realidad simples bromas o parte del intercambio cultural y lenguaje que existe en internet?

5. Finalmente, el entrenamiento que reciban los funcionarios, personal o responsables que llevan a cabo la implementación de las técnicas de investigación y vigilancia debe contar con un abordaje de derechos humanos, particularmente en la privacidad y la libertad de expresión, junto con el marco jurídico de protección de los datos personales.


por los Derechos Civiles