Ciudad Autónoma de Buenos Aires, 21 de abril del 2020.

A la Señora Ministra de Seguridad de la Nación
Ministerio de Seguridad de la Nación
Gelly y Obes 2289, C.A.B.A.
S / D

De nuestra consideración:

En virtud del canal de dialogo que el Ministerio de Seguridad de la Nación ha abierto con la Sociedad Civil organizada, el Observatorio de Derecho Informático Argentino, con correo electrónico en odiaasoc@gmail.com, realiza sus observaciones al REGLAMENTO GENERAL PARA LA REALIZACIÓN DE TAREAS DE CIBERPATRULLAJE POR PARTE DE LOS CUERPOS POLICIALES Y FUERZAS FEDERALES DE SEGURIDAD BAJO LA JURSIDICCIÓN DE LAS AUTORIDADES RESPONSABLES PARA SU EJERCICIO.

1) Sobre el término "ciberpatrullaje"

Desde el Observatorio de Derecho Informático consideramos que el término para referirse al conjunto de acciones y características descriptas en los arts. 2, 3 y 4 del proyecto debe ser el de Inteligencia de fuentes abiertas, que es como ha sido caracterizado por la doctrina internacional. Esta actividad recibe el nombre de *Open Source Intelligence* ('Inteligencia de Fuentes Abierta') que es definida como "*la disciplina utilizada para la adquisición, tratamiento y posterior análisis de la información obtenida a partir de la exploración de fuentes de carácter público o de cualquier recurso accesible de forma pública*"[1].

Este tipo de actividad es caracterizada por la doctrina como un modelo de investigación proactivo. Según Manfredi: "*Este tipo de investigación proactiva requiere de operadores entrenados no sólo en la disciplina de OSINT sino que deben tener un vasto conocimiento de las garantías constitucionales, manejo de evidencia digital y, sobre todo, interpretar y hacer conocer con claridad las actividades de investigación que llevó a cabo. El investigador debe conocer efectivamente el límite entre lo público y lo privado; no sólo basta considerar en qué lugar del ciberespacio se encuentra esa información, sino también poder discernir si la misma fue obtenida, publicada o dejada disponible por medios lícitos*"[2].

[1] Manfredi, Mariano Damián (2018); "La evolución de la Investigación de los ciberdelitos" en "Cibercrimen II" dirección de Daniela Dupuy, p. 326/327.
[2] Ibídem, p. 332.

Asimismo, entendemos que el término "ciberpatrullaje" puede llevar a la falsa impresión de una equivalencia con el policía que "patrulla" las calles. Esto no es así, ya que las habilidades con las que las fuerzas de seguridad cuentan para "controlar" el ciberespacio son radicalmente diferentes. La posibilidad que brinda la inteligencia de fuentes abiertas para obtener información de cientos, miles y hasta millones de personas, en un momento determinado, es sumamente sorprendente y potencialmente peligrosa.

Así lo ha visto también el Relator Especial sobre la Promoción y Protección del derecho a la libertad de opinión y expresión de la ONU quien advirtió que "*Los costos y obstáculos logísticos de realizar una vigilancia a gran escala siguen disminuyendo rápidamente, al tiempo que proliferan las tecnologías que permiten una interceptación, vigilancia y análisis amplios de las comunicaciones*."[3]. Por esta razón, y como veremos más adelante, por los efectos que este tipo de vigilancia y/o actividades tendrían en las vidas de los ciudadanos, entendemos que es necesario modificar dicho termino.

2) Comentario acerca de la RESOL-2018-31-APN-SECSEG#MSG.

Resumimos las principales observaciones acerca de la normativa vigente:

a. Si bien no estipula de manera expresa un número cerrado de delitos, ni lo limita a delitos graves, el art. 1 circunscribe la acción a seis "tópicos", que comprenden una serie no determinada a priori de delitos, pero no deja abierta la utilización de la técnica para imputar cualquier delito.

b. El art. 2 se refiere a "medios probatorios reunidos", lo ciertos es que hoy no existe legislación específica a nivel Federal que regule la incorporación de la "prueba digital" -como medio de prueba- en un proceso penal, mucho menos, las técnicas de investigación involucradas en un "ciberpatrullaje". Este punto será desarrollado al comentar el proyecto.

c. La prohibición estipulada en el art. 3 es acertada, no se puede hacer acopio de la información recabada, en los términos descriptos.

No obstante lo anterior, no hemos podido hacer un análisis lo suficientemente profundo de dicha norma. A efectos de no atrasar la presentación de las observaciones al Protocolo realizaremos posteriormente una presentación dedicada solamente a la resolución RESOL-2018-31-APN-SECSEG#MSG.

3) Comentarios al proyecto de resolución

[3] A/HRC/23/40 "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue" en https://undocs.org/es/A/HRC/23/40

i. Afectación al principio de legalidad.

Una resolución ministerial no cumple con el principio de legalidad exigido por la Constitución Nacional y los Tratados de DDHH. La realización de las tareas descriptas por las fuerzas de seguridad debe esta reglada por ley de manera expresa.

Sin perjuicio de ello, cabe señalar que el art. 14 de la Convención de Budapest sobre Ciberdelitos – ratificada por ley 27.411- exhorta a los estados parte a adoptar: "…*las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos*".

Teniendo en consideración lo señalado y dado que la resolución tendría una duración acotada, circunscripta al período de cuarentena dispuesto por el DNU 260/2020, vemos positivamente que, al menos, se reglamente el accionar de las fuerzas de seguridad a través de los principios de actuación enumerados en el art. 6, junto con las prohibiciones del art. 8.

ii) ¿Herramienta de prevención y persecución del delito o técnica de control social?

Desde el Observatorio de Derecho Informático exhortamos a cumplir con las obligaciones asumidas al ratificar la Convención de Budapest.

Así como se modificó el Código Penal para receptar los nuevos tipos penales que comprenden la ciberdelincuencia, corresponde reformar las leyes orgánicas de las fuerzas de seguridad y el Código de Procedimiento Penal Federal para que se regulen las nuevas técnicas de investigación –como la aquí tratada- y consecuentemente, los nuevos medios de prueba relacionados con estas técnicas.

Para cumplir con los objetivos previstos en el art. 5 del proyecto (identificar posibles delitos, investigar posibles hechos delictivos para comunicar posteriormente a las autoridades judiciales) resultan necesarias las reformas referidas. La información recolectada a través de estas técnicas de investigación solo podrá ser considerada "prueba" en un juicio oral, si existe la regulación en el código de procedimientos. Ante tal vacío legal, la herramienta cumplirá un fin de control social pero no servirá para fundar una condena penal.

La fórmula constitucional del art. 18 "nadie puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso" constituye una formulación castellana del *nullum crime, nulla poena sine lege* que coloca en primera línea a la referencia procesal para fijar la extensión del principio.

Si de lo que se trata es de no ser penado sin juicio previo, entonces la "ley" a la que hace referencia la formulación constitucional es no sólo la ley penal material, sino también la ley procesal penal. Pues ella es la que regula el juicio, que ha de ser también previo a la pena.

El imputado, entonces, tendrá que ser condenado conforme a un procedimiento fundado en ley previa. Y respecto de esa ley rigen los mismos requisitos que, sin hesitación, se imponen a la ley penal material: lex escrita, lex stricta y lex certa. "*En consecuencia, toda actividad procesal destinada a destruir el estado de inocencia constitucional que protege al imputado deberá estar previamente regulada en ley, y de modo estricto, claro y taxativo, pues, en definitiva, de dicha actividad dependerá la eventual imposición de una pena. La aplicación analógica de la ley procesal con la finalidad de posibilitar la condena del imputado queda, pues, vedada"*.[4]

La regulación taxativa de los medios de prueba tradicionales en cualquier código de procedimientos es precisamente una exteriorización del respeto al principio de legalidad penal en materia procesal penal. Es por ello que constituye un grave problema la falta de regulación procesal sobre los "medios de prueba" digitales.

En este punto corresponde recordar las palabras del Dr. Pérez Barberá: "…*las investigaciones que actualmente se llevan a cabo en Argentina mediante rastrillajes informáticos, intervenciones de e-mails, seguimiento de direcciones IP, grabaciones o filmaciones a distancia, etc., resultan inconstitucionales (sin perjuicio de la salvedad que quepa realizar respecto de la ley de estupefacientes). Pues tales medios de prueba no han sido previstos en las leyes procesales, y en consecuencia su utilización para fortalecer la hipótesis acusatoria (es decir: para perjudicar procesalmente al imputado) constituye una aplicación de la ley procesal penal por analogía in malam partem y, por lo tanto, contraria al principio de legalidad penal, que rige con toda su amplitud tanto en el derecho penal material como en el derecho procesal penal*"[5]

La actual práctica por parte de algunos tribunales que aplican criterios analógicos con las tradicionales medidas de prueba no basta. No solo no resulta suficiente para cumplir con los estándares constitucionales por carecer de normas que permitan la correcta ponderación para la evaluación y procedencia de las medidas, sino que además la mayoría de los jueces no cuenta con el conocimiento técnico específico para guiar la aplicación de esos medios, tornando así

[4] Pérez Barberá, Gabriel (2009); "Nuevas tecnologías y libertad probatoria en el proceso penal", p. 277.
[5] Ibídem, p. 280.

muy peligrosa la medida tanto para los derechos del imputado como para terceros. Toda injerencia estatal que pueda afectar derechos constitucionales debe estar autorizada por una ley previa, clara y capaz de dar cuenta de las exigencias que deben ser acreditadas, controladas y satisfechas por una investigación que emplea sistemas informáticos de vigilancia para cumplir con los estándares constitucionales de un debido proceso legal.

iii) Principio de necesidad y proporcionalidad.

El principio de necesidad determina que cualquier restricción por parte del Estado en los derechos fundamentales de sus ciudadanos deba ser absolutamente necesario. De esta manera, debe analizarse si la restricción impuesta por la norma es totalmente indispensable, y a su vez, que no existe forma de sustituir dicha medida por una que tenga menos injerencia en los derechos fundamentales del ciudadano.

Este principio es particularmente importante para analizar lo establecido por el protocolo. Esto así porque dicho examen sobre la necesidad de la medida no parece estar del todo claro. Entendemos que, debido al aumento en la ocurrencia de ciberdelitos, puede ser necesario contar con las suficientes herramientas para hacer frente a los mismos. Sin embargo, no vemos que dicho posible aumento justifique una intervención tan agresiva sin venia jurisdiccional previa sobre otros derechos de raigambre constitucional como lo son el derecho a la privacidad y a la libertad de expresión.

La libertad de expresión es un derecho absolutamente central en cualquier sistema democrático. Esto así porque "*[…] se trata de uno de los derechos individuales que de manera más clara refleja la virtud que acompaña—y caracteriza—a los seres humanos: la virtud única y preciosa de pensar al mundo desde nuestra propia perspectiva y de comunicarnos con los otros para construir, a través de un proceso deliberativo, no sólo el modelo de vida que cada uno tiene derecho a adoptar, sino el modelo de sociedad en el cual queremos vivir. Todo el potencial creativo en el arte, en la ciencia, en la tecnología, en la política, en fin, toda nuestra capacidad creadora individual y colectiva, depende, fundamentalmente, de que se respete y promueva el derecho a la libertad de expresión en todas sus dimensiones. Se trata entonces de un derecho individual sin el cual se estaría negando la primera y más importante de nuestras libertades: el derecho a pensar por cuenta propia y a compartir con otros nuestro pensamiento.*"[6].

En este sentido, lo expresado a través de redes sociales merece una especial protección por parte del Estado ya que es un lugar donde la ciudadanía se expresa con total libertad y en el

[6] CIDH. Informe Anual 2009. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión).

marco de un contrato firmado con una empresa proveedora del servicio existiendo entre ambas una razonable expectativa de privacidad y donde lo publicado se encuentra adaptado a las políticas de uso y a las idiosincrasias propias de cada red social.

Esta especial protección se traduce en que el estado, cuando tenga que cumplir con sus obligaciones de brindar una adecuada protección para la seguridad interior (que desde ya reconocemos que existen), que la injerencia en este derecho en particular se limite a lo mínimo y necesario. Sin embargo, los vagos conceptos de "seguridad interior", "seguridad nacional", etc. no son un marco adecuado para justificar esta injerencia.

Asimismo, la literatura especializada es abundante en cuanto a los efectos que pueden tener los actos estatales en las redes sociales en la manera en la que se manifiestan los ciudadanos. Este efecto se conoce como "chilling effect" o efecto inhibitorio[7]. También es abundante la literatura en cuanto a que estos efectos inhibitorios no se limitan solamente a la manera en la que las personas se expresan en las redes sociales si no que estos efectos también se pueden ver fuera de las redes sociales[8].

El Relator Especial de Naciones Unidas para la Libertad de Expresión ha dicho: "*No obstante, en muchos casos los Estados restringen, controlan, manipulan y censuran contenidos difundidos por Internet, sin fundamento jurídico o amparándose en leyes amplias y ambiguas, sin justificar el objeto de esas acciones o de una manera claramente innecesaria o desproporcionada para el logro del objetivo previsto, como se examina en las secciones siguientes. Esas acciones son claramente incompatibles con las obligaciones contraídas por los Estados en virtud del derecho internacional de los derechos humanos y a menudo crean un "efecto inhibidor" más amplio del derecho a la libertad de opinión y de expresión.*"

Por el otro lado, el principio de proporcionalidad obliga al estado a realizar un examen sobre la limitación o restricción que se produce al o los derechos relevantes son una medida equilibrada y justa entre el beneficio al "bien común" que se obtiene de la limitación y el perjuicio que sufre el derecho afectado en cuestión.

En el caso de este protocolo, entendemos que el uso de las técnicas de OSINT en el marco de las redes sociales podría ser proporcional siempre y cuando dicho uso se encuentre enmarcado en una investigación penal determinada y dicha técnica haya sido debidamente

[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645 "Chilling Effects: Online Surveillance and Wikipedia use." https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case "Internet surveillance, regulation, and chilling effects online: a comparative case study."

[8] https://www.researchgate.net/publication/296637938_The_extended_'chilling'_effect_of_Facebook_The_cold_reality_of_ubiquitous_social_networking "The extended chilling effect of Facebook: The cold reality of ubiquitous social networking.

autorizada por un juez competente. Por el otro lado, entendemos que en lo que se refiere a actividades de "prevención" en las cuales dicha autorización judicial no exista, el uso de estas técnicas de investigación puede no cumplir con este requisito de proporcionalidad ya que no se encontrarían "justificadas".

Usar palabras claves para "investigar de manera preliminar" por fuera del marco de un expediente judicial no es un accionar respetuoso de los derechos humanos y no cumple con los requisitos de necesidad ni proporcionalidad.

iv) El uso de estas técnicas y tecnologías en el marco de la pandemia.

Recientemente la Comisión Interamericana de Derechos Humanos ha realizado determinadas advertencias relativas al uso de este tipo de herramientas.

Asimismo, la CIDH[9] dijo que los estados deben "*Asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales. Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones.*"

En este sentido entendemos como positivo que el protocolo en cuestión solo vaya a funcionar durante el tiempo que transcurra la pandemia, sin embargo, nos parece que se podrían seguir haciendo esfuerzos para intentar transparentar las herramientas de vigilancia que serán usadas (que plataformas serán objeto de investigación, que información se buscara, que delitos se pretenden investigar, etc). Así también, entendemos que seria bastante recomendable establecer un mecanismo de supervisión que sea independiente y que supervise y verifique el uso que se le dará a estas herramientas. Si bien entendemos que existe un mecanismo de supervisión, creemos que el organismo supervisor deberían encontrarse por fuera del organismo que realizara las actividades investigativas. Proponemos, en el caso que se pueda, que dicho organismo supervisor este compuesto por integrantes del poder legislativo y de la sociedad civil.

v) Observaciones sobre la Ley de Protección de Datos Personales.

Si bien el protocolo tiene previsto que en el marco de las actuaciones relativas al uso de estas técnicas se deberá siempre ajustarse a lo dispuesto por la ley 25326 de protección de datos

[9] Pandemia y Derechos Humanos en las Americas. Resolución 1/2020. 10 de abril del 2020. http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf

de personales, entendemos que es esencial que en dicho protocolo se establezca expresamente un procedimiento mediante el cual los ciudadanos puedan ejercer su derecho a la información, acceso, rectificación, actualización o supresión (Arts. 13, 14 y 16 de la ley 25326) siempre que dichos derechos no interfieran o obstaculicen actuaciones judiciales en curso.

Caso contrario, las dependencias encargadas de llevar a cabo estas actividades, deberán asegurarle a la ciudadanía que estas podrán acceder a cualquier información recolectada, almacenada y/o tratada por dichas dependencias.

Esta interpretación coincide con la realizada por la CIDH en el informe previamente mencionado. En dicho informe también se exhorta a los estados a "*32. Asegurar el derecho de acceso a la información pública en el marco de la emergencia generada por el COVID-19 y no establecer limitaciones generales basadas en razones de seguridad u orden público. Los órganos que garantizan este derecho y los sujetos obligados deben otorgar prioridad a las solicitudes de acceso a la información relacionadas con la emergencia de salud pública, así como informar proactivamente, en formatos abiertos y de manera accesible a todos los grupos en situación de vulnerabilidad, de forma desagregada sobre los impactos de la pandemia y los gastos de emergencia, desagregados de acuerdo con las mejores prácticas internacionales. En los casos de postergación de los plazos de solicitudes de información en asuntos no vinculados a la pandemia, los Estados deberán fundamentar la negativa, establecer un espacio temporal para cumplir la obligación y admitir la apelación de estas resoluciones*".

Esto así, para asegurarle a la ciudadanía la posibilidad de acceder a toda aquella información que se recolecte sobre sus personas y a que estas puedan disponer de ellos conforme lo dispone el principio de autodeterminación informativa.

vi) Conclusión

Desde el Observatorio de Derecho Informático Argentino entendemos que el protocolo de actuación en análisis es un primer borrador. Sin embargo, entendemos que es necesario modificar algunas disposiciones para que este protocolo sea lo más respetuoso posible en términos de los Derechos Humanos. Para ello hacemos las siguientes sugerencias:

1) Que el protocolo se limite al uso de la Inteligencia de Fuentes Abiertas para aquellas actividades enmarcadas en un procedimiento judicial determinado.
2) Que se realice una enumeración de las herramientas utilizadas y se detalle aquellas redes sociales que serán objeto de investigación.
3) Se establezca un organismo supervisor independiente en el cual participen representantes del Poder Legislativo junto a representantes de la Sociedad Civil organizada.

4) Se arbitren las medidas necesarias para publicar un informe que evalúe de manera pormenorizada la necesidad de que las correspondientes fuerzas de seguridad tengan que contar con estas nuevas aptitudes.
5) Se incluya un apartado que expresamente le permita a los ciudadanos acceder, conocer, rectificar, y/o eliminar la información que haya sido almacenada sobre ellos, conforme las disposiciones del marco protectorio de los datos personales de las personas.

Sin nada más que agregar, aprovechamos para saludar respetuosamente a la V.E.,

Observatorio de Derecho Informático Argentino.