

XIX Jornadas de
Comunicaciones
Científicas de la Facultad
de Derecho y Ciencias
Sociales y Políticas

UNNE

2023

En homenaje a la Dra. Hilda Zulema Zárate

Corrientes - Argentina

XIX Jornadas de Comunicaciones Científicas de la Facultad de Derecho y Ciencias Sociales y Políticas: UNNE / Silvia Alegre... [et al.]; compilación de Martín Chalup; Lucía Sbardella; dirigido por Mario R. Villegas. - 1a ed. compendiada. - Corrientes:

Universidad Nacional del Nordeste. Facultad de Derecho y Ciencias Sociales y Políticas, 2023.

Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-987-3619-94-6

1. Derecho. I. Alegre, Silvia. II. Chalup, Martín, comp. III. Sbardella, Lucía, comp. IV. Villegas, Mario R., dir.
CDD 340.072

CIBERPATRULLAJE. LA VIGILANCIA DE LAS REDES SOCIALES FRENTE AL DERECHO A LA INTIMIDAD COMO DD. HH

Fava Elgul, Pía A.

elgul68@gmail.com

RESUMEN

La investigación propuesta tuvo como objetivo analizar hasta qué punto las fuerzas de seguridad pueden inmiscuirse en nuestras redes sociales con el fin de resguardar la seguridad y la lucha contra el terrorismo. Se cuestionó si no es irrazonable el hecho de que la vigilancia indiscriminada que se ejerce, simplemente, nos califica a todos en presuntos culpables y a nuestras actividades en sospechosas, y todo ello sin la existencia de pruebas concretas de que la vigilancia masiva sea realmente efectiva.

PALABRAS CLAVES

Vigilancia, Gubernamental, Monitoreo.

INTRODUCCIÓN

En los derechos humanos observamos que con frecuencia se produce un menoscabo del derecho en cuestión que muchas veces es vulnerado directamente o no realizado en la medida en que la Constitución Nacional Argentina, el propio ordenamiento jurídico, o demás normativas nacionales vigentes disponen. Es por ello, que el principal aporte de este trabajo fue demostrar las recurrentes amenazas directas e indirectas hacia nuestros derechos humanos, pertenecientes por nuestra sola condición de persona.

Es por ello, que estas prácticas de monitoreo, observación y análisis de información de la actividad de los ciudadanos en las redes sociales para detectar actividades que eventualmente pueden resultar criminales, implican un gran riesgo para nuestros derechos.

Otro inconveniente radica en que, cuando un derecho fundamental en su ejercicio colisiona con otro derecho del cual es titular otro sujeto, como ser el derecho a la intimidad, a la privacidad, a la propia imagen y el derecho a la seguridad pública es

difícil hacer prevalecer el uno sobre el otro.

Es por ello que cabe plantearnos ciertas cuestiones tales como ser:

¿El monitoreo masivo de publicaciones en redes sociales logra disminuir actividades criminales e individualizar a presuntos sospechosos? En el caso de ser así, ¿No se conculcan derechos humanos fundamentales?

MÉTODOS

En una primera etapa se realizó un relevamiento de información, a fin de determinar con mayor precisión a qué datos las fuerzas de seguridad pueden acceder y bajo qué argumento legal. Ello permitió dilucidar si efectivamente las fuerzas de seguridad y las fuerzas policiales tienen un poder tan amplio respecto a nuestros datos con el fin de cumplir su cometido y cuánta privacidad está dispuesta a sacrificar la sociedad civil.

Para el efectivo cumplimiento de los objetivos propuestos en el presente plan de trabajo se realizó una recopilación de material a través de fuentes de datos tales como revistas,

artículos periodísticos, libros y documentos jurídicos, entre otros, brindados mediante páginas oficiales, diarios internacionales, plataformas digitales de acceso a jurisprudencia y material doctrinario, etc. para realizar un posterior relevamiento de información. Como así también, se elaboró un análisis de la normativa vigente referida al objeto de estudio.

RESULTADOS Y DISCUSIÓN

El término “ciberpatrullaje” el cual es definido como una modalidad de ciberseguridad, que puede pensarse en un sentido análogo al patrullaje físico que, a través del monitoreo con el cruce de palabras clave, permite identificar la posible comisión de delitos. Actualmente, estos métodos están destinados a analizar las diversas publicaciones de los usuarios a través de sus redes sociales sin especificar, en primera instancia, qué se busca o quién está siendo observado.

En nuestro país, se considera expresamente prohibido utilizar los datos para algo diferente al propósito para el que fueron recolectados. Es por ello que surge la “Ley de Protección de Datos Personales” (Ley 25.326), reglamentación que regula los datos asentados en archivos, registros y bases de datos para garantizar el derecho al honor y a la intimidad de las personas.

En estos casos la problemática radica en la protección acentuada que la Constitución Nacional y las leyes que regulan la materia le dan a ese tipo de datos y no en la naturaleza misma de la práctica. Ante lo expuesto, el artículo 5 de la Ley 25.520 de Inteligencia Nacional establece que en el caso de que los funcionarios públicos encargados de realizar las actividades de inteligencia infrinjan deberes y obligaciones de sus funciones o no sean informados, incurrirán en responsabilidad disciplinaria. En el caso concreto, no podrán incurrir a la obediencia debida como eximente de responsabilidad.

El Ministerio de Seguridad ha citado con frecuencia el argumento de que las personas colocan la información en el espacio público, sin embargo, el mismo ignora las recomendaciones del Alto Comisionado de las Naciones Unidas para los Derechos Humanos del año 2018. En un informe específico sobre el derecho a la privacidad en la era digital, se determinó que no se cumplían los estándares de Derechos Humanos que deben tenerse en cuenta al regular los derechos en línea. En ese sentido, explica que la injerencia de los Estados en el derecho a la intimidad de las personas “sólo puede hacerse en la medida prevista por la ley, y en la legislación pertinente se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias” (Informe 2018, A/HRC/39/29, pár. 10). Dicho de otro modo, cualquier violación del derecho a la privacidad de una persona debe cumplir con un estándar de legalidad formal, que establece que la vulneración debe ser legal, necesaria y proporcionada. Dado el contexto de la situación de emergencia sanitaria global debido al COVID 19 el Ministerio de Seguridad de la Nación creó, en 2020, un “Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas” oficializado mediante la resolución 144/2020, que establece los mecanismos que las fuerzas de seguridad federales podrán emplear para detectar delitos en Internet.

El Ministerio de Seguridad aclaró que el objetivo del “ciberpatrullaje” es prevenir y sancionar aquellas posibles conductas delictivas cuyo caso sea previsible en función de la emergencia sanitaria establecida mediante el aislamiento social. Sin embargo, no se establecen motivos específicos y detallados de por qué realmente esta actividad es una herramienta particular para usar en situaciones de emergencia. Tampoco resulta el protocolo apropiado si el objetivo es mejorar las capacidades de inteligencia criminal para la

detección de fenómenos particulares.

De lo expuesto, surge evidente que, en la actualidad, nos enfrentamos a un nivel de invasión estatal que no respeta los estándares internacionales en materia de privacidad, en la medida en que toda la información que las personas publican en las plataformas de redes sociales puede ser objeto de vigilancia por parte de las fuerzas de seguridad vulnerando así, dos derechos que están estrechamente conectados: la privacidad y la libertad de expresión de las personas.

Conclusiones:

Por todo lo investigado podemos concluir:

1) La hipótesis de la presente investigación confirma que el ciberpatrullaje no posee un efecto positivo, no ha logrado disminuir y/o evitar la posible comisión de delitos que pongan en riesgo la seguridad nacional.

2) Conforme al análisis investigativo efectuado, se ha demostrado que en los casos en que se ha utilizado el Protocolo se evidenció la no comisión de los delitos por el cual ha sido dictado y, por el contrario, se han vulnerados los derechos fundamentales de las personas que han sido denunciadas y /u objeto de investigación por la posible comisión de un delito.

REFERENCIAS BIBLIOGRÁFICAS

- Serra, R. (2015). La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional. *Revista de Derecho Político*, 92.
- Castells, M. (2000). *La era de la información: economía, sociedad y cultura. Volumen I. La Sociedad Red*. Ed. Alianza Editoriales.
- Bidart Campos, German J. y otros. (1999). *El Amparo Constitucional*. Ed. Depalma.

Nino, C. (1992). *Fundamentos de derecho constitucional*. Ed. Astrea.

Sagüés, N. (1991). El amparo informativo. LL 1991-D, p. 1.034.

Badeni, G. (2011). *Manual de Derecho Constitucional*. Ed. La Ley.

Migliorisi, D. (2015). *Crímenes en la Web, los delitos del Siglo XXI*. Ed. Del Nuevo Extremo.

Poveda Criado, M. A. (2015). *Delitos en la red: cibercrimen, ciberdelitos, ciberseguridad, ciberespionaje y ciberterrorismo*. Ed. Madrid Fragua.

Daniela Dupuy, M. K. (2016). *Cibercrimen: aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet*. Ed. B de f.

EJE TEMÁTICO DE LA COMUNICACIÓN
Derecho y Nuevas Tecnologías

FILIACIÓN

AUTOR 1: Becario De Investigación De Grado - PI 20G001 SGCyT-UNNE - SGCYY - UNNE