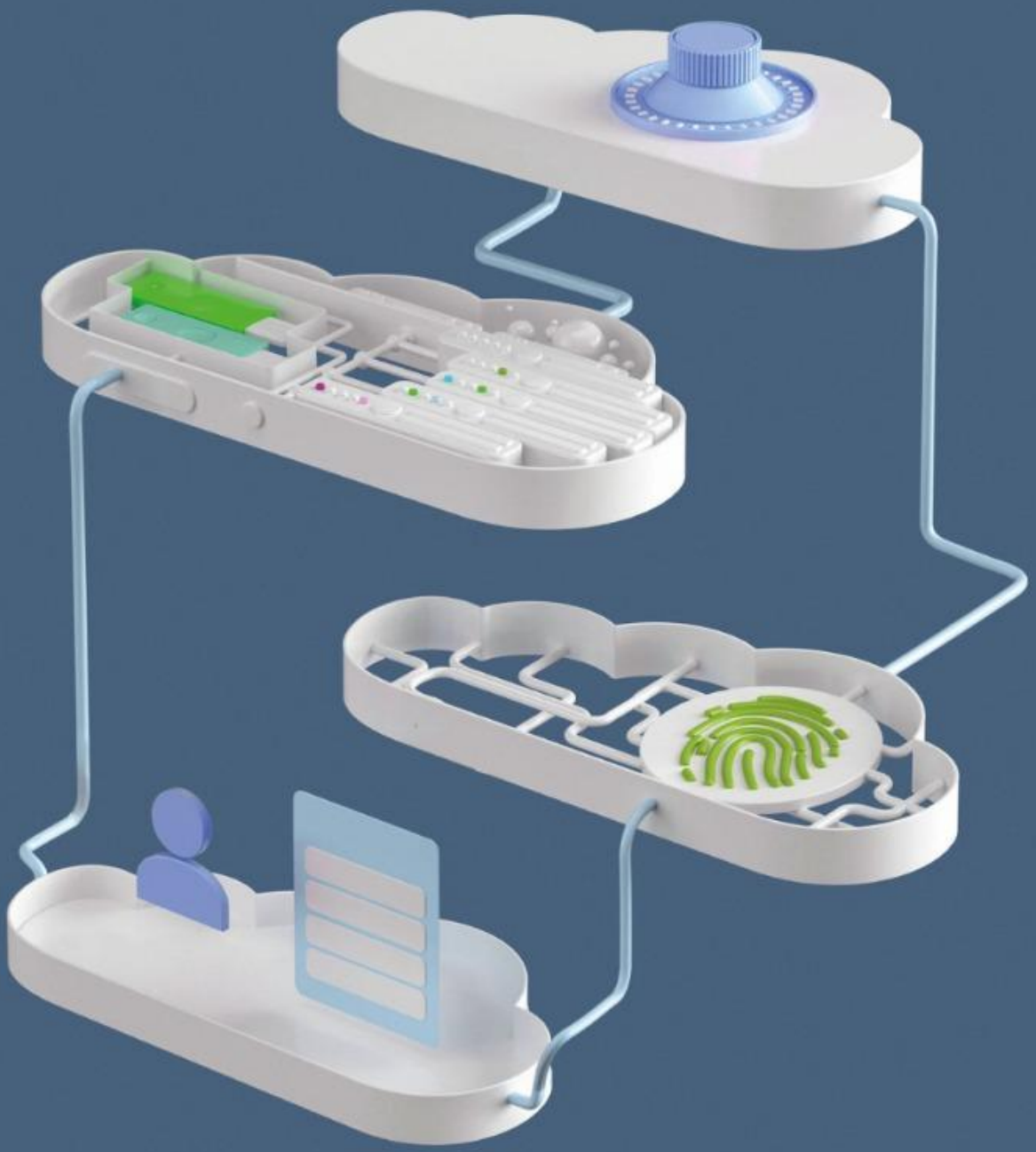
INTELIGENCIA ESTRATÉGICA EN REDES SOCIALES

UNIVERSIDAD NACIONAL DE LA PLATA

LA APLICACIÓN DE LA LEY NACIONAL DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA



TESIS

AUTOR
LIC. FRANCISCO RODRÍGUEZ

DIRECTOR
DR. JORGE SZEINFELD

MAESTRÍA EN INTELIGENCIA ESTRATÉGICA NACIONAL
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD NACIONAL DE LA PLATA

A mi papá, Eduardo Rodríguez.

Lo mejor que me pasó en la vida.

Resumen

El presente trabajo trata sobre el uso de redes sociales para la producción de inteligencia estratégica y su relación con las regulaciones sobre protección de datos personales. A través del análisis de las tendencias en la región y el mundo, la investigación se centra sobre los aspectos más relevantes en el desarrollo de regulaciones a nivel nacional en Argentina.

Abstract

This work deals with the use of social networks for the production of strategic intelligence and its relationship with regulations on the protection of personal data. Through the analysis of trends in the region and the world, the research focuses on the most relevant aspects in the development of regulations at the national level in Argentina.

ÍNDICE

Introducción

Desde hace más de una década, el avance del uso de la Inteligencia en Redes Sociales para la producción de conocimiento configura un nuevo fenómeno de creciente importancia en el escenario global de la inteligencia, tanto en organizaciones públicas como privadas. Dicho de otra manera: la inteligencia en redes sociales se perfila como una de las principales fuentes de producción de conocimiento de la mano de la expansión de internet y de la TICs (Tecnologías de Información y la comunicación) en la sociedad.

Sin embargo, aún no es claro el verdadero alcance de este campo o disciplina y su capacidad de ser científicamente verificable y sólida para lidiar con las características de gran volumen y baja calidad de datos, (también conocidas como "las cuatro V", que caracterizan a los datos en internet, gran: Velocidad, Volumen, Variedad y baja Veracidad). Por otro lado, existe preocupación sobre hasta qué punto estas prácticas no estarían vulnerando el derecho a la protección de los datos personales y el derecho a la privacidad de las personas.

Sobre estas tensiones versa esta tesis que busca presentar los principales debates y hallazgos en materia de inteligencia estratégica y redes sociales y, en particular, en relación a su regulación en Argentina.

Propósito

De acuerdo a lo desarrollado, pensamos que este trabajo puede resultar en un aporte valioso al campo académico ya que, si bien existen trabajos que abordan, por un lado, la legislación sobre protección de datos personales y, por otro la utilización de las redes sociales para la producción de conocimiento, no existen investigaciones que vinculen la efectividad de la aplicación de ésta ley en ésta práctica en especial.

En términos generales, identificar la interrelación entre la Ley Nacional de Datos Personales Nº 25.326 y el proceso de producción de Inteligencia mediante redes sociales, nos permitirá identificar las incidencias de la legislación vigente en esta práctica puntual.

En este sentido, buscaremos también: a) caracterizar las organizaciones que participan en el desarrollo de la actividad, b) definir los parámetros aceptados por la ley, así como los parámetros políticos bajos los cuales se sustentan los programas en cada organización, y c) identificar el nivel de valoración de la actividad para los objetivos de la organización.

Finalmente se intentará caracterizar las variables legales e institucionales que regulan la actividad, y contextualizar y valorar el aporte que puedan hacer los actores entrevistados al conocimiento del fenómeno.

Datos personales y datos sensibles

En el contexto de las redes sociales predominan los datos conocidos como “datos sensibles”, definidos como aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de sus datos[1].

En el ámbito normativo, nuestra Constitución Nacional, a través del artículo N°43[2], incorpora el instituto de *Habeas Data* del Pacto de San José de Costa Rica. La norma se aplica a todas las personas físicas y jurídicas con domicilio en el país y está destinada a regular la protección integral de los datos personales asentados en bases o registros públicos y privados para garantizar el derecho al honor y a la

[1] Definición de Datos Sensibles, Artículo 2, Ley N 25326, Ley Nacional de Protección de Datos Personales, República Argentina, 2000.
[2] Artículo N 43, Primera Parte, Capítulo Segundo, Nuevos Derechos y Garantías, Constitución de la Nación Argentina, 1994.

intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

En esta misma línea, en el año 2000 fue sancionada la Ley Nacional de Protección de los Datos Personales N°25.326 que norma sobre los derechos de los titulares de los datos personales. Esta ley define los roles de usuarios y responsables de bases de datos, determina un control, sanciones y acciones en relación a la protección de los datos personales. El objeto de la ley trata sobre: "...*la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".* La ley aclara: *"Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas*[3]".

Redes Sociales e Inteligencia

Dentro del campo de las llamadas "fuentes abiertas", son las redes sociales en internet las que, potencialmente, más atributos sobre datos personales podrían abarcar. Es por esto que el tratamiento de los datos sobre esta fuente implica grandes desafíos tanto para las organizaciones que hagan uso de ellos como para quienes los regulan y supervisan su cumplimiento.

El principal autor que aborda el tema del uso de inteligencia en redes sociales es David Omand[4], quien fue director del The Government Communications

[3] Ley Nacional de Protección de Datos Personales Nº25326, INFOLEG, Ministerio de Justicia y Derechos Humanos de la Nación, 2000.
http://servicios.infoleg.gob.ar/infoleginternet/anexos/60000-64999/64790/norma.htm

[4] David Omand, Ex Director del Government Communications Headquarters (GCHQ), organismo responsable de la recolección de inteligencia de señales (SIGINT) en Reino Unido, entre 1996 y 1997. Entrevistado el 17 de abril de 2020.

Headquarters (GCHQ), una organización de inteligencia y seguridad encargada de proporcionar inteligencia de señales (SIGINT) y garantizar información al gobierno y las fuerzas armadas de Reino Unido. Junto con los autores Jamie Bartlett y Carl Miller, propusieron a las Redes Sociales como una nueva “INT” (abreviatura de *intelligence*, en español *inteligencia*), fuente para el análisis de datos y producción de inteligencia.

Omand tiene una extensísima experiencia en Defensa e Inteligencia. Anteriormente se desempeñó como el primer Coordinador de Seguridad e Inteligencia del Reino Unido, responsable ante el Primer Ministro por la salud profesional de la comunidad de inteligencia, la estrategia nacional de lucha contra el terrorismo y la seguridad nacional. Durante siete años fue responsable del Comité Conjunto de Inteligencia y fue Secretario Permanente del Ministerio del Interior entre el año 1997 y el 2000. Durante la guerra de Malvinas ocupó el cargo de Secretario Privado Principal del Ministro de Defensa de Reino Unido.

Ámbitos de aplicación

Es de público conocimiento que algunas organizaciones estatales como las fuerzas de seguridad tienen equipos de trabajo que utilizan las redes sociales para conocer información sobre personas involucradas en un delito, con el fin de ubicar un prófugo de la justicia, conocer el alcance o las vinculaciones de una organización de tráfico de drogas u otro tipo de organización del crimen organizado. Este puede ser un uso típico de la producción de inteligencia criminal.

En diferentes sectores del ámbito público también existe la producción de inteligencia en redes sociales para conocer y proteger determinados recursos estratégicos de nuestro país, como puede ser a modo de ejemplo el litio. No es en este caso un tema de seguridad interior o defensa a priori, pero sí es un recurso natural que nuestro Estado busca proteger y tener conocimiento sobre aquellas amenazas potenciales que puedan afectar, o bien sobre qué oportunidades

podemos aprovechar teniendo un mejor conocimiento de la actividad y los actores de interés involucrados en esa área.

En el sector privado, múltiples empresas producen información en base a redes sociales para la toma de decisiones empresarias y de negocio. Algunas empresas se dedican exclusivamente a esta tarea con el fin de conocer a la competencia, a los clientes, a los proveedores, entre otros actores, conocer qué consumen los clientes propios, los de la competencia, etc. Esta clase de información muchas veces determinará decisiones para el futuro del negocio.

Más específicamente, como mencionamos anteriormente, debemos tener presente a David Omand como una figura central en el desarrollo del debate sobre redes sociales e inteligencia. Se trata del autor que plantea un debate acerca de producir conocimiento con las redes sociales como fuente. Se basa en hechos vinculados al terrorismo donde las redes sociales fueron una herramienta útil para identificar a los victimarios y también plantea otros interrogantes. Con un enfoque sobre el medio estatal, aborda cómo un organismo del Estado, debe tener apoyo de la comunidad para desarrollar este campo sin vulnerar derechos ni perder efectividad en la práctica.

Otro de los referentes es Mark Lowenthal quien es un autor destacado que escribió textos académicos sobre inteligencia y su relación con la política (con los decisores políticos) que son, a fin de cuenta, quienes consumen el producto de inteligencia en representación de la ciudadanía. En "*Intelligence. From secrets to policy*" (2015) describe múltiples elementos, organizaciones, prácticas y también le dedica un espacio a las redes sociales e internet. En principio él plantea que los análisis son "multifuentes" y que la complementariedad de ellas es lo que da un resultado diferencial. También le dedica un capítulo al aspecto ético de la actividad.

Otros actores que hacen aportes importantes en el debate son las ONGs que bregan por el acceso a la información, la privacidad y la protección de datos personales, tres temáticas que van juntas y que comparten el mismo espíritu, la protección de los derechos humanos. También organismos de protección de

derechos se manifiestan contra los llamados “apagones de internet” por parte de gobiernos autoritarios.

Un caso actual denunció Lawrence Mute, Relator Especial sobre Libertad de Expresión y Acceso a la Información en África, quien reclamó que se termine el bloqueo de internet por parte de los gobiernos de Etiopía y Guinea, en medio de la Pandemia COVID-19. Este hecho ha perjudicado a la población que no puede comunicarse e informarse sobre medidas de protección a la salud.

Tampoco podemos pasar por alto la influencia de las corporaciones privadas a las que pertenecen las redes sociales y sus políticas de protección de datos personales, sus contratos de términos y condiciones con los usuarios y su relación con empresas y estados, las implicancias jurisdiccionales de la justicia y los caminos extrajudiciales para efectuar reclamos.

Libertad de expresión, acceso a la información pública y la protección de datos personales

Como afirmamos, la libertad de expresión, el acceso a la información pública y la protección de datos personales, conforman un tridente de derechos emparentados que se complementan y se potencian uno con el otro. El primer derecho, la libertad de expresión, es un principio que apoya la libertad de un individuo o una comunidad para articular sus opiniones e ideas sin temor a represalias, censura o sanción.

La libertad de expresión es considerada un derecho humano en virtud del artículo 19 de la Declaración Universal de los Derechos Humanos (DUDH) y se reconoce en el derecho internacional también a través del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). El artículo 19 de la DUDH establece que "todos tendrán derecho a opinar sin interferencia" y "todos tendrán derecho a la libertad de expresión, este derecho incluirá la libertad de buscar, recibir y difundir información e

ideas de todo tipo, independientemente de fronteras, ya sea oralmente, por escrito o impreso, en forma de arte, o por cualquier otro medio de su elección ".

La versión del Artículo 19 en el PIDCP lo enmienda más adelante al afirmar que el ejercicio de estos derechos conlleva "deberes y responsabilidades especiales" y "por lo tanto, estar sujeto a ciertas restricciones" cuando sea necesario "para respetar los derechos o la reputación de otros" o "para la protección de la seguridad nacional o del orden público, o de la salud o la moral pública".

En el caso del derecho de acceso a la información pública, se encuentra amparado por el principio de "publicidad y transparencia en la gestión de gobierno", el cual cuenta con jerarquía constitucional y a su vez se suscribe a través del compromiso internacional asumido por nuestro Estado al adherir a numerosos tratados internacionales tales como la Convención Americana sobre Derechos Humanos, la Declaración de la Organización de los Estados Americanos para la Libertad de Expresión y la Convención Interamericana contra la Corrupción, entre otros.

En nuestro país, desde septiembre de 2016 se encuentra aprobada la ley 27.275 de Acceso a la Información Pública. Dicha ley, además de crear la Agencia de Acceso a la Información pública, obliga a los tres poderes del Estado, al Ministerio Público, a empresas, partidos políticos, universidades y gremios que reciban aportes públicos, a responder las solicitudes de información que eleve cualquier ciudadano en un plazo no mayor a un mes.

El Derecho de Protección de Datos Personales en nuestro país se encuentra regulado a través de la Ley Nacional 25.326 del año 2000. Dentro de su articulado se detallan los derechos de los que gozan los dueños de los datos personales, además de definir y clasificar los diferentes tipos de datos personales. Se describen también derechos y obligaciones de los administradores de archivos o bases que contengan datos personales.

La redacción, tratamiento y aprobación de la normativa en ambas cámaras significó en su momento una verdadera actualización de los derechos en la materia dándole

un respaldo interesante al funcionamiento institucional y administrativo del órgano de control.

Aspectos metodológicos

Desde el punto de vista metodológico, por ser una tesis exploratoria, esta investigación se basa en la recolección de información a partir de diversas fuentes. En primer lugar, las fuentes primarias están conformadas por el análisis de la legislación vigente a nivel nacional e internacional en materia de Protección de Datos Personales, Derechos Humanos, Inteligencia, Seguridad Interior y Defensa Nacional, así como también diferentes documentos, investigaciones y papers universitarios que indagan el rol de las redes sociales en internet.
En segundo lugar, como fuentes secundarias, se consultará bibliografía de autores especializados tanto sobre Protección de Datos Personales como sobre la producción de Inteligencia. Y a través de entrevistas a personas que cumplen un rol dentro de la actividad de producción de conocimiento utilizando redes sociales como fuente. Estas entrevistas buscarán determinar el grado de conocimiento de la ley entre los actores del sector y su visión sobre ésta en términos de factibilidad y eficacia en su implementación.

Este trabajo recorrerá experiencias en el sector público y privado sobre la ley nacional de protección de datos personales y sobre el modo de tratamiento de los datos. Intentaremos entender si la legislación vigente se adapta al contexto actual en la materia.

CAPÍTULO 1

CONCEPTOS BÁSICOS DE LA INVESTIGACIÓN

En el presente capítulo se presentarán algunos conceptos básicos para abordar la temática desde un entendimiento común y conceptual que nos permita lograr una comprensión más objetiva y horizontal de los temas.

Estas definiciones nos permiten unificar el criterio sobre cada temática o fenómeno, para no dar por hecho interpretaciones o referencias hacia otros conceptos que puedan guardar similitudes o prestarse a confusión.

Algunos conceptos, por ser relativamente nuevos en el vocabulario interesado, todavía no gozan de reconocimiento en el público en general, otros pueden tener un significado ambiguo o poco claro. Es interés de este trabajo dirigirse no sólo a la comunidad académica de pertenencia a esta temática, sino también a toda la sociedad, partícipe de múltiples campos y de diversas especialidades.

Inteligencia

Un primer concepto que abordaremos es el de *Inteligencia*. Cuando nos referimos a Inteligencia en este trabajo, estamos hablando sobre el proceso de producción de conocimiento para la toma de decisiones, indistintamente del campo profesional en donde se aplique.

Vulgarmente, en algunos sectores de la sociedad, o en el lenguaje coloquial también, se considera a la Inteligencia como sinónimo de espionaje, y mayoritariamente al espionaje practicado de forma clandestina. Esa no es la significación que le daremos en este trabajo al término Inteligencia.

Académicamente, la Inteligencia consta de un ciclo, conformado por un conjunto de etapas, que como un proceso, van conduciendo y ordenando el trabajo o esfuerzo de inteligencia que, como dijimos, tiene siempre el fin de ser un producto para la toma de decisiones de uno o un grupo de decisores.

Si bien la inteligencia, según la definición académica, refiere a la “recolección de datos” en una de las etapas del ciclo, esta recolección no tiene que ser, (ni por definición ni por objeto) clandestina o secreta, aunque muy frecuentemente, numerosas actividades de inteligencia se realizan de manera secreta. Consideramos que dependerá, en última instancia, de la naturaleza de la organización que lleve a cabo la tarea y las características del contexto en el que se aplica.

Es entendible que si, por ejemplo, las Fuerzas Armadas, la Agencia Federal de Inteligencia, el Poder Judicial o la Unidad de Información Financiera, realizan inteligencia, posiblemente manejen requerimientos de secreto más altos que otras organizaciones que no están vinculadas a la seguridad pública o la defensa nacional. Pero esta protección del secreto se explica debido a su naturaleza y cultura organizacional más que a la tarea de inteligencia en sí.

Por esto, invitamos al lector de este trabajo a entender el concepto de inteligencia sin el sesgo de la clandestinidad, sino como un conjunto de pasos que llevan a datos aislados a convertirse en información y finalmente en conocimiento útil para la toma de decisiones.

Tal como expresa Sherman Kent: *“Aunque existe en ella una buena dosis de comprensible misterio, la inteligencia es una cosa simple y que se evidencia por sí misma. Como actividad, es la prosecución de cierta clase de conocimiento; como fenómeno, es el conocimiento resultante. En reducida escala, es lo que todos nosotros hacemos cada día. Cuando una ama de casa decide estirar su presupuesto, cuando un médico diagnostica una dolencia, cuando cualquier persona toma una decisión con respecto a un problema, por lo general efectúa un trabajo preliminar de inteligencia. A veces el trabajo es tan simple e instintivo, que esa persona no lo reconoce como inteligencia, tal como encontrar el mecánico indicado en la sección clasificada de una guía telefónica. A veces es formal, arduo y sistemático, como el brillante análisis de Arthur Koehler sobre la escalera, en el caso de Lindbergh. Pero, ya sea efectuado instintivamente o mediante un esfuerzo*

mental, consciente y hábil, el trabajo de inteligencia no es, en esencia, más que la búsqueda de una respuesta mejor y más sencilla[5].

Inteligencia Estratégica

La palabra estrategia deriva del latín strategĭa, que a su vez procede de dos términos griegos: stratos “ejército” y agein “conductor” o “guía”. Por lo tanto, el significado primario de la palabra estrategia podría interpretarse como “el arte de dirigir las operaciones militares”. Si bien su origen viene del área militar, su significado es aplicado a diversas especialidades y actividades.

Cuando hablamos de estrategia, nos estamos refiriendo a la evaluación y aplicación de un plan de acciones vinculado a determinados actores, en un contexto determinado con el fin de conseguir determinados objetivos estratégicos. Lo estratégico evoluciona siempre en un ambiente complejo, donde existe una tensión entre los diferentes actores que buscan subsistir manteniendo el mayor nivel de libertad de acción posible.

El Mg. Roberto Alemanno (2018), especialista en Inteligencia Estratégica, considera que la estrategia es una dialéctica de voluntades en procura de lograr maximizar los beneficios, que se concreta mediante el intercambio de intereses. Este intercambio constituye un trueque virtual, se plantea la oferta esperando la aceptación o rechazo que se verá plasmada por una contraoferta. Es un juego mental entre los ámbitos de decisión estratégica que permanentemente están analizando el costo-beneficio de la transacción. Cuanto mayores beneficios, más libertad de acción se consigue[6].

Según Alemanno, existen tres niveles de decisión. De menor a mayor complejidad, el primero es el táctico, que elige aplicar entre un menú de opciones pre establecidas la que corresponde según el mensaje recibido. Utiliza mayormente información precisa y detallada. Un ejemplo de este nivel puede ser el trabajo que

[5] **Kent, Sherman,** Inteligencia Estratégica: Para la política mundial norteamericana, Editorial Pleamar, 1978.
[6] **Gauna, Eduardo,** Apuntes de Inteligencia estratégica, Amazon Mexico Services, 2018.

realiza un cajero de un banco. Ante un cliente que quiere retirar dinero en efectivo, si el monto solicitado está disponible en la cuenta del cliente y el banco tiene disponibilidad en ese momento, él ejecutará la decisión de darle el dinero, siguiendo un protocolo diseñado previamente por otros decisores de mayor jerarquía.

El segundo nivel de decisión es el operativo que utiliza una gran cantidad de información estadística. El ámbito operativo recibe objetivos a lograr y medios para hacerlo. Con ellos diseña formas de empleo de esos medios, los que son puestos en acción por la táctica.

El tercer nivel es el estratégico, donde el diseño de una misma acción debe lograr efectos diferentes en forma simultánea en la mente de distintos actores. Aquí podemos detectar claramente la complejidad que debe enfrentar la conducción estratégica. En primer lugar, interpretar lo que otros actores “piensan” y luego fijar objetivos y asignar medios acordes para lograr que esos actores acepten las propuestas, todo esto mientras los demás están haciendo exactamente lo mismo. Esto nos permite afirmar que el ámbito estratégico es un ámbito de intercambio de mensajes simbólicos, basados en una interpretación de las acciones que cada actor está desarrollando tratando de darles significado en nuestra racionalidad[7].

En síntesis, las decisiones tácticas utilizan mayormente información precisa y detallada. Las operacionales, una gran cantidad de información estadística, y las estratégicas son puramente especulativas. Es decir que el ámbito estratégico concibe situaciones, el gerencial diseña acciones y el táctico las ejecuta.

El proceso de toma de decisión en sí mismo es un proceso que conceptualmente es muy simple. Ante la aparición de un incentivo se analiza la situación, se estudian alternativas y se selecciona un modo de acción efectivo. Esta simpleza conceptual no quita complejidad al proceso cuando comenzamos a estudiar la naturaleza de los incentivos.

[7] **Gauna, Eduardo,** Apuntes de Inteligencia estratégica, Amazon Mexico Services, 2018.

Teniendo en cuenta lo antes dicho, la Inteligencia Estratégica que definimos como la producción de conocimiento para la toma de decisiones, no se dará en cualquier contexto, sino justamente en el ámbito estratégico.

Inteligencia Criminal

La Inteligencia Criminal se trata de la reunión de información dirigida a evitar y prevenir las actividades criminales específicas (de la Seguridad Pública) que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las Instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional[8].

Es decir que su objetivo es proteger el derecho de los ciudadanos a la seguridad pública generando conocimiento preventivo exclusivamente sobre aquellas organizaciones del crimen organizado que puedan vulnerar dicho derecho, o bien que ya lo hayan hecho, y en ese caso la Inteligencia Criminal actuará como auxiliar de la justicia.

Un ejemplo de esta actividad puede encontrarse en el Departamento Central de Inteligencia Criminal, de la Prefectura Naval Argentina, que tiene responsabilidad sobre tareas de inteligencia en la Prefectura Naval Argentina y acompaña el accionar institucional desde sus orígenes históricos en 1756, cuando se estableciera la primera Capitanía de Puerto, con funciones eminentemente policiales relacionadas con la seguridad de la navegación o en el ámbito portuario.

Mediante entrevista realizada a Hugo García, jefe de Inteligencia Criminal de la Prefectura Naval Argentina, se tomó conocimiento del trabajo de la Dirección de Inteligencia Criminal. Esta interviene en la recolección, análisis e integración de la información de interés en el área jurisdiccional de la fuerza. Dentro de las principales actividades se incluyen la producción de inteligencia criminal sobre las

[8] Cairo, Saniez, Manual de Inteligencia criminal, Ed. Seguridad y Defensa, 2006.

acciones de toda índole que puedan vulnerar la operatividad de los puertos y las vías navegables, así como la salvaguardia de los intereses marítimos, fluviales, pesqueros y portuarios de la Nación. Su origen data del 12 de marzo de 1951, cuando el entonces Prefecto Nacional Marítimo daba lugar a la creación de la División Informaciones y Seguridad, que luego de sucesivas transformaciones dio origen al actual organismo.

Según García, cuando Prefectura recibe instrucción de reunir información en virtud de sus funciones de Seguridad Interior, muchas veces se utiliza información proveniente de redes sociales, siempre mediante un pedido de una autoridad del Poder Judicial de la Nación. De modo que la actividad de recolección de datos personales sería en estos términos una práctica legal según la actual ley.

Ciberdefensa y Ciberseguridad

La Ciberdefensa es la actividad de protección de los intereses estratégicos de un país en Internet. Es una, relativamente, "nueva" actividad de las fuerzas armadas de cada nación, que así como su ejército protege los activos en tierra, la armada o marina en el mar y la fuerza aérea en el territorio aéreo, en el "territorio" de Internet es especialidad de comandos de ciberdefensa creados para ese fin.

La evolución de las tecnologías de la información y las comunicaciones ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas. La ciberdefensa, además de prevenir los ataques, les da respuesta con el fin de salvaguardar la seguridad[9].

La International Telecommunication Union (ITU), organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, establece cinco elementos fundamentales para desarrollar las estrategias de Ciberseguridad entre

[9] https://www.argentina.gob.ar/noticias/ciberdefensa-el-desafio-de-las-nuevas-generaciones Fecha de consulta 19/05/20

los que se encuentra el desarrollo de un marco legal para la acción y de medidas técnicas o la aplicación de una cultura de Ciberseguridad y de cooperación internacional[10].

La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos (vinculado con delitos comunes y no con ataques sobre intereses estratégicos, en esos casos serían temas de Ciberdefensa). También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término es amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final[11].

Con relación al rol de las redes sociales en la Ciberdefensa y la Ciberseguridad, Roberto Uzal, que se desempeña como Director de la maestría en Ciberdefensa y Ciberseguridad - UBA afirma que es esencial. Sugiere que, por ejemplo, han habido y hay múltiples campañas comunicacionales insidiosas, con el fin de influir por ejemplo en la opinión de un electorado, a través del uso de técnicas de Data Analytics.

Y amplía que “La fuente de ingresos de datos muchas veces proviene de las bases que disponen las redes sociales. Estos grandes agregados de datos, a los que se acceden de forma a veces lícita a veces no, son un insumo clave que segmentado y dirigido, son usados lamentablemente para la concreción de estas operaciones sobre la comunidad”

Algo similar pasa con las bases de datos de clientes bancarios o de tarjetas de crédito, desde donde estas organizaciones de ciber fraude se alimentan para montar sus acciones. El caso de Cambridge Analytica es un ejemplo de la capacidad de

[10] https://www.nextibs.com/que-es-ciberdefensa-se-diferencia-ciberseguridad/ Fecha de cosulta 19/05/20
[11] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security Fecha de consuta 19/05/20

incidencia en la opinión pública a través del procesamiento de grandes volúmenes de datos, la segmentación y el uso de esta información.

Una característica que debemos tener en cuenta al referirnos a Ciberdefensa es la complejidad que toma el factor territorial. Ya no podemos hablar de territorio tal cual lo entendimos hasta hace algunas décadas, las fronteras se borran y todo forma parte de una misma cosa, por lo que la aplicación de las soberanías y la protección de los intereses de cada nación va a tener que adaptarse a este nuevo escenario, sin lugares y sin distancias. No todos los Estados e instituciones lo entienden porque continúan basando algunos criterios de acción en la ocurrencia territorial de los fenómenos.

Los delitos de Ciberdefensa, como puede ser la intrusión de un Estado sobre algún activo estratégico de otro Estado a través de internet, también ven afectado el factor tiempo. Las acciones de esta especie se desarrollan en pocos segundos y los sistemas de los Estados para proteger estos activos deben resolver la intrusión también en una brevedad similar, para conseguir neutralizar efectivamente el ataque.

Para conocer quien realizó el ataque, se debe resolver la atribución, es decir la fuente de la agresión y para ello los sistemas trabajan desandando el camino que el atacante realizó, son decisiones que deben tomarse en fracciones de segundos y para lo cual el Estado va necesariamente a violar la jurisdicción de algunos Estados amigos por los que haya pasado el agresor. Esto no está bien visto, pero es un nuevo problema.

Sobre la posibilidad de que haya una vulneración del derecho de protección de datos personales en acciones de Ciberdefensa o de Ciberseguridad, Uzal cree que para reducir esto, es muy útil la elaboración de una matriz de riesgo, que no es otra cosa que listar los blancos más tentadores para un posible ciberagresor y este listado puede incluir una correspondencia en valores monetarios y sociales, es decir la afectación económica y social de suceder el evento sobre un determinado activo. Este análisis sumado a un eje que incluya la probabilidad de que estos hechos

ocurran, nos puede ayudar mucho a focalizar los esfuerzos en ciberdefensa y a su vez a disminuir cualquier vulneración innecesaria sobre datos personales u otros derechos individuales.

En este sentido, la Corte Suprema de los Estados Unidos, emitió una acordada donde declaró que su jurisdicción era global en cuanto a “ciber felonías” y le otorgó especialmente al Federal Bureau of Investigation (FBI) jurisdicción global en materia de ciberdelitos. Es decir que en relación a la aplicación del Derecho de Protección de Datos Personales u otros derechos emparentados, cuando una acción del FBI vulnere derechos de ese tipo en países aliados de los Estados Unidos, será una acción legal, al menos para esos países. Este tipo de decisiones políticas refuerzan la idea de que lo geográfico carece de sentido cuando nos referimos a cibercrímenes.

Repasando el escenario mundial, sabemos que China tiene un gran desarrollo en Ciberdefensa, pero también pesan sobre ellos algunas sospechas sobre cómo han podido acceder a conocimiento científico tecnológico, que a otras naciones les costó un desarrollo de años, en tiempos marginales. Como el caso de Editas Medicine, una compañía promocionada por el MIT de EEUU que investiga modificaciones en el ADN para conseguir combatir mejor algunas enfermedades. China llegó a resultados más avanzados poco tiempo después de que Editas Medicine tuviera sus primeros resultados después de mucho tiempo de desarrollos.

Rusia por su parte, también es otra de las potencias mundiales en materia de Ciberdefensa. Una muestra de ello se da cuando Putin estaba a cargo de la KGB, el Director de Tecnología Informática de ese organismo era el dueño de una de las empresas más importantes en la materia, nada menos que Eugene Kaspersky, dueño de Kaspersky Lab. Conocido por ser uno de los antivirus más populares del mundo.

Irán, después de haber sufrido ciberataques en su planta nuclear de la ciudad de Natanz, comenzó a desarrollar un alto nivel de medidas empoderando su equipo de ciberdefensa y en la actualidad es considerado una potencia en la materia.

Sobre los delitos que comete el Ciber Crimen Organizado Trasnacional, Uzal opinó que los delitos son diversos, dependiendo cual sea el interés del ciberagresor. Si persigue un interés económico, podrá tratar de vulnerar la seguridad de un banco o usuarios de cuentas bancarias para transferir fondos, o realizar ciber extorsiones amenazando con el manejo de cierta información sensible. Robar conocimiento científico tecnológico, etc.

Si el interés es geopolítico, o religioso y se busca generar un acto terrorista, o la afectación vital de una comunidad, el blanco del ciberagresor puede ser una de las industrias críticas de la comunidad como puede ser afectar una planta potabilizadora de agua y con esto la salud de la comunidad, o afectar una central nuclear convirtiendo en arma una instalación o solo cortando el suministro. Los blancos son tan variados como motivaciones haya.

Aunque suene contradictorio, los principales problemas relacionados a la seguridad en internet no provienen de internet, sino de la variante humana en el uso de internet. Estos problemas que se producen por acción humana en el uso de redes sociales por ejemplo, son las que afectan los derechos de la sociedad en general. Puntualmente cuando se omiten algunos aspectos éticos en el uso de internet, ya sea por parte del Estado, actores privados o particulares, la vulneración de sus datos personales puede crecer exponencialmente.

Finalmente el especialista aseguró que hay que hacer foco en el factor humano, entender de un modo más acabado las diferentes personalidades que hay en una sociedad y que en determinados lugares de decisión afectan sustancialmente nuestros derechos. Es ahí donde se ve la brecha más amplia y el flanco más vulnerable en lo que hace a la ciberseguridad y la ciberdefensa.

Redes Sociales

Una de las dimensiones centrales de esta investigación son las redes sociales. Las redes sociales a las que nos referiremos no son las contempladas por las teorías en las ciencias sociales, que se refieren a “una estructura social, compuesta por un conjunto de actores, tales como individuos u organizaciones, que están relacionados de acuerdo a algún criterio”. Dichas redes sociales “reales”, normalmente se representan simbolizando los actores como nodos y las relaciones como líneas que los unen.

En este trabajo nos referiremos exclusivamente a las llamadas redes sociales en internet. Estas se refieren al conjunto de perfiles individuales, de grupos, comunidades y organizaciones vinculados unos a otros a través de páginas web en internet que les permiten dentro de determinados términos y condiciones, relacionarse compartiendo información y datos personales principalmente.

Cada región y país tiene sus sitios o aplicaciones de redes sociales de preferencia. Entre los más populares podemos mencionar Instagram, Facebook, Twitter, LinkedIn y Snapchat. También existe una clara preferencia por una u otra red social según la edad del usuario y su pertenencia socio cultural así como el país.

Los formatos son diversos, si bien cada producto tiene sus características, la posibilidad de compartir imágenes, videos, textos, opiniones, mencionar a otros, etc. juegan un rol decisivo en el flujo de datos personales que la legislación busca proteger.

La Inteligencia Criminal, por ejemplo, hace uso de las redes sociales para buscar datos sobre una persona o un grupo que estén investigando. En este caso, la red social será la fuente de datos para los investigadores y serán las personas investigadas o sus contactos en la red social quienes ofrecerán involuntariamente información sobre la persona investigada.

En otros, las compañías dueñas de las redes sociales, entregan por pedido del poder judicial o de las autoridades de un país, información de sus usuarios, cuando consideran que la vulneración de la privacidad de un usuario será un medio para colaborar en la acción del poder judicial.

El crecimiento de las redes sociales, se visualiza en el volumen de usuarios nuevos, y también en el cambio de sus características de uso. Los cambios que parecen ir detrás de lo que los usuarios y las audiencias valoran como atractivo al momento de su uso, también ponen en evidencia las relaciones que establecemos con el consumo de esta tecnología. Por qué son tan adictivas y destinamos tanto tiempo en ellas.

Del otro lado de la pantalla, el fin de las compañías es mantener a los usuarios el mayor tiempo posible online para mostrarles publicidades o campañas de sus clientes. Según un informe de las compañías *Hootsuite* y *We are social*, durante 2019 las personas pasaron 2 horas y 24 minutos en redes sociales todos los días a través de diferentes dispositivos. Eso significa que 1 de cada 3 horas pasadas en internet son usadas en plataformas sociales. La cifra aumenta en las personas entre 16 y 24 años de edad que pasaron cerca de tres horas al día en redes[12].

El mismo estudio refleja que la mayor parte del mundo está en redes sociales, aportando datos significativos al respecto tales como que: El 50 % de la población mundial está usando redes sociales, es decir, 3.8 mil millones de personas (un aumento del 9.2% desde 2019); El 97 % de los consumidores digitales han utilizado las redes sociales en el último mes y que el 84 % de las personas que cuentan con acceso a internet usan redes sociales.

En el aspecto regional, América Central y Asia Oriental tienen la mayor saturación de redes sociales, con un 84 % cada una. En Europa, el norte de Europa tiene el mayor porcentaje de usuarios de redes sociales (79 %), en comparación con el sur

[12] Cooper, Paige, Evolution in the daily time spent on social media, Hootsuite, 2020. https://blog.hootsuite.com/es/125-estadisticas-de-redes-sociales/#generales
Consultado el 4-06-2020

de Europa (que cuenta con 66%), Europa occidental (62 %) y Europa oriental (57 %).

El norte de África presenta el mayor uso de redes sociales con un 55%, seguido del sur de África con un 49%. Mientras tanto, África oriental (13 %), media (10 %) y occidental (21 %) tienen el mayor margen de crecimiento[13].

Otro hecho que empujó este crecimiento exponencial fue la evolución del mercado de los smartphones. Desde que los celulares permiten navegar y sobre todo con la proliferación de las aplicaciones, las redes sociales se vieron beneficiadas a través de usuarios que las querían en la palma de su mano y en cualquier lugar donde estuviesen. Este beneficio fue recíproco, tanto para las redes sociales como para las compañías fabricantes de celulares inteligentes. En 2018, el 58% de los ingresos a sitios web se hicieron desde celulares[14].

Según la organización que estudia el mercado de la industria de celulares, *GSMA Intelligence*, en el año 2003 las líneas móviles activas en el mundo rondaban los 1.000 millones. Catorce años más tarde, en mayo de 2017, se superaron oficialmente los 5.000 millones de líneas activas, un aumento de aproximadamente 1.000 millones de líneas móviles cada tres o cuatro años.

Es importante agregar que para este trabajo entrevistamos a la actual interventora de la Agencia Federal de Inteligencia (AFI), Cristina Caamaño, designada por el presidente Alberto Fernández al frente del organismo de inteligencia argentino desde diciembre de 2019 con la misión de general reformas profundas en la estructura, como así también cambios en la cultura laboral de producción de inteligencia estratégica.

---

[13] Cooper, Paige, Evolution in the daily time spent on social media, Hootsuite, 2020. https://blog.hootsuite.com/es/125-estadisticas-de-redes-sociales/#generales Consultado el 4-06-2020

[14] Enge, Eric, Mobile Vs. Desktop Usage in 2019, Perficient.com, 2019. https://www.perficient.com/insights/research-hub/mobile-vs-desktop-usage-study Consultado el 4-06-2020

Caamaño consideró sobre las redes sociales que si bien son un fenómeno abrieron un abanico muy interesante, pero también complejo en términos de derechos. “Cuando una persona publica en alguna red social contenidos personales debe entender que esa información queda a disposición por un período de tiempo indeterminado. Sin embargo, las redes sociales, y ahora opino como fiscal jubilada, pueden aportar información para reconstruir el contexto de determinadas personas o hechos puntuales”.

También destacó que “A su vez, las redes sociales son utilizadas como canales orgánicos de instituciones públicas y privadas para comunicar temas de interés en su materia. El Estado es un conjunto complejo de agencias. Es muy difícil pensar qué tipo de conocimiento útil se puede producir de manera uniforme. No es lo mismo pensar a la Agencia Federal de Inteligencia que, por decir algo, al PAMI. No es lo mismo pensar a las redes sociales como una fuente de información o como un canal de comunicación institucional”.

Sobre el estado en el que recibió la AFI en relación al uso de redes sociales, Caamaño describió que “nos encontramos con prácticas absolutamente ilegales al momento de asumir la Intervención. Las fuimos denunciando penalmente. Una parte de la información recopilada tenía como fuente a las redes sociales. Inmediatamente, ordené detener todo tipo de tarea de reunión de información sobre ciudadanos, que representaba uno de los eslabones de las prácticas de inteligencia ilegal”.

Y finalmente consideró que “lo importante es el respeto de las garantías constitucionales de las personas. El Estado, con la excusa de la seguridad nacional, no puede violar los derechos de los ciudadanos”.

Datos, información y conocimiento

A fin de comprender con mayor claridad las diferencias entre estos tres conceptos, y a los fines de la presente investigación, el dato es la unidad más pequeña de la

información. Puede tratarse de un número, un nombre, una imagen, etc. En la temática de datos personales, los datos pueden ser un número de documento, teléfono, peso o estatura de la persona, dirección postal, la huella dactilar, la forma del iris del ojo o los patrones morfológicos de la cara.

En este sentido, cuando hablamos de datos, nos referimos a estos números o nombres sueltos, pero, como se verá a continuación, cuando estos datos se relacionan con un contexto, estamos refiriendo a *información*, y toman un sentido muy particular. Significan algo más que caracteres aislados.

Por ejemplo, el dato puede ser, a modo de ejemplo: “15 grados centígrados en la escala de celsius”. Es un dato que no nos dice demasiado por sí solo. Pero si esa temperatura se da en un lugar y en una época del año, puede significar una temperatura alta o baja dependiendo del contexto.

Por otra parte, cuando nos referimos a información estamos hablando de uno o un grupo de datos interpretados y analizados en un contexto determinado. Ya no son datos aislados. La significación de un dato en un contexto o en otro puede determinar informaciones muy distintas, es por ello que este relacionamiento tiene una implicancia importante a la hora de entender que significa una información.

Según la especialista en calidad de información, Mag. María José Espona “Lo único real es el hecho, al que nosotros usualmente no tenemos acceso por lo que utilizamos datos o informaciones procesadas por otros, desconocidos en la mayoría de los casos, para tener alguna referencia sobre el evento ocurrido”[15].

El conocimiento, finalmente, es un paso superior al de la información. Tiene que ver con la historicidad de la información, de los actores y de las fuentes. Es la capacidad de relacionar y analizar determinada información para comprender lógicas y patrones de un fenómeno determinado y fundamentalmente poder predecir el comportamiento de un evento en el futuro.

[15] Espona, María José, Material de clase, UNLP, 2014.

Volviendo al ejemplo meteorológico, fenómenos como sequías o inundaciones, son muchas veces pronosticados con el suficiente tiempo para poder tomar decisiones que mitiguen los daños sobre una comunidad o sobre el ecosistema de una región.

Este tipo de conocimientos se construyen en base a datos recolectados con instrumentos tecnológicos. Los analistas los ponen en contexto y valorando la historicidad de esa información pueden hipotetizar sobre que va a suceder. Este ejemplo sintetiza el significado de conocimiento.

Tecnología de la información

La tecnología de la información se refiere al uso de dispositivos físicos o virtuales para la recolección, el procesamiento, almacenamiento o transmisión de datos.

Esta rama de la ciencia tecnológica tomó una importancia exponencial cuando internet se volvió un elemento masivo y con ello la posibilidad de reunión y análisis de grandes volúmenes de datos. También el factor económico que presentó la aparición de internet fue determinante para las tecnologías de la información, influyendo en la baja de costos y en la viabilidad de conectar datos de diferentes puntos del planeta de forma instantánea.

Los procesos también fueron evolucionando de la mano de computadoras con procesadores cada vez más potentes y de tamaños cada vez más reducidos. El almacenamiento en la nube también cumple su rol en este cambio. La información está disponible en volúmenes y lugares que antes eran impensados. Esto también tiene importancia para la preservación de la información, pero también encuentra críticas acerca de la protección de los datos personales que esta información pueda contener, como así también sobre la jurisdicción legal en que los servidores físicos se sitúan.

La tecnología de la información cambió radicalmente y su potencia hoy influye decisivamente sobre la toma de decisiones en las sociedades modernas, la

conexión de las economías hacen que un hecho que sucede en una región instantáneamente influya sobre la toma de decisiones y el valor de los activos de otra. En la vida familiar, por ejemplo, facilita la capacidad de encontrar un vuelo o un hotel más económico al planificar un viaje, hasta el uso vital de poder pronosticar más eficazmente un fenómeno climático, como mencionamos.

En lo que hace a los datos personales, existe cierta preocupación en la sociedad sucedieron y suceden hechos de uso de datos personales en redes sociales para favorecer campañas electorales, crear y viralizar noticias falsas con el fin de influir opiniones y decisiones.

Otro tipo de hechos está relacionado con delitos, fraudes o engaños con el fin de robar datos de una tarjeta de crédito con técnicas de *Phishing*.

El *Phishing* es una técnica de engaño que se ha popularizado en los últimos años en internet. Lo que busca es simular ser un correo electrónico, por ejemplo, de alguna entidad oficial o compañía solicitando al usuario hacer click en un enlace que lo llevará ya sea a modificar su contraseña aludiendo un motivo de seguridad, o acceder a un beneficio. Una vez que el usuario engañado hace click en el enlace por lo general el sitio apócrifo (que en apariencia simula ser un sitio de confianza reconocido, como Amazon, Mercado Libre, el banco de la persona, su correo electrónico, etc) le solicita al usuario poner su nombre de usuario y contraseña.

Hecho esto, el delito ya se habrá concretado y la información personal habrá sido enviada a los delincuentes informáticos. Muchas veces piden datos de tarjetas de crédito, o solo con tener los datos de acceso a cuentas pueden comprar a nombre del usuario atacado, acceder al homebanking o quizás solo robar el perfil de red social para usarlo en campañas de manipulación o marketing online. Los fines son diversos, lo que es seguro es que ninguna de estas maniobras beneficiará al usuario y los derechos sobre los datos personales estarán vulnerados.

Una buena práctica para evitar este tipo de ataques consiste en leer la dirección desde donde nos han enviado el correo y plantearnos si tiene aspecto o no de un

mail de una entidad oficial. También es importante no abrir un link que venga en un correo electrónico donde inmediatamente soliciten cargar manualmente datos y contraseñas. Otro aspecto a tener en cuenta es la dirección electrónica de los sitios, aquellos que comienzan HTTPS (S de Security) en vez de con HTTP, cumplen con mayores protocolos de seguridad informática.

Las redes sociales son un medio para estas prácticas, por eso nuestra atención y la desinformación y permisos que les damos a las aplicaciones en los teléfonos celulares también forman parte de este espacio gris, con poder para simplificar la vida o bien para comercializar vulnerabilidades. La información personal tiene un precio para quien sin escrúpulos busca obtener un rédito económico sobre datos, en apariencia simples, pero que en determinados contextos y usos se valoran especialmente.

Big data

El Big Data o ciencia de los “grandes datos” es el análisis de una gran cantidad de datos.

El concepto, también conocido como “Macrodatos”, tiene su fundamento en la interpretación de grandes volúmenes de datos para encontrar patrones, entender comportamientos y, en el mejor de los casos, predecir eventos sobre el fenómeno estudiado. Es decir que Big Data tiene que ver con la cantidad de datos y no con su tamaño individual.

Es importante señalar que para el procesamiento de los datos siempre va a ser necesario un software que tenga capacidad para procesar el volumen de datos que se quieran estudiar. Los software para macrodatos necesitan de cierta expertise por parte del usuario del sistema informático. Uno de los más populares se llama “R”.

A los fines de la presente investigación, nos interesa comprender el concepto de Big Data porque los datos que se generan en las redes sociales en internet son

masivos, o por lo menos quienes buscan tomar decisiones en base a los datos en ese contexto van a analizar grandes volúmenes que les signifique un peso específico en la comprensión de un fenómeno para la toma de decisiones.

Ahora bien, en el caso de las redes sociales en internet, esta intencionalidad de análisis masivo de datos a priori parece poner en segundo plano la identidad del usuario o por lo menos restarle importancia al dueño del dato personal y su individualidad, en aras de valorar la información que se produce analizando el resultado y la relación de cientos de miles de datos.

No obstante, desde el enfoque de este trabajo se resalta la relevancia que el derecho de protección de los datos personales tenga en el campo de la Big Data. En definitiva, es preciso remarcar que el único apoderado sobre los datos personales es el titular y por más que se los reúna con otros miles de datos, si la fuente del análisis es un dato personal, debe ser manipulado con ese status, con el debido conocimiento y autorización de su titular.

Calidad de la información

Se trata de una disciplina dentro de las ciencias sociales, que plantea una metodología con el fin de ponderar la calidad de información. Esta herramienta cobra una importancia singular en un contexto de “sobre información” y generación exponencial de contenidos on line, en diferentes plataformas y formatos.

María José Espona, especialista en Calidad de Información destaca que la mayoría de las personas considera a la calidad en relación a la precisión y la confiabilidad en los datos, mientras que un segundo grupo considera que la calidad está relacionada con la utilidad que posea en el contexto en la que la utilizarán[16].

[16] Espona, María José, Metodologías para el análisis de información: una necesidad de nuestros días, Paper, 2017.

Espona afirma que el objetivo de establecer una relación entre hecho, dato e información tiene que ver con que no podemos hablar de calidad de datos, sin saber de dónde vienen los datos o información sobre los cuales vamos a determinar o valorizar su calidad. Una vez que tenemos la información y la procesamos, obtenemos un producto de inteligencia que luego se transforma en conocimiento. Los datos son los ladrillos y pilares con los que construimos conocimiento y si ellos no son buenos, nuestro edificio se cae como un castillo de naipes.

La universidad norteamericana Massachusetts Institute of Technology (MIT), tiene un programa de Calidad de Información liderado por el profesor Richard Wang. El mismo establece dieciséis dimensiones para ponderar la calidad de la información. Dentro las categorías que se miden están: Precisión, objetividad, credibilidad, reputación, relevancia, valor agregado, actualidad, completitud, cantidad, interpretabilidad, facilidad de entender, representación concisa, representación consistente, accesibilidad y seguridad de acceso.

Esta especialidad no sólo pone foco en analizar estas categorías, que desde ya son extensas, sino que también se ocupa de estudiar el flujo de la información y de las decisiones tomadas en base a dicha información en el interior de las diferentes organizaciones.

Espona (2017) analizó las categorías que propuso el MIT y las agrupó en cuatro dimensiones para que la interpretabilidad de las mismas sea más sencilla:

Categoría	**Definición**
Intrínseca	Denota que la calidad del ítem está autocontenida, es decir, que el contexto no determina la calidad. Incluye las dimensiones: credibilidad, precisión, objetividad y reputación.
Contexto	Se tiene en cuenta al contexto como algo esencial. Incluye cinco dimensiones: valor agregado, relevancia, oportunidad, completa y cantidad de datos.
Representación	Refleja la importancia de la presentación de los datos y aspectos metodológicos. Incluye las dimensiones de interpretabilidad, facilidad de comprensión, consistencia representacional y representación concisa.
Accesibilidad	Lidia con la disponibilidad de datos y sobre cómo están protegidos del uso no autorizado. Las dimensiones son la accesibilidad y seguridad.

Cuadro 1: Fuente: Espona, María José, Categorías de Calidad de Datos, 2017.

Todas estas herramientas y aportes que surgen desde la academia ofrecen una mirada mucho más profunda y crítica sobre el manejo de datos. Poner el foco en la calidad de los datos no solo es el objetivo de aquellos que pretendan producir información valiosa para la toma de decisiones, también lo será para las legislaciones e instituciones que busquen proteger los datos personales de los ciudadanos, conocer y categorizar de que tipo de dato estamos hablando, por qué y cómo lo protegemos. También esta mirada sirve para ponderar si, en todo caso,

existe o no una reunión excesiva de datos. Es decir, si se están recolectando datos que no serán útiles por su baja o inadecuada calidad.

Empresas de medios

La mayor parte de la información que circula en la sociedad lo hace a través de fuentes abiertas y semiabiertas, y un porcentaje considerable de la misma se canaliza a través de las empresas de medios de comunicación.

Si bien la recolección de datos de medios de comunicación en muchos casos no nutre por completo el ciclo de inteligencia, (fuentes de inteligencia basada en datos abiertos - OSINT por su sigla en inglés “Open Source Intelligence”) , es un buen proveedor de alertas tempranas. Esto, sumado a la creciente accesibilidad que las tecnologías de la comunicación desarrollaron en los últimos diez años, sobre todo a través del uso de internet, nos presentan un escenario interesante para hacer algunas observaciones sobre aspectos a tener en cuenta para el análisis de este tipo de fuentes.

En los medios de comunicación, sea cual fuere el formato del producto que ofrecen (TV, Radio, Portales Web, Medios Gráficos, Agencias de noticias y sus variantes “trasmedia” - mezcla de dos o más formatos mencionados), el rol de los productores se emparenta a la función del analista de inteligencia en algunos aspectos que tienen que ver con el monitoreo de la información, el manejo de diversas fuentes, la selección de los datos y el análisis de dichos datos para la posterior producción de información.

Claro está que, a diferencia del analista, donde su producto es utilizado por un decisor para la toma de decisiones, que persigue la mayor “objetividad” y se busca prospectar sobre determinado fenómeno; muy por el contrario, el productor tiene como objetivo recolectar datos y analizarlos para construir información diseminable masivamente a la sociedad bajo el interés económico de su empresa y, en segundo lugar, con el fin de que dicha información o producto consiga agrupar la mayor

cantidad posible de audiencia receptora de los mensajes publicitarios de sus anunciantes. Lo que se conoce como público cautivo.

Si bien nos referimos en el párrafo anterior a la “producción” de información en empresas de medios, la característica de mayor robustez dentro de estas organizaciones, por sobre cualquier otro aspecto, es su aparato de diseminación. Con esto nos referimos a la potencia y capacidad de hacer “masivo” un mensaje o producto en un corto periodo de tiempo. Esta es la cualidad que dota a los medios de un impacto psicológico destacable y por lo que consiguen instalar temas en la opinión pública, generando parámetros de decisión dentro del recorte que cada empresa busca establecer como el espacio natural de la información pública.

En este sentido debemos decir que, el analista que busque datos para construir su propia información en base a información diseminada por medios, va a tener que formar un criterio muy específico y transitar diferentes procesos para comprender la lógica de los intereses de cada grupo mediático, su línea editorial, intereses empresarios (económicos) e institucionales (políticos), target de la audiencia, etc. Posiciones que fluctúan en fracciones de tiempo cada vez más reducidas.

A la vez deberá establecer mecanismos que permitan certificar la veracidad de los datos recolectados e intentar correlacionar varios datos de fuentes diversas, algunos forzados (“sucios”) o bien modificados individualmente por pertenecer al proceso constructivo de información de diferentes medios.

A fin de cuentas, se deberá consolidar dicha fuente como OSINT V (OSINT Validada). El conocimiento sobre las características culturales de cada sociedad serán determinantes para que el analista pueda comprender, con el menor margen de error y en el menor tiempo posible, ponderando qué datos e informaciones son relevantes y cuáles no, según el requerimiento sobre el cual esté trabajando en la reunión de información, aspecto que se denomina también “contexto-dependiente”.

La naturaleza de las empresas de medios también conlleva un alto grado de vulnerabilidad y permeabilidad a intereses corporativos y sectoriales de grupos de la

sociedad que buscan modificar, instalar o silenciar informaciones según sus propios intereses.

Finalmente, otra característica que sería importante nombrar, es la creciente digitalización de los contenidos de fuentes abiertas y en este caso mediáticas, como se da en la tendencia de desaparición de los diarios y revistas de papel y la conversión a formatos digitales (webs, portales, e-books, contenidos en redes sociales, etc).

Este crecimiento exponencial del contenido online, desde el punto de vista de la Inteligencia Estratégica, hace sumamente importante el manejo de softwares y desarrollos de monitoreo de palabras clave que puedan hacer una primera búsqueda, un tamizado grueso (también una alerta temprana) de aquellos datos que se actualicen en la web, para un posterior análisis pormenorizado para el que sólo estará capacitado el analista (la mente humana).

Noticias falsas

Las noticias falsas, conocidas popularmente como *fake news*, son un concepto relativamente reciente que si bien no está circunscripto a las redes sociales es allí donde habitualmente o bien se genera o se potencia.

Las noticias falsas están caracterizadas por su gran impacto, pero fundamentalmente por su contenido falso. La noticia que se da, siempre es falsa, y con su gran impacto busca ser viralizada con velocidad en la mayor cantidad de usuarios, grupos y sitios webs posibles.

El objetivo de las fake news puede ser diverso: dañar la reputación de una persona o una organización, alterar la toma de decisiones de una comunidad antes de una elección, influir en la decisión de compra de un producto o servicio, entre otras.

En muchos casos, el camino de la fake news empieza con una redacción robusta y falsa pero verosímil. También en ocasiones se le añaden imágenes o videos, que pueden estar retocados digitalmente o no ser actuales ni relacionados al hecho que se busca instalar.

En esos puntos se respalda el éxito de una fake news, en el camino se apela a ganar en viralización, es decir que usuarios la repliquen en sus cuentas, y de ser posible, usuarios influyentes (popularmente llamados *influencers*) con muchos seguidores y con un prestigio que los hacen creíbles entre sus comunidades.

Allí radica la segunda parte de su éxito, cuando un *influencer* replica una fake news, aunque no haya verificado demasiado la calidad de la información que comparte, le da indirectamente su aval, dotándola de una aparente confiabilidad. Muchos otros en consecuencia la compartirán, ya no por la correspondencia de los hechos con la verdad, sino por la reputación que el *influencer* o el usuario de confianza (un amigo o un familiar) le da implícitamente a esa noticia.

Otro aspecto que se debe tener en cuenta es el fenómeno llamado *Deep fake*, que consta de la edición audiovisual de las declaraciones de una persona influyente. A través del uso de programas digitales insertan otra boca y otro discurso donde estaba la original, de esta forma le hacen decir al actor algo que no dijo con las consecuencias que esto trae al difundirse y no percibirse la falsedad de dicho video dada la alta calidad de edición.

Un video ya no es una evidencia irrefutable de que alguien haya dicho algo, ya no es una prueba de verdad. Desde nuestra perspectiva destacamos que estas ediciones violan el derecho de protección de datos personales, ya que la voz y la imagen del rostro son datos personales que no deben alterarse sin permiso del titular.

Privacidad

Según la Real Academia Española, la privacidad se define como: *el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.*

En ese sentido, el Artículo 12 de la Declaración Universal de los Derechos Humanos adoptada por la Asamblea General de Naciones Unidas establece que el derecho a la vida privada es un derecho humano: *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*[17].

Participar de una red social para una persona es una elección que, salvando casos especiales, se toma en completa libertad. En ese contexto uno elige compartir una gran cantidad de datos personales de manera voluntaria. También acepta términos y condiciones legales tan extensos y complejos que rara vez se leen y que son un requisito para crear un perfil.

Así comienza la vida de un usuario en una red social, un nacimiento bastante condicionado desde el punto de vista del derecho a la privacidad y de la protección de los datos personales. También hay otros derechos que comparten con los recién mencionados una frontera difusa, y estos son los derechos de seguridad pública, el derecho de libertad de expresión y el de libre acceso a la información pública.

En la legislación argentina, el Artículo 18 de la Constitución de la Nación establece que *el domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación.*

Mientras que el Artículo 19 a su vez dice que: *Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un*

[17] Declaración Universal de Derechos Humanos, Artículo 12, 1948.

tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados[18].

En este contexto, es legítimo interpretar que el usuario no está solo junto a la empresa proveedora del servicio de la red social; el Estado tiene un rol importante y el deber de velar por la protección de todos los derechos que mencionamos, pero en ocasiones debe elegir y demostrar que anular el derecho a la privacidad de una persona se justifica para proteger otro derecho de mayor afectación a la comunidad como puede ser (en determinado contexto) el derecho de gozar de seguridad pública.

Se espera que el Estado a través de sus políticas públicas respete la proporcionalidad de cada caso justificando el criterio de "necesidad y legitimidad".

Tanto en nuestro país como en otras partes del mundo, para reforzar el derecho a la protección de los datos personales, la actualización de las legislaciones, busca ser una base de sustento donde hagan pie los derechos básicos sobre la materia. Sin embargo, muchas veces conseguir los consensos sobre un texto legislativo es una tarea que en el caso de lograrse, su dilación en el tiempo juega en contra de los derechos que busca proteger.

La velocidad con que la tecnología de la información evoluciona pone en aprietos al sistema legislativo de una lógica de funcionamiento bastante distinta a la libertad de internet y sobre todo a su velocidad. En este punto los cuerpos legislativos y las autoridades administrativas de los países tienen un desafío que asumir. ¿Crear nuevas leyes, modificar las existentes, crear mecanismos administrativos, ofrecer mecanismos de evaluación y tomas de decisiones por caso?. Estos son algunos de los interrogantes principales que surgen.

¿Cómo mejorar la protección de la privacidad de las personas? El derecho a la privacidad, el derecho a que nuestros actos, (o al menos algunos de ellos) queden

[18] Ley N° 24430, Constitución de la Nación Argentina, Primera Parte, Capítulo Primero, Artículo 19, 1995.

en privado es uno de los derechos esenciales para la vida en sociedad y desde el origen de internet la percepción de vulnerabilidad del mismo está en aumento. La exposición es mucho mayor para cualquiera que lo desee voluntariamente, pero también las amenazas a las vulneraciones de privacidad son mayores para aquellos que quieren mantener en privado todos o algunos aspectos de su vida.

Participación ciudadana

Las formas en que las personas participamos de acciones sociales, políticas o culturales también experimentaron un cambio sustancial a partir de la emergencia de internet. En este caso, las posibilidades que dio internet y las redes sociales en especial fueron sumamente significativas.

Antes los medios para tener una participación ciudadana activa tenían que ver con la posibilidad de participar de reuniones o encuentros mayoritariamente de forma física. Eran lugares de encuentro para diferentes causas los clubes, las sociedades de fomento, los locales de los partidos políticos y algunos lugares de la vía pública como plazas, todos con un límite físico para reunir personas.

Los lugares de encuentro tenían un aspecto geográfico muy marcado, las reuniones se convocaban por barrios, a los vecinos de una comunidad se los convocaba a través de volantes o carteleras, mensajes también de una difusión local y restringida muchas veces al “boca en boca” o a través de medios locales.

Las redes sociales en internet rompieron con los límites físicos, y con la regionalización de las causas en las que la gente participa y se involucra para intervenir en los cambios o expresiones de la sociedad. Ahora una causa puede reunir a miles o millones de personas, dado que hay “espacio” para todos. No es necesario concurrir a un lugar específico.

La posibilidad de participar también se hizo más horizontal, ya todos podemos intervenir, y opinar y esa garantía es uno de los principales atractivos de

participación. Esto también cambia el concepto de poder, la verticalidad construida durante tantos miles de años ve en estas plataformas utilizadas para la participación ciudadana su variante.

A su vez surgieron plataformas de redes sociales pensadas en el impulso económico que puede dar la participación ciudadana. Estos sitios dan la posibilidad de organizar colectas para apoyar de forma voluntaria a determinado proyecto, popularmente conocidas como *crowdfunding* (financiación colectiva) ó *fundraising* (recaudación de fondos). Este tipo de webs ha sido muchas veces el puntapié inicial de muchos emprendimientos que potenciaron economías regionales o que crearon productos y servicios que antes no existían.

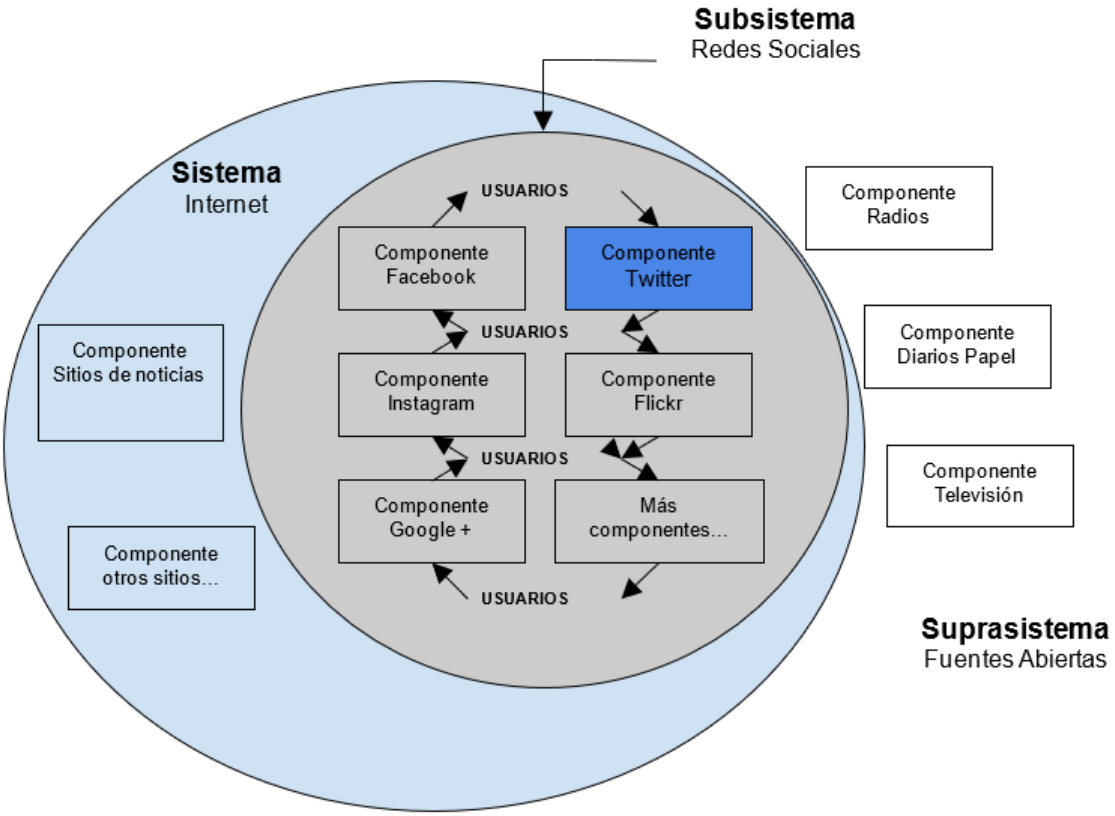
Método sistémico e hipótesis competitivas

Método sistémico

También conocido como la *Teoría General de los Sistemas*, el método sistémico fue propuesto por el biólogo Ludwing Von Bertalanffy, el cual nos brinda una herramienta científica de análisis y representación de la realidad que se destaca por la capacidad de integración y relación de la información. Principalmente representado a través de conjuntos y vínculos o relaciones. Para su creador la teoría debía ser un mecanismo de integración entre las ciencias naturales y las ciencias sociales con el fin de formar y asistir a los científicos.

Este método de análisis nos ayuda a generar una normalización de los datos para poder clasificar características, funciones y comportamientos dentro de un sistema. También nos permite pensar en términos de patrones aplicables a un conjunto de características o comportamientos y, finalmente, nos facilita la contabilidad de estos comportamientos de forma totalizable y por qué no, estadística. De alguna manera el método reutiliza el modo de trabajo previamente desarrollado en el área de Sistemas (Informática, por ejemplo) y lo lleva a otras disciplinas y ciencias.

Aplicación del método sistémico en Redes Sociales



Fuente: Elaboración propia

Como vemos en la representación de arriba, el componente Twitter, a modo de ejemplo, está dentro del Subsistema “Redes Sociales” que, a su vez, está dentro del Sistema “internet”, el que pertenece al Suprasistema “Fuentes abiertas”.

Según este análisis, podemos determinar que el sistema de Redes Sociales en internet, por su *entitividad*, es considerado un sistema “modelo” al no ser totalmente “real” ni de existencia “ideal”. Del mismo modo, lo clasificamos como un sistema “complejo”, “artificial” y, según su grado de intercambio (aunque tenga unos pocos elementos aislados) es considerado mayoritariamente “abierto”.

Este método de análisis es particularmente interesante de usar para pensar las Redes Sociales, dadas las características de interdependencia tan presentes en las comunidades en internet, siempre vinculadas e interrelacionadas. Del mismo modo, para el trabajo de Inteligencia en Redes sociales, el método sistémico aporta a un determinado problema una comprensión del contexto, y la definición de ese problema será lo que nos llevará a diseñar en un principio un modelo de sistema u otro.

Las Redes Sociales en internet, según la descripción y la representación en el diagrama, conlleva las siguientes características: A) Sinergia: su comportamiento siempre será analizado como un todo y no como la suma de sus componentes. B) Totalidad: Cada parte o componente del sistema se entiende organizadamente en conjunto a todos los elementos del sistema, si algo cambiara en una parte del sistema, cualquier otro componente se vería afectado en alguna medida. C) Recursividad.

Cada parte del sistema, es un sistema en sí mismo. Instagram, por ejemplo, es un sistema en sí mismo, que está dentro del sistema internet. D) Homeostasis. Es la característica que torna de cierto equilibrio al sistema. Si el componente “Facebook” deja de funcionar, posiblemente el componente “Instagram” compense esa baja ya que muchos usuarios canalizarán sus contenidos en otro componente, estabilizando el sistema. E) Entropía. Es la tendencia a la degradación de los sistemas.

En Redes Sociales lo vemos cuando aplicaciones dejan de tener una funcionalidad aceptada y deben recibir modificaciones constantemente para mantener su funcionamiento y aceptación. Sin cambios la entropía los desnaturalizaría hasta que se tornen obsoletos y desaparezcan. F) Retroalimentación. Consiste en como un elemento alimenta a otro por el hecho de estar intercomunicados dentro del sistema. Un ejemplo de esto se observa en las “Fake News” (noticias falsas), o con los “Memes”. Son contenidos muchas veces con origen en el sistema Redes Sociales que pasan a medios tradicionales. También sucede al revés, notas periodísticas originadas en medios tradicionales alimentan a las Redes Sociales.

Las etapas de este análisis están regidas bajo el método inductivo. Es decir que se pasa de lo particular a lo general, partiendo desde el problema o tema, para luego incorporar a los actores o elementos que rodean al tema.

Seguidamente se analizarán y describirán los subsistemas y sistemas integrados por los elementos hasta llegar a un suprasistema que los contenga a todos (ver esquema).

Por otra parte, para analizar las redes sociales y las fuentes abiertas de información, debemos trazar fronteras o límites gráficos que separan, o en otros casos, conectan actores o hechos dentro del análisis. Este aspecto del trabajo con sistemas puede aportar una claridad de comprensión singular.

Hipótesis competitivas

El método de Análisis de Hipótesis Comparadas (AHC), creado por el Ex-CIA Richards Heuer, también conocido como Hipótesis Competitivas es una herramienta muy útil para formular juicios diferentes que nos permitan valorar conclusiones alternativas sobre un evento.

Esta técnica, difundida en 1999 por el autor del libro *Psychology of Intelligence Analysis,* nos ayuda a evitar la tendencia natural de percibir sólo aquella información que confirma la hipótesis principal que tenemos sobre un tema, conocida como “estratégia de complacencia”.

Intuitivamente, ante un determinado fenómeno, todas las personas percibimos una respuesta como la más probable y la “estratégia de complacencia”, consiste justamente en complacer esta intuición buscando solo información o evidencia que la sustente, o en todo caso que la rechace.

Este método cobra una importancia significativa en el contexto del análisis en redes sociales que, al tener una gran cantidad de información disponible, si solo buscamos

información que sustenta nuestra hipótesis “intuitiva” es probable que encontremos alguna evidencia que nos contente y esto nos lleve a dejar de buscar otra información que podría refutar nuestra hipótesis o bien abrirnos el camino a nuevas hipótesis que nos acerquen a la verdad del fenómeno.

Algunas evidencias pueden funcionar tanto para una hipótesis A como para una hipótesis B, es decir que si damos por cierta la hipótesis A cuando la primera información es compatible, podemos estar desconociendo una hipótesis B que sea diferente y también compatible con la misma evidencia.

El uso de internet para combatir actividades terroristas

Si bien las organizaciones terroristas estan utilizando internet como un medio de explotación para sus objetivos estratégicos, internet es también un medio desde donde se puede potenciar las oportunidades para el combate del terrorismo y las actividades ilícitas, poniendo el foco en la investigación, la prevención y métodos de reunión de inteligencia más adaptados al desafío actual. Es decir que aquello que puede ser visto como una amenaza, como lo puede ser el medio de internet y las redes sociales para el terrorismo, es también una oportunidad para los Estados que desarrollen capacidades profesionales y técnicas a la altura de las circunstancia.

Internet no solo posibilita la reunión de inteligencia para la toma de decisiones, sino que también da lugar a la reunión de datos que sirvan como pruebas para el juzgamiento de esos actos terroristas. Las comunicaciones de los sitios web, salas de chats y grupos temáticos en redes sociales, son todas posibles fuentes de información de donde se puede extraer una cantidad importante de información sobre el funcionamiento, las actividades y, en ocasiones, los blancos de los terroristas.

El medio electrónico de comunicación, si bien tiene sus códigos, pone a disposición una gran cantidad de datos disponibles globalmente, lo que posibilita su recolección inmediata posterior a su publicación.

El aporte del análisis humano, muchas veces no puede ser reemplazado por la tecnología de la información que nos de un software. Pero sí podemos desarrollar una retroalimentación entre ambas capacidades. La traducción específica de los códigos que pueda utilizar una determinada organización posiblemente será un desarrollo más propio de la HUMINT, pero dicha resultante se torna exponencial al sistematizarse e incorporarse a una plataforma software que por ejemplo busque en la web esos datos específicos.

Para reducir la radicalización y la violencia extremista mediante la detección de propaganda extremista en internet, y responder con contraargumentos dirigidos mediante una amplia gama de tecnologías de las comunicaciones, incluidas las herramientas digitales, el Centro de Comunicaciones Estratégicas contra el Terrorismo, con sede en los Estados Unidos, ofrece un ejemplo de una iniciativa interinstitucional lanzada recientemente.

Por ejemplo, según se informó, “en mayo de 2012 el Centro respondió, dentro de las 48 horas, a anuncios publicitarios que promovían la violencia extremista aparecidos en varios sitios web de Al-Qaida en la Península Arábiga, con contraargumentos publicados en esos mismos sitios web que presentaban una versión modificada de ese mismo mensaje con el fin de demostrar que las víctimas de las actividades de la organización terrorista eran ciudadanos yemeníes. La campaña de contraargumentos fue posible gracias a la cooperación entre el Departamento de Estado de los Estados Unidos, la comunidad de los servicios de inteligencia y las autoridades militares. El Centro también utiliza plataformas de redes sociales como Facebook y YouTube para sus comunicaciones con contraargumentos”[19].

[19] ***Fedotov, Yury,*** Uso de internet con fines terroristas, Oficina de las Naciones Unidas contra la droga y el delito, Viena, Austria, 2013.

https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Las acciones contra el terrorismo a su vez promueven la protección de los derechos humanos que si bien son objetivos complementarios que se refuerzan mutuamente y deben perseguirse al mismo tiempo.

Si bien la prohibición de la incitación al terrorismo puede implicar restricciones a la libertad de expresión. La libertad de expresión no es un derecho absoluto. Ese aspecto limitante de derechos, es en nuestro país muchas veces criticado y es una realidad considerada políticamente incorrecta.

En los hechos, la libertad de expresión se puede restringir por parte de los Estados, a condición de que la restricción satisfaga pruebas estrictamente concebidas de legalidad, necesidad, proporcionalidad y no discriminación, cuando esa libertad se usa para incitar a la discriminación, la hostilidad o la violencia. Una de las principales dificultades en los casos de incitación a cometer actos terroristas es determinar por dónde pasa la línea de aceptabilidad, ya que esto varía mucho de un país a otro, según las diferentes historias culturales y jurídicas. El derecho a la libertad de asociación es igualmente un derecho limitado, que puede ser objeto de restricciones y excepciones de interpretación estricta.

La lucha contra el uso terrorista de internet puede implicar la vigilancia de sospechosos y la reunión de información sobre ellos. Debe prestarse especial atención a la protección de las personas contra las injerencias arbitrarias o ilegales en su derecho a la vida privada, que incluye el derecho al carácter confidencial de la información sobre la identidad de una persona, así como su vida privada. Por eso la importancia de la vigencia de las leyes de protección de datos personales, que en cada país, si bien internet es un espacio global, se manifiestan de manera particular.

Las leyes nacionales (de acceso a la información, libertad de expresión y protección de datos personales, principalmente) deben ser suficientemente detalladas con respecto, entre otras cosas, a las circunstancias específicas en que puede permitirse tal injerencia. Deben existir garantías apropiadas para evitar el abuso de los instrumentos de vigilancia secreta. Además, todos los datos personales

recogidos deberán estar debidamente protegidos para defenderse contra el acceso, la divulgación o el uso ilegales o arbitrarios.

Las acciones de las fuerzas de seguridad y servicios de inteligencia.

Para el control de los casos de terrorismo con uso de internet por presuntos terroristas se precisa de la realización de actividades muchas veces intrusivas o coercitivas de registro, vigilancia o monitorización por los servicios de inteligencia o los organismos encargados de hacer cumplir la ley. Es importante para que los datos recolectados tengan sustento legal, que estas técnicas de investigación estén debidamente autorizadas por las leyes nacionales y, como siempre, que la legislación de apoyo defienda los derechos humanos fundamentales protegidos por las normas jurídicas internacionales.

Acciones de almacenamiento, vigilancia e interceptación de información.

En 2007, se promulgó la Ley de datos sobre comunicaciones. El propósito de esa ley era organizar, de manera más estructurada y progresiva, la práctica establecida en cuanto a la obtención de datos sin contenido (datos de tráfico) de las empresas de telefonía fija y móvil, así como de los proveedores de acceso a internet. La Ley no se aplica a los proveedores de servicios de internet, que ofrecen otros servicios, como el almacenamiento de información, intercambio de información, correo electrónico, servicios sociales y demás. En la actualidad, en los casos en que las autoridades desean obtener información de los proveedores de servicios de internet, es aplicable una disposición legal anterior que les permite, en general, emitir una citación con apercibimiento y obtener información de cualquier persona que tenga información que pueda ser de utilidad para una investigación.

La recolección de pruebas de formato digital desde 2010 en Israel, fue respaldada a través de un proyecto de ley para la codificación de las facultades de investigación en relación con los datos tanto físicos como digitales. Con este instrumento legislativo el país busca organizar y darle mayor robustez a la reunión de pruebas digitales extraídos mayormente de internet.

Francia, por su parte en 2006, aprobó una legislación contra el terrorismo que promueve los efectos de las investigaciones relacionadas con el terrorismo. El foco de la iniciativa hace referencia en la vigilancia de las comunicaciones y el acceso de las fuerzas de seguridad a los datos de comunicaciones de las compañías telefónicas, los proveedores de internet y sobre aquellos lugares de acceso libre a la web como pueden ser bares, cafés, estaciones de trenes y numerosos espacios públicos que suman la provisión del acceso gratuito y a través del cual potenciales terroristas podrían usar.

La ley francesa de lucha contra el terrorismo especifica que los proveedores de servicios de internet, los proveedores de hospedaje y las compañías telefónicas deben informar los metadatos sobre el tráfico. Los números llamados y las direcciones IP involucradas en cada comunicación a los organismos gubernamentales especializados. Esta información no debe ser masiva, sino sólo en casos relacionados con la investigación de presuntas actividades terroristas.

Según el artículo 6, las compañías de telefonía móvil y aquellos lugares donde ofrecen internet a sus clientes deben llevar un registro preventivo de las conexiones de clientes durante 12 meses y ponerlo a disposición de la policía en los casos que lo requieran. También la legislación autoriza el uso de cámaras de videovigilancia en espacios públicos, como estaciones de colectivos y trenes, iglesias y mezquitas, negocios, fábricas y centrales nucleares. El artículo 8 autoriza a la policía a monitorear de forma automática a vehículos y ocupantes en las rutas y autopistas francesas (permitiéndose incluso registrar datos tales como imágenes del número de dominio del vehículo e imágenes de los ocupantes del vehículo). La vigilancia preventiva no queda ahí, también la ley permite el monitoreo de los concurrentes en grandes reuniones o espectáculos públicos.

En 2011, el Código de Procedimiento Penal fue modificado para otorgar nuevas facultades a los organismos a cargo de las investigaciones de atentados terroristas. Estos permisos incluyen el derecho a incautar todos los documentos necesarios para la investigación en curso. Pueden recolectar y archivar datos de computadoras, descifrar datos informáticos protegidos, proceder a una infiltración digital, grabar datos informáticos como imágenes, videos, conversaciones y documentos, como así también acceder a escuchas telefónicas y la interceptación de otras comunicaciones que dichos dispositivos electrónicos les permitan.

También la ley establece un respaldo jurídico para las actividades de los funcionarios de fuerzas de seguridad o inteligencia que participan, con motivo de las investigaciones en curso vinculadas a terrorismo, participen en las discusiones en línea en salas de chat. Si bien para ello desarrollaran técnicas especiales que contemplen el uso de perfiles apócrifos, la ley les brinda protección legal ante reclamos por la ejecución de dichos perfiles y prácticas tendientes a esclarecer algun hecho, o llevar adelante una investigación con el fin de mitigar las acciones del terrorismo.

Cuando se investiga un delito en que se hizo uso de internet, en China, los reglamentos facultan a las fuerzas de seguridad a solicitar al proveedor de servicios de internet y al proveedor de comunicaciones por internet que suministren los documentos y datos datos necesarios para la investigación. Las empresas deben preventivamente y de manera obligatoria retener por ley durante 60 días dicha información por si es solicitada.

En Reino Unido, se establece un marco jurídico para regular cinco tipos de actividades de vigilancia permitidas para los organismos del gobierno, según la ley de reglamentación de los poderes de investigación del año 2000:

La primera es la Interceptación de comunicaciones, como sería pedir acceso al contenido de las comunicaciones telefónicas o electrónicas, como puede ser un mail o un WhatsApp. El segundo tipo de vigilancia permitida, la llamada Vigilancia

intrusiva donde se desarrollan por ejemplo una vigilancia encubierta en locales privados o vehículos a través de diferentes INTs.

Seguidamente la ley describe la Vigilancia dirigida, como sería la vigilancia secreta de un blanco identificado en el espacio público. Luego detalla el uso exclusivo de fuentes humanas en una acción encubierta lo que usualmente se le llama a la tarea que desarrollan los agentes encubiertos también entendido como HUMINT.

Finalmente en quinto lugar, se especifica el uso de metadatos, que son los datos sobre comunicaciones pero no su contenido. Quien llamó a quién a qué hora, quién le envió un WhatsApp a quién con qué frecuencia, qué duración tuvieron las llamadas, los puntos geográficos desde donde las antenas localizaban los dispositivos, etc[20].

En el caso de India en el año 2000, se aprobó la Ley de Tecnología de la Información, modificada luego en 2008, y que establece el delito de “terrorismo cibernético” (artículo 66F).
La misma legislación trata la retención de los datos y dispone que los proveedores de internet “deberán conservar y retener la información que pueda especificarse por el tiempo y en la forma y formato que prescriba el Gobierno central” y tipifica como delito con castigo de prisión el no hacerlo.

El artículo 69 le da poder a las autoridades de gobierno para solicitar “interceptación, monitorización y descifrado de la información generada, transmitida, recibida o almacenada en cualquier dispositivo informático”.

Mediante dicho artículo se establece las obligaciones y garantías jurídicas que deben acompañar a los actos estatales, mientras que el artículo 69A faculta a los organismos del Estado para dictar instrucciones de bloqueo del acceso del público por medios informáticos a toda información cuya supresión sea, a juicio de esos

[20] ***Fedotov, Yury,*** Uso de internet con fines terroristas, Oficina de las Naciones Unidas contra la droga y el delito, Viena, Austria, 2013.
https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

organismos, necesaria o conveniente, en aras de la soberanía, la integridad, la seguridad y las relaciones internacionales de la India, o para impedir la incitación a la comisión de delitos conexos “de competencia de un tribunal”, incluido el terrorismo.

Finalmente, el artículo 69B faculta a determinados organismos del Estado para monitorizar, reunir y almacenar datos de tráfico o la información generada, transmitida o recibida a través de cualquier dispositivo informático.

En Nueva Zelandia, la Ley de registro y vigilancia de 2012 actualiza, consolida y armoniza las facultades de los organismos encargados de hacer cumplir la ley para registrar, vigilar e interceptar comunicaciones a fin de hacer frente a las nuevas formas de tecnología. La Ley crea una nueva definición de la expresión “registros de sistemas informáticos”, que se hace extensiva al registro de computadoras que no están conectadas internamente, pero son capaces de acceder a una red a distancia.

Para dar robustez a las garantías jurídicas, la ley especifica que el registro de computadoras de acceso remoto está permitido sólo en dos situaciones:

1) Cuando una computadora tiene la capacidad de acceder legalmente a un sistema informático objeto del registro y, por tanto, es considerada parte de ese sistema.

2) Cuando no hay ningún lugar físico que registrar (por ejemplo, en el caso del correo electrónico, al que el usuario puede acceder desde distintos lugares, como los cibercafés).

En Israel, un país sumamente sofisticado en telecomunicaciones, en su artículo 13 de la Ley de Comunicaciones de 1982 establece que el Primer Ministro podrá ordenar a los proveedores de acceso a internet, dentro de Israel, que introduzcan las modificaciones tecnológicas que requieran las fuerzas de seguridad (que, según se definen, incluyen los servicios de policía, de seguridad y otros servicios especiales) para los fines de la lucha contra el terrorismo.

Si bien la legislación se aplica solamente a proveedores de acceso a internet, que reciben sus licencias por parte del Ministerio de Comunicaciones, no se aplica a los proveedores de servicios de almacenamiento de datos o de servicios de gestión de contenido que operan en Israel, ya que estos proveedores no necesitan licencia de dicho Ministerio.

Como mencionamos anteriormente, en Nueva Zelandia, la Ley de telecomunicaciones (capacidad de interceptación) de 2004 precisa las obligaciones de los operadores de redes de asistir a los organismos oficiales autorizados en la ejecución de operaciones de interceptación o la entrega autorizada de datos asociados a llamadas.

Se los obliga a garantizar que todas las redes públicas de telecomunicaciones o de servicios que poseen, controlan o mantienen en funcionamiento tengan capacidad de interceptación. Se considera que las redes o los servicios tienen esta capacidad cuando los organismos oficiales autorizados pueden interceptar las telecomunicaciones o los servicios de manera tal que se identifiquen e intercepten solo las telecomunicaciones objeto de investigación, se suministren los datos asociados a llamadas y los contenidos de estas (en una forma utilizable) y permitan una interceptación discreta, oportuna y eficiente de manera que proteja la privacidad de otros usuarios de las telecomunicaciones y evite una injerencia indebida. Acciones que en los hechos, probablemente no son tan sencillas de armonizar.

En el caso de Brasil, la Ley Federal 9.296 de 1996, junto con el artículo 5 (XII) de la Constitución Federal de 1988, regula las escuchas telefónicas por los organismos oficiales autorizados. Si bien reconoce que es inviolable el secreto de las telecomunicaciones, la Ley prevé, con sujeción a una orden judicial, casos específicos de suspensión de este principio para fines de investigación criminal o instrucción penal. La Ley establece los procedimientos que han de seguirse en casos de escuchas telefónicas, que se realizan bajo la supervisión de un juez. Una vez ejecutada la intervención telefónica, se transcriben los resultados, que se

entregan al juez, junto con un resumen de todas las medidas adoptadas en virtud de la autorización.

Las empresas de telecomunicaciones se han visto en la necesidad de establecer y capacitar unidades especializadas e invertir en la tecnología necesaria para cumplir con la legislación. En cuanto al costo de adquirir capacidad de recolección de estos datos, corresponde a las empresas de telecomunicaciones proporcionar el personal y los recursos técnicos necesarios para prestar apoyo a las actividades autorizadas de interceptación. Este caso refleja el hecho de que, por imposición de la Constitución de Brasil, las empresas brasileñas de telecomunicaciones operan un servicio público, concesionado por el gobierno, que cumplido determinado plazo y condiciones debe volver a ser operado por el Estado, eventualmente. Pero en sí es la operación de un bien público, como puede ser el espacio radioeléctrico, o bien el servicio público sobre el que los ciudadanos tienen derechos.

Otros Estados, como el de Indonesia, que a raíz de los atentados de Bali de 2002, aprobó legislación antiterrorista que dota a los organismos de aplicación de la ley y de seguridad, a los efectos de las investigaciones relacionadas con el terrorismo, a interceptar y examinar la información que se expresa, envía, recibe o archiva por medios electrónicos o con un dispositivo óptico.

En Argelia, en 2006, se aprobó una ley que permite la vigilancia de video y micrófono y la interceptación de correspondencia, si están autorizadas y se ejecutan bajo supervisión directa del fiscal. La misma ley autoriza la técnica de infiltración con el fin de investigar el terrorismo o la delincuencia organizada y permite que el agente cometa, en el curso de la infiltración, infracciones leves especificadas. El secreto de la identidad del agente está cuidadosamente protegido por la ley, pero la infiltración debe llevarse a cabo bajo la autoridad del fiscal o del juez de instrucción.

En Malasia, la Ley de las Comunicaciones y Multimedia de 1998 contiene varias disposiciones relativas a la regulación de las investigaciones de internet e investigaciones penales conexas. Por ejemplo, el artículo 249 de la Ley, que trata de la cuestión del acceso a los datos informáticos durante los registros, establece que

el acceso incluye la obtención de “contraseñas, claves de cifrado o descifrado, software o equipo y demás medios necesarios para permitir la comprensión de los datos informáticos”.

En EE.UU., las empresas de telecomunicaciones deben, desde 1994, proporcionar capacidad de interceptación en las redes de telefonía y banda ancha en todo el país.

Control del contenido

La cuestión de la medida en que los gobiernos deben regular los contenidos relacionados con el terrorismo en internet es muy discutible. Los enfoques varían considerablemente, y en tanto que algunos Estados aplican a internet y a otros proveedores de servicios conexos estrictos controles reglamentarios, recurriendo incluso en ciertos casos al uso de tecnología para filtrar o bloquear el acceso a algunos contenidos, otros adoptan un enfoque reglamentario más liberal, confiando en mayor medida en la autorregulación del sector de la información.

En el artículo “Terrorism and the internet: should web sites that promote terrorism be shut down?” (El terrorismo e internet: ¿deberían cerrarse los sitios web que promueven el terrorismo?), Barbara Mantel observa que “la mayoría de los proveedores de servicios de internet, empresas de hospedaje de sitios web, de intercambio de ficheros y de redes sociales tienen acuerdos de condiciones de servicio que prohíben determinados contenidos”. Por ejemplo, señala, el servicio de hospedaje de sitios web para pequeñas empresas comerciales, de Yahoo, prohíbe expresamente que los usuarios utilicen el servicio para proporcionar apoyo o recursos materiales a cualquier organización u organizaciones designadas por el Gobierno de los Estados Unidos como una organización terrorista extranjera. En ese sentido, hay cierta medida de autorregulación en la sociedad de la información.

Al evaluar el enfoque y el nivel de intervención en esta esfera, los gobiernos deben tener en cuenta una serie de factores, incluidos el lugar donde se hospeda el

contenido, las garantías constitucionales o de otra índole relacionadas con el derecho a la libertad de expresión, el contenido mismo y las consecuencias estratégicas, desde el punto de vista de los servicios de inteligencia o de aplicación de la ley, de monitorizar ciertos sitios o de infiltrarse en ellos o de hacerlos inaccesibles.

En el Reino Unido, el artículo 3 de la Ley de Terrorismo de 2006 contiene un recurso innovador, a disposición de las autoridades que se ocupan de los casos de posibles actos de incitación por internet, que faculta a la policía para emitir una notificación de retiro ("take down" notice) a las personas asociadas con el funcionamiento de sitios web o con otros contenidos de internet.

El artículo 3 de la Ley se aplica a los casos de delitos tipificados en los artículos 1 y 2 de esa Ley en que "a) se publica, o se hace publicar, una declaración en el curso de, o en conexión con, la prestación o el uso de un servicio prestado por vía electrónica, o b) se realizan actos comprendidos dentro del ámbito de aplicación del artículo 2 2) [difusión de una publicación terrorista] en el curso de, o en conexión con, la prestación o el uso de dicho servicio".

El artículo 3 2) establece que, si la persona a la que se ha hecho la notificación no retira el contenido relacionado con el terrorismo, y si es posteriormente acusada de delitos en virtud de los artículos 1 o 2 de la Ley de Terrorismo de 2006 en relación con dicho incumplimiento, se podrá hacer en el juicio una presunción juris tantum de que el contenido en cuestión tenía su aprobación.

A pesar de la disponibilidad de estas notificaciones de retiro como medida preventiva, en la práctica esta facultad no se ha usado todavía. En la mayoría de los casos, especialmente cuando el contenido ofensivo está hospedado en sitios web de terceros, tiende a contravenir los términos y condiciones de servicio del proveedor, de modo que las autoridades pueden negociar con éxito la eliminación del contenido prohibido.

En el Reino Unido, la unidad especializada en derivaciones, en la lucha contra el uso de internet por terroristas, coordina las respuestas nacionales a las denuncias del público, así como del Gobierno y del sector de las comunicaciones, de contenidos de internet relacionados con el terrorismo y actúa como centro especial de asesoramiento de la policía.

En Ecuador, también el gobierno ha contratado a una firma española, Ares Rights, durante el gobierno del presidente Correa, con el fin de denunciar por la vía legal todos aquellos contenidos que por su contenido ofensivo o amenazante puedan ser requeridos a las empresas de internet y de redes sociales para su baja definitiva. Este mecanismo muchas veces recibe críticas por parte de las ONGs, que ven en este accionar legal una instigación sobre la libertad de expresión de la sociedad.

Reunión de inteligencia

La reunión de inteligencia es un componente clave de las actividades de lucha contra el terrorismo, pues la información obtenida de este modo muchas veces pone en marcha investigaciones que llevan al enjuiciamiento de los sospechosos, o se utiliza como prueba en el juicio, en la medida permitida por la legislación y las normas de procedimiento nacionales. Sin embargo, las distintas finalidades para las que se reúne la inteligencia, y los diferentes organismos que pueden obtener o utilizar esta información, pueden obligar a buscar el justo equilibrio entre intereses en conflicto. Por ejemplo, los servicios de policía o de inteligencia dedicados a la obtención de inteligencia pueden hacer especial hincapié en la protección de la confidencialidad de la fuente de la información, mientras que los funcionarios judiciales tendrán que considerar, entre otras cosas, el derecho del acusado a un juicio imparcial y a un acceso igual a las pruebas presentadas en su contra. Se debe poner el debido cuidado en asegurarse de que haya un sistema de control adecuado para proteger los derechos humanos fundamentales consagrados en las convenciones internacionales aplicables.

En algunos Estados Miembros, la inteligencia procedente de fuentes anónimas no es admisible como prueba en los tribunales; sin embargo, los datos de inteligencia corroborados por fuentes autorizadas o por otras pruebas pueden admitirse. Por ejemplo, en Irlanda, los datos de inteligencia reunidos sobre terroristas pueden constituir indicios racionales de que una determinada persona es miembro de una organización ilegal cuando esos indicios son presentados bajo juramento por un funcionario policial con un rango de al menos comisario principal.

Retención de los datos

Varios Estados Miembros han introducido recientemente, o se proponen introducir, legislación por la cual se exige a los proveedores de servicios de telecomunicaciones que capturen y archiven de forma automática los datos de las comunicaciones de sus usuarios. En 2006, impulsada en parte por los ataques terroristas de Madrid en 2004 y Londres en 2005175, la Unión Europea aprobó una directiva sobre la retención obligatoria de los datos de tráfico de las comunicaciones (Directiva 2006/24/CE del Parlamento Europeo y del Consejo de la Unión Europea, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE)176. La Directiva 2006/24/CE reconoce las dificultades causadas por las diferencias legales y técnicas entre las disposiciones nacionales relativas a los tipos de datos que deben retenerse, así como en cuanto a las condiciones y los períodos de retención de los datos. Por tanto, la Directiva tiene por objeto armonizar las obligaciones mínimas de retención de datos de los proveedores de servicios de comunicaciones electrónicas que operan en los Estados miembros de la Unión Europea para fines de prevención, investigación, detección y enjuiciamiento de delitos[21].

[21] ***Fedotov, Yury,*** Uso de internet con fines terroristas, Oficina de las Naciones Unidas contra la droga y el delito, Viena, Austria, 2013.

https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

La Directiva 2006/24/CE obliga a los Estados miembros a adoptar legislación que exija a los proveedores de telecomunicaciones retener determinados datos de tráfico relativos a las comunicaciones electrónicas durante un período de entre seis meses y dos años. Estos datos de tráfico incluyen la información necesaria para identificar al iniciador y al destinatario del correo y de las comunicaciones de telefonía de internet, junto con información sobre la hora, la fecha y la duración de las comunicaciones electrónicas, pero no se extiende a su contenido. Estos datos deben ponerse a disposición, en relación con la investigación, la detección y el enjuiciamiento de delitos graves, de las autoridades policiales nacionales y, por conducto de las autoridades nacionales, de sus homólogos de otros Estados miembros de la Unión Europea, de acuerdo con los requisitos de la legislación nacional respectiva.

Algunos Estados miembros de la Unión Europea han indicado que los registros de retención de datos son el único medio de investigar ciertos delitos que entrañan la comunicación por internet, tales como los anuncios en salas de charla, que pueden rastrearse solo a través de los datos de tráfico de internet. Varios Estados miembros de la Unión Europea también han informado del uso de datos retenidos por los proveedores de servicios para exculpar a personas de quienes se sospechaba la comisión de delitos sin tener que recurrir a otros métodos de vigilancia más intrusivos, tales como la interceptación y los registros domiciliarios.

Sitios web y otras plataformas que hospedan contenido generado por los usuarios

Los contenidos relacionados con el terrorismo hospedados en sitios web populares que presentan material generado por el usuario tienen la posibilidad de llegar a un público mucho más amplio que el contenido de los sitios web tradicionales, tableros de anuncios y foros web especializados, que generalmente atraen a un grupo de personas autoseleccionado. Según el sitio web de intercambio de videos YouTube,

cada minuto los usuarios suben a ese sitio 48 horas de videos generados por usuarios, lo que equivale a casi ocho años de contenido cargado por día. El hecho de poder llegar, según se estima, a ocho millones de usuarios de YouTube al mes, usuarios únicos por sus características, reduce considerablemente las barreras para el acceso a contenidos relacionados con el terrorismo. El fuerte aumento de la popularidad de los contenidos generados por usuarios en los últimos años acrecienta la dificultad logística de monitorizar los contenidos relacionados con el terrorismo.

Algunos sitios web y plataformas de medios sociales también incluyen disposiciones en sus condiciones de uso que prohíben el uso de sus servicios para promover, entre otras cosas, las actividades terroristas. Por ejemplo, las condiciones de servicio de Twitter, red de información en tiempo real, prohíbe el uso del servicio para la publicación de amenazas directas y específicas de violencia contra terceros o para cualquier propósito ilegal o en apoyo de actividades ilícitas. En caso de incumplimiento de dichas condiciones, el proveedor de servicios se reserva el derecho (aunque no está obligado a hacerlo) de eliminar o rechazar la distribución de contenido ofensivo o interrumpir el servicio. Además, no pueden ser usuarios de Twitter los que tengan prohibido recibir servicios con arreglo a las leyes de los Estados Unidos o cualquier otra jurisdicción aplicable, lo que excluye el uso de sus servicios por parte de organizaciones designadas como terroristas. Sin embargo, aun cuando existan esas condiciones, pueden surgir dificultades en la aplicación, debido en parte a la amplia base de usuarios y el alto volumen resultante de contenido generado por usuarios que hay que monitorizar.

Varios países han tipificado específicamente los actos de incitación o glorificación del terrorismo, mientras que otros se basan en los actos delictivos preparatorios como la instigación o la asociación ilícita, con el fin de darle un marco de protección legal a los derechos humanos que se puedan potencialmente vulnerar.

No es menor considerar que las técnicas de investigación en internet que los organismos policiales o de inteligencia de los estados, deben estar debidamente autorizadas por las leyes nacionales y emplearse de manera que se respeten los

derechos humanos fundamentales protegidos por las normas internacionales de derechos humanos.

Si bien los Estados necesitan la cooperación de las empresas de telecomunicaciones cuando recurren a la monitorización electrónica, las escuchas telefónicas y técnicas similares de investigación electrónica, es aconsejable que se les proporcione una base jurídica clara para las obligaciones y especificidades técnicas de la recolección de los datos.

La cooperación internacional a través de instrumentos legales de acuerdos entre paises es siempre un insumo necesario en muchos juicios de actos de terrorismo debido a su característica global. También sería de mucha útilidad llegar a un consenso para la aplicación de una legislación global en la materia, pero este hecho encuentra siempre discrepancias basadas en desiciones gopoliticas, donde el terrorismo lamentablemente es un factor más dentro de los intereses estratégicos de algunos estados sobre otros.

La legislación nacional de protección de datos o sobre privacidad restringe con frecuencia la capacidad de los servicios de policía y de inteligencia para compartir información con los homólogos tanto nacionales como extranjeros. El logro de un equilibrio razonable entre el derecho humano a la privacidad y el interés legítimo del Estado de investigar y perseguir los delitos es un problema permanente para los gobiernos y, en algunos casos, en particular los que entrañan respuestas al terrorismo, este conflicto de intereses ha sido motivo de preocupación.

En muchos casos de terrorismo, las pruebas presentadas por la fiscalía se basan en la inteligencia reunida. La integración de las actividades de inteligencia en los sistemas de justicia penal sigue siendo un problema fundamental para las autoridades que combaten el terrorismo, o, dicho de otro modo, ¿cómo pueden las autoridades proteger la confidencialidad de la inteligencia en que se basan las pruebas al tiempo que cumplen sus obligaciones de garantizar un juicio imparcial y una defensa eficaz de los acusados, incluida la obligación de revelar todos los elementos importantes de la acusación a la defensa?

En los casos de terrorismo en que se usan computadoras o internet, las pruebas digitales son parte importante de la acusación. El uso de tales pruebas invariablemente da lugar a cuestiones relacionadas con la admisibilidad. Es de suma importancia proceder con extremo cuidado durante toda la investigación y el enjuiciamiento del caso para asegurarse de que los métodos de obtención, conservación, análisis y presentación de las pruebas digitales estén en plena conformidad con las normas pertinentes respecto de las pruebas o los procedimientos y sigan las buenas prácticas establecidas.

CAPÍTULO 2

EXPERIENCIAS Y ESTADO DE SITUACIÓN SOBRE LA PROTECCIÓN DE DATOS PERSONALES EN PAÍSES DE LA REGIÓN Y EL MUNDO

En esta parte se presenta el estado de situación a nivel regional y global en relación a los últimos avances en materia de protección de datos personales. El abordaje releva las regulaciones actuales, así como eventuales proyectos de ley que intentan abordar los nuevos desafíos en la materia.

Concepto

La protección de datos personales, como concepto, abarca a todas aquellas acciones, mayoritariamente promovidas o reguladas por el Estado, con el fin de velar por los derechos de los titulares de los datos personales de un país o una región.

Regulaciones Internacionales

A nivel internacional existen dos grandes líneas de regulación en lo que hace a las protección de los datos personales, las regulaciones europeas y las norteamericanas. No obstante coexisten al mismo tiempo países con legislaciones más desarrolladas que otras, culturas y ciudadanías con mayor y menor nivel de trabajo en la materia. En esto la idiosincracia, el modelo de gobierno y hasta sus acuerdos geopolíticos son una influencia en las ideas que sostiene cada nación en la temática.

Estándar internacional

La Organización Mundial de Normalización, pos sus siglas en inglés ISO (International Organization for Standardization), presentó en 2007 la norma ISO/IEC 29100 que proporciona estándar global y voluntario para la protección de datos

personales dentro de los sistemas de tecnología de la información y la comunicación.

Esta norma muestra los requisitos que las organizaciones deberían cumplir para salvaguardar la privacidad en cualquier sistema en que se procese información vinculada a datos personales. Estas regulaciones pueden aplicarse, y así están diseñadas complementariamente con las legislaciones de cada país o región.

La ISO/IEC 29100 establece once principios para un mejor tratamiento de los datos personales:

1. *Consentimiento y elección:* Con este principio, el titular de los datos personales, puede escoger el procesamiento o no de sus datos. Además, se le brinda detalles sobre sus derechos de participación y acceso.
2. *Propósito de legitimidad y especificación:* Antes de que la información sea reunida, se le informa al titular el propósito del tratamiento de datos.
3. *Limitación de la recolección:* Debe ser limitada a las necesidades del propósito especificado.
4. *Minimización de datos:* Se aplica el criterio de borrar los datos que tengan propósitos expirados.
5. *Limitación de uso, retención y divulgación:* Se realiza de acuerdo a los propósitos explícitos, específicos y legítimos establecidos según la normativa local.
6. *Precisión y calidad:* Este principio busca que los datos procesados sean exactos, actualizados y relevantes para el propósito de uso.
7. *Franqueza, transparencia y aviso:* Proporciona al titular la información sobre las políticas de procesamiento de los datos.
8. *Participación y acceso individual:* Brinda facilidades al titular para que revise sus datos. También determina procedimientos para que los dueños de los datos logren ejercer sus derechos veloz y eficientemente.
9. *Responsabilidad:* Entre varias medidas, se establece informar al titular en el caso de que surja una brecha de seguridad que perjudique sus datos.

10. *Seguridad de información:* Establece controles operativos, estratégicos y funcionales con el fin de garantizar la confidencialidad e integridad de los datos personales.
11. *Cumplimiento de privacidad:* Mediante auditorías periódicas, se hace una verificación de todos los niveles de protección de los controles de seguridad.

Convenio 108

La Argentina suscribió desde junio de 2019 al "Convenio 108"[22]. Actualmente el único instrumento multilateral de carácter vinculante sobre protección de datos personales del mundo, que tiene como objetivo proteger la privacidad de las personas contra abusos en el tratamiento de sus datos personales.

Esta herramienta a la que adhirió nuestro país, convirtiéndose en el miembro N°54 en suscribir, proporciona mayor seguridad jurídica y previsibilidad sobre las relaciones internacionales al garantizar por parte de sus miembros la puesta en práctica de medidas en cada legislación nacional donde se apliquen los principios del Convenio 108.

El Convenio también fue firmado en conjunto con un "Protocolo Adicional", que amplía la base de derechos de los titulares de los datos al requerir que cada Estado miembro designe una autoridad independiente que vele por las garantías de la protección de los datos personales a la vez que fija normas sobre cómo deben realizarse los flujos de datos personales transfronterizos.

[22] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Consejo de Europa, Serie de Tratados Europeos N° 108, Estrasburgo, 1981. https://rm.coe.int/16806c1abd

Regulaciones en UE

El 25 de mayo de 2018 comenzó a regir en la Unión Europa el Reglamento General de Protección de Datos, (GDPR, por sus siglas en inglés), sancionada en 2016 por el parlamento europeo, dicha legislación es obligatoria para todas las empresas del continente, pero también impacta sobre los gigantes tecnológicos como Google, Amazon y Facebook, y sobre cualquier compañía que maneje datos personales de ciudadanos europeos, en cualquier parte del mundo.

La nueva legislación llegó a conocimiento de muchos de nosotros por los contactos que las compañías efectuaban vía email, donde informaban de una nueva política de términos y condiciones del servicio, justamente adecuándose a los cambios de la normativa europea.

Mediante este cambio, los usuarios pueden objetar la captura de sus datos personales para su utilización con fines publicitarios o propagandísticos, también disponen de un pleno derecho a la portabilidad de sus datos, pudiendo mover los mismos de un servicio a otro.

Las empresas y organizaciones que almacenen datos personales de europeos, deberán crear, en los términos que la norma lo establece, el puesto de Oficial de Protección de Datos (DPO en inglés). La función de esta persona será la de asegurar que los datos de los usuarios estén debidamente resguardados y que la organización cumpla con las reglamentaciones.

Otro punto alto de la nueva normativa europea es el que viene de la mano de las sanciones económicas. Si una compañía incumple la ley podría pagar multas de hasta veinte millones de euros o el 4% de sus ingresos anuales, lo que sea mayor. Es decir que si Google la incumpliera debería erogar 3.600 millones de euros, o si Facebook lo hiciera debería pagar una suma cercana a los 1.300.

Este factor ejerce una presión importante para las compañías que, desde hace tiempo, están revisando sus prácticas para que este cambio no las afecte

vitalmente. Microsoft, por ejemplo, desde hace dos años destina un equipo de mil quinientos ingenieros para adecuar las actividades de la compañía a la nueva normativa, según declaró Alejandro Anderlic, director de Asuntos Corporativos y Legales de la compañía.

Facebook tuvo un año negro en este sentido después del escándalo de Cambridge Analytica. Su titular Mark Zuckerberg, no solo tuvo que dar explicaciones y reconocer “falencias” sobre la seguridad de los datos frente al congreso de los Estados Unidos, también anunció que la compañía, con más de dos mil millones de usuarios se acogería a la nueva normativa europea. No solo para sus usuarios de la comunidad sino para todos sus usuarios a nivel global.

Este terremoto político también tuvo impacto económico para la compañía ya que Facebook tuvo que pagar U$S 5.000 millones, aproximadamente la mitad de las ganancias netas de un año de la compañía, al estado norteamericano. Otra estrategia legal de la compañía fue la de migrar el domicilio fiscal de la organización de Irlanda a los Estados Unidos, donde las nuevas regulaciones norteamericanas podrían ser menos severas.

Fue comprobado que Cambridge Analytica no solo influyó en la elección de los Estados Unidos asesorando a al Partido Republicano de Trump, sino también a la iniciativa Brexit, que promovió la salida de Reino Unido de la Unión Europea y su influencia fue a través del uso no permitido de los datos sensibles de millones de personas para dirigirles campañas de propaganda, oficial y extraoficialmente. Aquellos datos que las legislaciones intentan proteger por sobre cualquier otro se vendieron como de manera simple y de forma oculta. La verdad a medias de la compañía y su supuesto *Mea culpa* llegó solo cuando ese secreto fue imposible de contener resguardado.

Reino Unido

El Reino Unido tiene desde 2018 una ley de Protección de Datos. Esta legislación precisa y regula cómo las organizaciones, las empresas o el gobierno utilizan la información personal. Es la implementación del Reglamento General de Protección de Datos (GDPR) del Reino Unido.

Según la ley, todos los responsables del uso de datos personales deben seguir reglas estrictas llamadas "principios de protección de datos". Deben asegurarse de que la información sea: utilizada de manera justa, legal y transparente; utilizada para fines específicos y explícitos; se use de manera adecuada, relevante y limitada solo a lo necesario; precisa y, cuando sea necesario, actualizada; mantenida no más de lo necesario; manejada de manera que garantice la seguridad adecuada, incluida la protección contra el procesamiento, acceso, pérdida, destrucción o daño ilegal o no autorizado.

Implica una protección legal más sólida para la información más sensible, como: carrera, origen étnico, opiniones políticas, creencias religiosas, afiliación sindical, genética, biometría (donde se usa para identificación), salud, vida sexual u orientación sexual.

Cabe destacar que existen salvaguardas separadas para los datos personales relacionados con condenas y delitos penales.

Según la Ley de Protección de Datos de 2018, las personas tienen derecho a averiguar qué información almacena el gobierno y otras organizaciones sobre éstas. Esto incluye el derecho a: estar informado sobre cómo se utilizan sus datos, acceder a datos personales, tener datos incorrectos actualizados, tener datos borrados, detener o restringir el procesamiento de sus datos, portabilidad de datos (que le permite obtener y reutilizar sus datos para diferentes servicios), objetar cómo se procesan sus datos en ciertas circunstancias.

También se tiene estos derechos cuando una organización utiliza sus datos personales para: procesos automatizados de toma de decisiones (sin participación humana), perfiles, por ejemplo para predecir el comportamiento de las personas o sus intereses.

Siguiendo con el contexto del Reino Unido, Según David Omand[23], los gobiernos deben comenzar respetando los derechos de privacidad de los ciudadanos y reconociendo que las intrusiones deben ser necesarias para fines definidos (seguridad nacional, prevención y detección de delitos graves) y el grado de intrusión debe ser proporcional al daño que se espera evitar.

De acuerdo al especialista, en el Reino Unido esto se conoce como 3R (en inglés):

Estado de derecho; ley actualizada para regular la recolección intrusiva de inteligencia, proporcionando transparencia al ciudadano en cuanto al efecto de la ley y con sanciones legales por uso indebido. Un tribunal independiente considera cualquier queja presentada por ciudadanos o grupos de la sociedad civil.

Regulación; con el Secretario de Estado (Secretario de Relaciones Exteriores para el Exterior y el Ministro del Interior a nivel nacional) firmando personalmente órdenes de arresto a granel sujetas a revisión judicial por un juez superior que actúa como Comisionado, quien con un equipo de inspectores asegura que el trabajo de las agencias permanezca dentro de la ley. Las solicitudes de datos de comunicaciones ahora son otorgadas por una oficina independiente bajo el Comisionado. La supervisión parlamentaria continúa por el Comité de Inteligencia y Seguridad del Parlamento, al que se le han otorgado poderes mejorados para obtener evidencia de las agencias.

Restricción; que requiere que, el uso por parte de las agencias de seguridad e inteligencia de los poderes coercitivos del Estado, para investigar la vida privada de

[23] David Omand, Ex Director del Government Communications Headquarters (GCHQ), organismo responsable de la recolección de inteligencia de señales (SIGINT) en Reino Unido, entre 1996 y 1997. Entrevistado el 17 de abril de 2020.

otros, se justifique como necesario y proporcionado. La evaluación de la proporcionalidad debe realizarse llevando a cabo un ejercicio de equilibrio en el que el potencial de daño a los demás de las operaciones se compara con los daños al público que están diseñados para evitar, por ejemplo, comprometer los derechos de privacidad de aquellos que no son objeto de investigación contra el salvamento de vidas y daños a la propiedad por la detención de terroristas y ataques cibernéticos. Debe existir una creencia razonable en el valor de la actividad, sobre la base de la experiencia o la investigación específica, para justificar el nivel de riesgo ético que pueda estar involucrado.

Regulaciones en los EE.UU.

En los Estados Unidos, las normativas que regulan la protección de datos personales son diversas y varían entre los estados. Si bien en general se entiende se trata de menores exigencias que en Europa, la autonomía de cada estado norteamericano sobre la protección de los datos y la privacidad de las personas hace que no haya una sola política pública para todo el país, así como acontece para otras regulaciones.

La cultura y diseño de las estructuras de poder en los Estados Unidos tienen el mismo criterio. Cada estado mantiene una autonomía pronunciada con el estado nacional en legislaciones, seguridad, economía, justicia y hasta incluso en cuestiones electorales.

A nivel nacional, según el informe anual de la ONG Alianza Regional (2016), la historia de la reglamentación sobre privacidad en los Estados Unidos se ha caracterizado por la autorregulación del sector y la legislación reactiva . “La naturaleza exacta y el alcance del derecho a la privacidad [en los Estados Unidos], sin embargo, nunca han sido enteramente definidos”[24].

[24] Barry contra N.Y., 712 F.2d 1554, 1558 (2d Cir. 1983).

Los representantes empresariales y quienes proponen incrementar el acceso a la información personal se apresuran a señalar los múltiples beneficios de la autorregulación y de un mayor acceso y uso de la información personal –como, por ejemplo, los números de seguridad social.

El acceso a bases de datos computarizadas que contienen información de identificación permite que los organismos obtengan datos sobre los individuos que, de otra manera, no podrían ser localizados. Algunos de estos beneficios son: posibilitar que las agencias de la ley ejecuten sentencias; que los grupos de interés público hallen a niños desaparecidos; que los bancos, compañías de seguros y de crédito prevengan el fraude; que los periodistas brinden información precisa; que los abogados localicen a testigos e identifiquen a las partes involucradas; y que los ciudadanos encuentren a sus familiares perdidos.

Contrariamente, hay quienes exigen una mayor protección de la información personal (incluso en los registros públicos) en vista del rápido desarrollo de las redes computarizadas y de internet. Dada la facilidad con que la información se puede obtener, compartir y difundir a amplia escala geográfica, es factible que los errores sean replicados o magnificados, y así se dañe a un individuo por tiempo indefinido.

La promulgación, por parte del Congreso, de la Ley de Gobierno Electrónico de 2002[25] es sólo un ejemplo de la reacción del Gobierno de los EE.UU. a los reclamos del público por mayores medidas de privacidad. La Sección 205(c)(3) requiere que la Corte Suprema de los EE.UU. establezca reglas “para proteger la privacidad y la seguridad en cuestiones relacionadas con la clasificación electrónica de documentos y la disponibilidad pública de los documentos clasificados por medios electrónicos”.

Por otro lado, cada empresa que opere en el país depende del estado en el que radique su casa matriz para definir qué requisitos se le exigirán en materia de

[25] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 44 U.S.C.A. § 101.

protección de datos personales. Por ejemplo, el estado de California en 2018 aprobó la Consumer Privacy Act (CCPA). Una normativa que está casi a los niveles de exigencia que el Reglamento General de Protección de Datos (RGPD) europeo. No es menor que haya sido California ya que en su territorio se encuentra Sillicon Valley, en la bahía de San Francisco, que aloja las sedes de muchas compañías globales de tecnología.

Los estados de Arizona y de Vermont también han incluido modificaciones en las leyes relativas a datos personales, exigiendo un nuevo sistema de notificación en caso de fallo de seguridad o bien mayor transparencia a quienes tratan con información personal de los usuarios. Ninguno tan exigente como el caso de California, pero sí la tendencia es elevar la vara sobre los requisitos para las empresas.

De todas maneras, la RGPD europea fue una ley que condicionó el manejo de los datos personales en todo el mundo porque independientemente de dónde se encuentre la empresa, si recoge o trata información personal de ciudadanos de la Unión Europea, es imprescindible que cumpla con los requerimientos del Reglamento General de Protección de Datos.

Con respecto a los actores que influencian estas medidas, en los Estados Unidos uno de los más relevantes es la Comisión Federal de Comunicaciones (FCC), una agencia estatal independiente, bajo responsabilidad directa del Congreso. La FCC fue creada en 1934 con la Ley de Comunicaciones y es la encargada de la regulación de telecomunicaciones interestatales e internacionales por radio, televisión, redes inalámbricas, teléfonos, satélite y cable.

Otros actores con intereses potentes sobre el tema son el Departamento de Comercio, que trabaja en diseñar el marco legislativo que regule la recogida y el tratamiento de datos y las empresas prestatarias de internet conocidas como *internet service providers (ISP).*

Estas últimas recibieron mayor flexibilidad por parte del Congreso, al revocar en marzo de 2018 una normativa anterior creada durante el gobierno de Obama que las condicionaba y regulaba con mayor rigurosidad.

La normativa obligaba a tener el consentimiento de sus usuarios antes de compartir su información personal con terceros. Actualmente, se permite a las empresas de telecomunicaciones vender todo tipo de datos de los internautas, desde su historial de navegación, hasta su localización, el registro del uso de aplicaciones o el tipo de dispositivo desde el que usan la red, entre otros.

También los Estados Unidos cuentan con leyes específicas relacionadas a la protección de datos personales. Algunas de ellas son: La Ley de Transferencia y Responsabilidad de Seguro Médico, (Health Insurance Portability and Accountability Act, HIPAA por sus siglas en inglés), de 1996 por el Congreso de los Estados Unidos y firmada por el Presidente Bill Clinton. Dicha normativa mejora la portabilidad de la cobertura del seguro médico y simplifica la administración de la atención médica.

Asimismo obliga a todas las empresas de sanidad a cumplir de forma efectiva las garantías administrativas, técnicas y físicas necesarias para proteger la privacidad de la información y mantener la integridad de los datos de los empleados, los clientes y los accionistas[26].
Volviendo al contexto, las legislaciones más importantes vinculadas a información personal en los Estados Unidos son: La Ley de Libertad de la Información (Freedom of Information Act FOIA) de 1966 y la Ley de Privacidad (Privacy Act) promulgada en 1974.

---

[26] **Health Information Privacy for Consumers**, Department of Health and Human Services. https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html (Consultado última vez: 30/04/2019).
Comments on FACTA disposal rule: Disposal of consumer report information and records. https://www.privacyrights.org/blog/comments-facta-disposal-rule-disposal-consumer-report-information-and-records (Consultado última vez: 30/04/2019).
Children's Online Privacy Act, Federal Trade Commission. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (Consultado última vez: 30/04/2019).

La primera, la ley de Libertad de Información, busca “asegurar una ciudadanía informada, vital para el funcionamiento de una sociedad democrática, necesaria para controlar la corrupción y exigir que los gobernantes rindan cuentas a sus gobernados”.

La ley establece el acceso presunto de toda persona a registros gubernamentales, existentes o inéditos, sobre cualquier tema. Constituye la vía principal para que los individuos obtengan acceso a los registros de dependencias federales. El Congreso intentó así crear un sistema de monitoreo para que el público pudiera controlar a los organismos públicos a través de los documentos que estos publican.

Los legisladores asumieron que, si el gobierno se veía obligado a brindar información al público, entonces no excedería las limitaciones legales al recolectar y usar información personal. Para cumplir con este objetivo, la ley requiere que las agencias gubernamentales hagan públicos sus registros ante la solicitud de un individuo.

Este estatuto se aplica a todos los registros compilados por entidades del gobierno federal, e incluye la información en formato electrónico. La ley reconoce, no obstante, la necesidad de salvaguardar la información personal, y protege la privacidad restringiendo el acceso o eximiendo registros públicos en determinadas instancias (ONG Alianza Regional, 2016).

La ley de Libertad de Información señala nueve categorías de registros sobre los que se marcan ciertas restricciones vinculados a la seguridad nacional y sobre temas sensibles para los intereses del país. Entre ellas se destacan:

1. Información sobre defensa nacional o para fines de política exterior, clasificada adecuadamente como secreta según criterio establecido por orden del Ejecutivo.
2. Información relativa únicamente a reglas de manejo y prácticas del personal interno de los entes gubernamentales.

3. Datos específicamente eximidos de su divulgación por medio de un estatuto que requiera evitar la revelación de tales asuntos de modo no discrecional, o que establezca un criterio determinado para que permanezcan ocultos, o que refiera a tipos particulares de asuntos que deben permanecer ocultos.
4. Secretos industriales o información financiera o comercial privilegiada o confidencial que haya sido obtenida de una persona.
5. Memorandos y cartas entre, o al interior de, entidades gubernamentales que legalmente no estarían disponibles, excepto a pedido de otra agencia en un litigio.
6. Archivos del personal y archivos médicos o similares cuya divulgación constituye una invasión injustificada de la privacidad personal.
7. Ciertos tipos de registros de investigación recopilados con el fin de asegurar el cumplimiento de la ley.
8. Cierta información referida a la regulación de las instituciones financieras.
9. Información y datos geológicos y geofísicos

La ley de Privacidad (1974), amplía los derechos que establece la ley de Libertad de la Información, protegiendo los datos personales en base de datos federales. Se dan medidas de prevención ante un posible uso indebido de las bases de los organismos públicos nacionales, buscan regular los derechos del gobierno de tener información sobre las personas y el derecho de las personas de proteger su privacidad.

Existen diez categorías de información eximidas de acceso al público:

1. Información recopilada con razonable antelación a acciones o procedimientos civiles; excepción directa (autoejecutable).

2. Registros de la Agencia Central de Inteligencia (CIA por sus siglas en inglés): información concerniente a registros poligráficos, fuentes y métodos para obtener información de inteligencia –incluyendo las instalaciones, organización, funciones, nombres, títulos oficiales, salarios o números del

personal empleado por el organismo– y documentos o información provistos por gobiernos extranjeros.

3. Registros de los organismos de aplicación del derecho penal recopilados durante el curso de un procedimiento de aplicación de la ley y que se relacionen directamente con las funciones específicas del organismo.

4. Información clasificada por orden del Poder Ejecutivo en interés de la defensa nacional o la política exterior.

5. Registros de aplicación del derecho civil; registros de organismos de aplicación del derecho penal que no se relacionan directamente con las funciones específicas del organismo; la cobertura es menos amplia allí donde el individuo haya sido privado de un derecho, privilegio o beneficio como resultado de la información buscada.

6. Información pertinente a la protección del Presidente de los Estados Unidos u otros individuos según lo establecido en la sección 3056 del Título 18.

7. Información recolectada y utilizada únicamente con fines estadísticos y requerida por ley.

8. Material de investigación utilizado únicamente para determinar la idoneidad, elegibilidad y calificaciones de los potenciales empleados civiles de organismos federales, o el acceso a información clasificada cuando el material proviene de fuentes confidenciales.

9. Material de evaluación utilizado para decidir el nombramiento o promoción de empleados federales, siempre y cuando su divulgación comprometa la objetividad y equidad del proceso.

10. Registros de evaluación militares.

Los especialistas de la ONG Alianza Regional (2016), consideran poco probable que se llegue a un consenso entre los defensores de la autorregulación y los ciudadanos por una mayor regulación gubernamental. El gobierno norteamericano y el Poder Judicial, buscan regular esa tensión entre el derecho a la privacidad y el derecho de acceso a la información.

China

En el país asiático, los temas relacionados a datos personales y, por lo tanto, a información están siempre antecedidos muy fuertemente por criterios de ciberseguridad en relación a ciberterrorismo y vulneraciones que otros estados puedan ejercer sobre China.

A finales de 2017 el gobierno chino presentó un anteproyecto conocido como “Ley de supervisión”. El mismo establece protocolos de control sobre todos los datos que circulan dentro del país y entre el país y el extranjero dándole al Estado un poder omnipotente, violando parámetros internacionales sobre Derechos Humanos y la libertad de expresión.

La “Ley de Supervisión”, más allá de haber recibido críticas, fue aprobada y puesta en funcionamiento en 2018 por la Asamblea Popular China (órgano legislativo), estipulando dos años hasta su implementación total. Con la ley se creó una Comisión de Supervisión con jerarquía constitucional superior al Tribunal Supremo Popular y a la Fiscalía General. Sin mecanismos de control externos deja a un lado las instituciones judiciales.

La implicación de este sistema en las libertades sociales son para nuestra cultura difíciles de comprender. Según el nuevo sistema, se les permite a los organismos de supervisión detener e interrogar a personas de la administración pública o del

partido comunista durante un período de hasta seis meses, sin obligación de informar a sus familias, ni de brindarles asistencia legal alguna[27].

A pesar de las implicancias que genera la ley sobre la comunidad, desde el gobierno argumentan que es el modo de proteger la privacidad de los datos y reducir las vulnerabilidades ante ciberataques, y destaca entre sus puntos positivos cierta regulación de la protección de los datos personales al prohibir a los proveedores de servicios de internet recabar y vender sin autorización la información personal de sus usuarios, además de otorgar a sus clientes el derecho de reclamar que se borren sus datos en caso de uso abusivo.

La ley prohíbe a los usuarios de internet publicar contenido que perjudique “el honor nacional” o con intenciones de “deponer el sistema socialista”, como así también contenido que busque “alterar el orden social o económico” del país.

Las empresas extranjeras que operan sobre sectores que la ley denomina “claves” son blancos de un control diario sobre sus datos, además de exigirles el almacenamiento de los mismos en servidores en territorio chino. Los sectores claves pueden ser diversos, ya sea energía, finanzas, servicios públicos, pero también “cualquier otra infraestructura de información clave que pueda causar graves daños a la seguridad nacional, la economía o el interés público, si se destruyeran, quedarán inutilizadas o se filtraran”, es decir que casi cualquier sector sería objetivo del control estatal.

Según el gobierno “Más de 10.000 sitios web chinos se ven manipulados cada mes y cerca de un 80% de los sitios gubernamentales han sufrido ataques, muchos de ellos originados en Estados Unidos”. Es por eso que el tema de datos personales es a veces el vagón de cola de los intereses geopolíticos de China que parece regular estrictamente las tecnologías extranjeras en las que no puede confiar mientras se

[27] **La nueva Supervisión China amenaza a los derechos humanos dentro del sistema,** Amnistía Internacional, Marzo de 2018.
https://www.amnesty.org/es/latest/news/2018/03/china-new-supervision-law-threat-to-human-rights/
Fecha de consulta: 23 de julio de 2019.

esfuerza por desarrollar sustitutos nacionales[28]. Ejemplos de esto son Weibo, Renren, Youku y Baidu. Sitios chinos que reemplazan la demanda de Twitter, Facebook, Youtube y Google, respectivamente.

Comentario

[28] **La polémica ley de ciberseguridad entra en vigor en China,** El País, Mayo de 2017 https://elpais.com/internacional/2017/05/31/actualidad/1496241283_691973.html
Fecha de consulta: 23 de julio de 2019.

Regulaciones en Latinoamérica

Mercosur

Como señaló el jefe de Inteligencia Criminal de la Prefectura Naval Argentina, Hugo García[29], la dinámica alcanzada en el proceso de integración entre los países miembros del MERCOSUR generó, desde el punto de vista policial, la necesidad de implementar una modalidad de trabajo impuestas por otras comunidades.

En ese sentido, se intensificó el intercambio de información e inteligencia criminal con organismos nacionales y de los países involucrados, con la finalidad de llevar a cabo un seguimiento constante de las organizaciones criminales cuya magnitud constituya un real peligro para la sociedad.

A continuación, se detalla el abordaje para protección de datos personales en los países del MERCOSUR, así como en países vecinos.

Brasil

En el caso de Brasil, nos encontramos con una situación reciente. El 14 de agosto de 2018, el presidente firmó la aprobación de la ley de Protección de Datos (LGPD por sus siglas en portugués). Esta ley, sin embargo, sufrió vetos del presidente antes de ser finalmente firmada por él.

Inicialmente, el texto original había sido aprobado en ambas cámaras del Congreso por votación unánime. La ley, tal como la definen los congresistas, es un “marco de trabajo legal para la protección, uso y tratamiento de la información personal”. La intención que se persiguió desde el legislativo fue la de dar a las personas mayor

[29] Entrevista realizada el 18 de mayo de 2018.

poder controlar sus datos, al exigir que las personas jurídicas obtengan el consentimiento de la persona antes de recopilar su información.

Esta es una acción importante en Brasil, donde diversos sectores como ser comercios, el transporte público y otros servicios a menudo captan los datos sin un consentimiento explícito ni notificación previa por parte del titular de los datos personales.

A partir de los vetos del presidente Temer, el texto del proyecto se vio modificado en algunos temas claves.

El primero es el veto a la creación de una autoridad independiente y de un consejo de protección de datos personales, que estaría vinculado a esa autoridad, lo que garantizaba una participación multisectorial. Eso condiciona a la ley sobre las garantías de aplicabilidad.

Una vez que esta modificación recibió duras críticas, el Gobierno comunicó que enviaría al Congreso un proyecto de ley o una medida provisional para crear esa autoridad, pero la información previa indica que el modelo que enviará el Ejecutivo no respeta las características de autoridad que se negoció en ese texto en el parlamento.

Ese es el principal problema que se identifica ya que, sin una autoridad realmente independiente, con autonomía administrativa y sancionadora, la ley tiene serios riesgos de no ponerse en práctica o bien no resultar eficaz.
Otra crítica que recibió la presidencia de Brasil fue el veto al artículo 28 que establece el deber público de informar a la sociedad, de manera proactiva, cuando se compartan datos personales con otros órganos del poder público. Ese artículo, que genera transparencia en el tratamiento de datos por parte del poder público, fue vetado sin ser justificado.

El tercer aspecto, que para las organizaciones de defensa de libertad de expresión también es significativo, es el veto al artículo que garantizaba la protección a los

datos personales de los solicitantes de información a través de la Ley de Acceso a la Información (LAI). Disposición que garantizaba acceso a los datos a las personas que solicitan información al poder público[30].

La nueva legislación impactará en la forma de recoger y tratar los datos de los usuarios. Desde 2020 las empresas o instituciones que recolectan datos personales en Brasil, ya sea en internet o en el mundo físico, no sólo tendrán que pedir la autorización a los usuarios, sino también poner a disposición toda la información sobre el tratamiento que le den a los datos, no pudiendo hacerlo en términos generales o vagos.

Esto quiere decir que cualquier ciudadano brasileño tendrá el derecho de saber cómo y por qué las organizaciones están recogiendo sus datos y podrán solicitar la revocación o la rectificación de ellos en cualquier momento[31].

Los datos considerados “sensibles” como sexo, etnia, convicciones religiosas, opiniones políticas y datos sobre salud, tienen aún más protección. El objetivo es evitar acciones discriminatorias a través del uso de esos datos, como, por ejemplo, en procesos de selección de personal o en contrataciones de planes de salud.

Los cambios que trae la ley incluyen multas por incumplimiento para las organizaciones que traten datos personales, las cuales también serán aplicadas a empresas internacionales que manipulen datos de ciudadanos brasileños, sin embargo, a diferencia de la multa de GDPR europea, que puede alcanzar hasta el

[30] **¿La futura ley de protección de datos de Brasil protegerá el derecho a la privacidad de las personas?**, Global Voices.org
https://es.globalvoices.org/2018/10/03/la-futura-ley-de-proteccion-de-datos-de-brasil-protegera-el-derecho-a-la-privacidad-de-las-personas/
Fecha de consulta 22 de marzo de 2019

[31] **En qué consiste la Ley General de Protección de datos recientemente aprobada en Brasil**, Amanda De Sousa Alencar, Derechosdigitales.org
https://www.derechosdigitales.org/12309/en-que-consiste-la-ley-general-de-proteccion-de-datos-recientemente-aprobada-en-brasil/
Fecha de consulta 1° de mayo de 2019

4% de los ingresos globales de una empresa, la ley de Brasil es menos severa, llegando hasta el 2% y limitada a US$ 13.5 millones por infracción[32].

Chile

El caso chileno también planea la modificación de la ley nacional, pero va más allá y se plantea modificar la Constitución Nacional.

El senado chileno promovió la elevación a rango constitucional del derecho de todas las personas a que sus datos personales se encuentren protegidos.

En ese sentido tres senadores, y dos ex senadores plantearon modificar el N° 4, del artículo 19 del Texto Constitucional, que asegura "el respeto y protección a la vida privada y a la honra de la persona y su familia" en el siguiente sentido:

"4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

Si bien esta reforma modifica directamente a la constitución chilena y no la ley N°19.628 sobre protección de la vida privada, el proyecto que modifica dicha ley se encuentra actualmente en tramitación e implica cambios entre los que se destaca la creación de un organismo regulador llamado Agencia de Protección de Datos Personales[33].

---

[32] **Brasil: los retos de la implementación de la nueva Ley de Protección de Datos**, América Economía.
https://www.americaeconomia.com/tmf-group/brasil-los-retos-de-la-implementacion-de-la-nueva-ley-de-proteccion-de-datos Fecha de consulta 30 de abril de 2019.

[33] **Senado aprobó reforma constitucional de protección de datos personales en Chile**, Diego Bastarrica.
https://www.fayerwayer.com/2018/05/senado-aprobo-ley-proteccion-datos-personales-chile/ Fecha de conslta 1° de mayo de 2019.

Ley de derecho a la privacidad N°19.628
https://www.leychile.cl/Navegar?idNorma=141599

Dentro de las modificaciones que se prevén en la ley, también figura una restricción al uso de los datos personales de libre acceso. La regla general es que, para tratar un dato personal, se requiere el consentimiento de su titular. Actualmente, el hecho de que un dato se encuentre en una fuente accesible al público se configura como excepción a este principio, pero una excepción tan amplia que termina transformando la desprotección en la regla general. De ahí la proliferación de sitios web que exponen datos personales o de empresas que los utilizan para entregar inteligencia de negocio o para campañas políticas, como mencionamos anteriormente.

En esta nueva versión de la ley chilena se establece que la definición de qué se considera una fuente “accesible al público” no será amplia, sino taxativa. Esto quiere decir que un número limitado y establecido de fuentes de información tendrán esta categoría en Chile, y que ese listado será revisado anualmente por la entidad encargada de protección de datos. En definitiva, pocas fuentes abiertas serán de uso legal.

Un punto que recibió críticas en el proyecto de modificación de la ley es que sólo deberán registrar las bases de datos que administran los organismos públicos y no las organizaciones privadas. Pero por otro lado, los buscadores en internet como Google y Yahoo serán considerados como responsables de base de datos, debiendo desindexar cualquier dato personal que un titular requiera, lo que se conoce como “derecho al olvido”. Este último punto puede dificultar tareas como las investigaciones del Poder Judicial, el periodismo de investigación y derechos como libertad de expresión y el derecho a obtener información.

Con respecto al órgano de control, en principio el proyecto de modificación proponía que dependa del Ministerio de Hacienda, pero el Poder Ejecutivo propuso que

---

Avanza la tramitación de la ley de datos: lo bueno, lo malo y lo feo, Pablo Violler, Derechos Digitales
https://www.derechosdigitales.org/12316/avanza-la-tramitacion-de-la-ley-de-datos-lo-bueno-lo-malo-y-lo-feo/ Fecha de consulta 1° de mayo de 2019.

dependa del Consejo de la Transparencia para que éste cuente con mayor autonomía e independencia. Algunos legisladores piensan que la mejor opción sería crear un organismo cien por ciento autónomo por fuera de las estructuras del diseño estatal actual.

El órgano de control de Datos Personales chileno, se dividirá en dos áreas: Una para acceso a la información y otra para protección de datos personales y aumentar el número de consejeros de cuatro a cinco. Del mismo modo, los consejeros pasan a tener dedicación exclusiva, se establecerán incompatibilidades respecto de aquellos que puedan tener intereses en el sector privado y quienes hayan sido sancionados previamente por tratamiento indebido de datos personales.

Si bien el contexto muestra la inminencia de la aprobación del proyecto de ley y la reforma constitucional, al momento del cierre de este trabajo no se concretaron ambas iniciativas.

Colombia

La República de Colombia regula el derecho de Hábeas Data y el Derecho a la Información a través de la ley 1581, sancionada en 2012. El primero de ellos, Habeas Data, trata el derecho constitucional que todas las personas tienen de conocer, actualizar y rectificar aquellos datos personales que formen parte de un archivo o base, tanto en entidades públicas como privadas. Sin embargo hay bases que quedan exentas del control de la ley y son:

Aquellas que se circunscriben al ámbito exclusivamente personal o doméstico, las que tengan por finalidad la seguridad o la defensa nacional, aquellas con fines de inteligencia y contrainteligencia del Estado, bases periodísticas y otros contenidos editoriales, y aquellas que son reguladas por la ley 1266 de 2008 y la ley 79 de 1993. El tratamiento de datos sensibles está expresamente prohibido por la ley.

La legislación se refiere también especialmente al tratamiento de los datos personales de los niños, niñas y adolescentes, proscribiendo el tratamiento de los datos de estos grupos, excepto de aquellos que sean de naturaleza pública.

Los derechos del titular de los datos son: Conocer, actualizar y rectificar sus datos personales frente a los responsables o encargados del tratamiento, siempre de forma gratuita. Solicitar prueba de la autorización otorgada al responsable del tratamiento. Ser informado por el responsable del tratamiento o encargado, previa solicitud, respecto del uso que le ha dado a sus datos personales.

Asimismo el titular tiene derecho también a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley, revocar la autorización o solicitar la supresión del dato cuando en el tratamiento no respeten los principios, derechos y garantías constitucionales y legales.

El titular debe autorizar el uso de sus datos, y dicha autorización debe ser a través de un medio que luego pueda ser objeto de consulta, para poder corroborarlo ante un reclamo o posterior control de la autoridad.

Los responsables de bases de datos personales sólo podrán suministrar dicha información a sus titulares, sus representantes legales o terceros que él/la autorice, entidades públicas o administrativas que los necesiten por el ejercicio legal de su función o bien por requerimiento de una orden judicial.

El plazo que tiene el responsable de una base de datos personales para contestar ante una consulta es de diez días hábiles, de no poder cumplir con ese tiempo de respuesta deberá informar al titular, y en ese caso solo podrá demorarse cinco días hábiles más.

La autoridad de protección de datos personales que establece la ley es la Delegatura para la protección de Datos Personales, que depende de la Superintendencia de Industria y Comercio de Colombia. La Delegatura tiene facultades para bloquear bases de datos personales en los casos que considere que

se pueden estar vulnerando derechos del titular. También es el organismo que da conformidad sobre transferencias internacionales de datos personales, administra y regula el Registro Nacional Público de Bases de Datos.

El organismo tiene capacidad de aplicar multas de hasta el equivalente a dos mil salarios mínimos mensuales, puede suspender las actividades relacionadas con el tratamiento de datos hasta por seis meses, cerrar de forma temporal o definitiva las actividades de tratamiento de datos personales.

El 18 de enero de 2018, la Presidencia de Colombia emitió el decreto 90/2018 a través del cual redujo sustancialmente el universo de obligados a llevar a cabo la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos y se amplió el plazo para cumplir con dicha obligación[34].

Perú

Desde 2011 se encuentra vigente la Ley de Protección de Datos Personales N°29.733 que tiene por objeto garantizar en el Perú el derecho de las personas a la protección de sus datos personales y su privacidad. Es de obligatorio cumplimiento para las entidades del Estado, las personas naturales y jurídicas.
Esta legislación establece obligaciones sobre las empresas para que aseguren un adecuado tratamiento de los datos personales de sus clientes, proveedores, trabajadores y otras personas vinculadas a su actividad. Asimismo, esta legislación

[34] **ABC Ley 1581 de 2012 Protección de Datos Personales**, Banco Caja Social.
https://www.bancocajasocial.com/abc-ley-1581-de-2012-proteccion-de-datos-personales
Fecha de consulta: 25 de abril de 2019.

Decreto 090 de 2018 – Nueva Regulación frente al Registro Nacional de Bases de Datos, Universidad Externado.
https://dernegocios.uexternado.edu.co/comercio-electronico/decreto-090-de-2018-nueva-regulacion-frente-al-registro-nacional-de-bases-de-datos/
Fecha de consulta: 25 de abril de 2019

Decreto reglamentario Ley 1581/2012, Ministerio de Tecnologías de la Información y las Comunicaciones.
https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf
Fecha de consulta: 25 de abril de 2019.

y su reglamentación reconocen los derechos de las personas a quienes pertenecen dichos datos.

Las principales obligaciones para las empresas son: Primero inscribir ante la Autoridad de aplicación los Bancos de los Datos Personales que posean, esta información puede estar almacenada en soportes automatizados y digitales como físicos tales como archivadores, documentos o legajos impresos, detalla la ley.

Las empresas además deberán obtener un consentimiento informado por parte de los titulares de los datos personales. Dicho consentimiento debe ser previo al tratamiento de los datos, libre sin condicionamientos para el titular, expreso e inequívoco, evitando confusiones o dobles interpretaciones[35].

Quienes posean bases de datos personales deberán aplicar medidas de seguridad técnicas, organizativas y legales con el objetivo de evitar filtraciones o sustracciones de los datos. La ley exige la elaboración de políticas de privacidad, manuales organizativos que asignen cuidados y responsabilidades en el tratamiento de los datos personales, compromisos de confidencialidad y cláusulas contractuales, entre otras.

También se obliga a garantizar a los titulares el acceso, la rectificación, la cancelación y la oposición o derecho a supresión de los datos personales recopilados sin un consentimiento expreso.
Finalmente, la ley indica comunicar el flujo transfronterizo cuando la empresa que posee un bases de datos personales transfiere datos a un destinatario situado en un

---

[35] **Ley de Protección de Datos Personales N°29733/07**, Ministerio de Justicia, República del Perú.
https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf
Fecha de consulta: 25 de junio de 2019.

Decreto reglamentario de la Ley de Protección de Datos Personales N°29733, Año 2013.
https://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf
Fecha de consulta: 25 de junio de 2019.

Regulaciones, decretos y legislación relacionada a Datos Personales en Perú.
https://www.minjus.gob.pe/legislacion/
Fecha de consulta: 25 de junio de 2019.

país distinto al país de origen (Perú), debe informar el nombre y la ubicación de ese destinatario. Por ejemplo, debe informar la transferencia de datos a una empresa del mismo grupo en el exterior, o a una empresa que le brinda los servicios cloud computing (Almacenamiento en la nube).

La Autoridad Nacional de Protección de Datos Personales ha sancionado por incumplimientos de la ley a más de setenta organizaciones por un total de 2 millones de soles peruanos, aproximadamente 600 mil dólares.

Ecuador

En enero de 2019, la autoridad de aplicación en el Ecuador, la Dirección Nacional de Registro de Datos Públicos (DINARDAP), presentó un anteproyecto de Ley Orgánica de Protección de Datos Personales.

Actualmente el artículo 66 de la Constitución del Ecuador de 2008, contempla el derecho a la protección de datos de carácter personal, pero hasta ahora este derecho no estaba regulado.

Así como en otros países de la región, se tomaron varios aspectos de la legislación de la Comunidad Europea. El anteproyecto está siendo sometido al debate dentro de la comunidad ecuatoriana y seguramente recibirá modificaciones por parte de los grupos e instituciones más interesados en la futura legislación.

Agotada esta instancia y llegado a un consenso será presentado como proyecto ante la Asamblea Nacional del Ecuador, el poder legislativo de dicho país. Allí será nuevamente discutido, modificado de ser necesario y finalmente votado por los representantes de los partidos.

Dentro de los principales puntos que incluye el anteproyecto destacamos un mayor reconocimiento de derechos a favor de los titulares de los datos personales,

considerando el derecho al pleno acceso a los datos, mayor transparencia sobre el uso, derecho a la eliminación de los datos, entre otros.

Sobre el tratamiento de los datos el anteproyecto prevé la aplicación de los principios de legalidad, lealtad, legitimidad y finalidad. También un régimen especial para datos sensibles vinculados a la minoridad, es decir datos cuyos titulares sean niños, niñas o adolescentes.

Se establece un protocolo especial de seguridad de datos y de transferencias internacionales de datos, como así también obligaciones y responsabilidades legales para los encargados del tratamiento.

Otro de los puntos destacados es la propuesta de implementación de un régimen de infracciones ante determinados incumplimientos tales como la falta de notificación de vulneraciones o amenazas a la seguridad de los datos. También se propone penar la utilización de datos para fines distintos a los declarados por parte de las organizaciones que los recolectan y procesan.

Las principales problemáticas que experimentan los ecuatorianos no son ajenas a la realidad de la región. Muchas empresas obtienen datos personales con fines comerciales por medios legales, pero éticamente cuestionables como es el caso de las compañías que comparten datos personales de clientes con firmas asociadas, como ser un banco que sea dueño de una empresa de seguros y/o de una empresa de turismo. En ese caso queda expuesto el uso diferido al fin de la recolección autorizada por parte de los titulares.

También están los casos de datos personales obtenidos de manera ilegal, accesibles a través de un mercado de bases de datos que se recolectan y comercializan de manera informal mayoritariamente en internet y sin considerar ningún derecho a los titulares de los datos.

Si bien en Ecuador todavía no existe una regulación específica, el artículo 229 del Código Orgánico Integral Penal sanciona con penas de uno a tres años de prisión a

quien revele datos que violen “el secreto, la intimidad y la privacidad de las personas” y si quien comete este delito es un empleado público o bancario la pena sube hasta cinco años. Por otro lado la comercialización de “referencias crediticias” está prohibida por el artículo 360 del Código Orgánico Monetario Financiero[36].

Venezuela

Venezuela no cuenta con una ley que regule la protección de los datos personales. A pesar de ello la Constitución Nacional en su artículo 60 indica que “toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de información para garantizar el honor y la intimidad personal y familiar de los ciudadanos”.

La Carta Magna, en su artículo 28 señala que “toda persona tiene derecho a acceder a la información que sobre sí misma o sobre sus bienes consten en registros públicos o privados”. Y la Ley Orgánica del Tribunal Supremo de Justicia en el artículo 167 describe que “los ciudadanos tienen derecho a conocer la información que sobre ellos se refiera y esté contenida en los archivos de los bancos públicos y privados, pudiendo también solicitar confidencialidad sobre los mismos”.

---

[36] **Paradigmas de la protección de datos personales en Ecuador,** Revista de Derecho, No. 27, Luis Enríquez Álvarez
http://repositorio.uasb.edu.ec/bitstream/10644/5945/1/05-TC-Enriquez.pdf
Fecha de consulta: 22 de julio de 2019.

Ecuador no tiene ley para proteger datos personales, El Universo.
https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales
Fecha de consulta: 22 de julio de 2019.

¿Qué propone la Ley Orgánica de Protección de Datos Personales en Ecuador?, Revista Gestión Digital.
https://revistagestion.ec/index.php/estrategia-analisis/que-propone-la-ley-organica-de-proteccion-de-datos-personales-en-ecuador
Fecha de consulta: 22 de julio de 2019.

La última iniciativa de promover un proyecto de ley de protección de datos personales en el poder legislativo venezolano (Asamblea Nacional) se dio en 2004, a través del diputado Guillermo Berdugo del partido Acción Democrática. Dicho legislador desde la Comisión de Ciencia, Tecnología y Medios de Comunicación, promovió una consulta popular por el proyecto de ley pero la misma no prosperó[37].

Uruguay

En Uruguay existe desde 2008 la ley 18.331 que regula la protección de datos personales. Existe también una autoridad de aplicación que regula la ley, la Unidad de Protección de Datos Personales. La normativa establece que las personas, públicas o privadas registren sus bases de datos en el Registro de Bases Personales de la Unidad Reguladora de Control de Datos Personales.

Se establecen en el artículo 18 de dicha normativa una diferenciación entre aquellos datos que además de ser personales son datos sensibles. Regula además formas aceptadas de recolección, acceso y transmisión de datos. En el artículo 37 se explicita el derecho de hábeas data cuando señala que “toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento,

---

[37] **Saber Más III,** Informe sobre Acceso a la Información Pública y Protección de Datos Personales, Alianza Regional.
https://transparencia.org.ve/wp-content/uploads/2016/05/21.-SABER-MAS-III-Proteccion-de-datos-personales.pdf
Fecha de consulta: 22 de julio de 2019.

El derecho a la privacidad en la República Bolivariana de Venezuela, Harvard University y Privacy International.
http://hrp.law.harvard.edu/wp-content/uploads/2016/04/UPR-Venezuela-Stakeholder-Report-Spanish.docx
Fecha de consulta: 22 de julio de 2019.

discriminación o desactualización- a exigir su rectificación inclusión supresión o lo que entienda corresponder".

Al igual que en nuestra legislación, en Uruguay existen una serie de datos personales que no tienen una protección especial, y por más que refieran a una persona individualizable son de libre acceso. Ejemplos de este caso son los datos de identificación como pueden ser: Nombre, apellido, estado civil, firma, firma electrónica, lugar y fecha de nacimiento, nacionalidad y edad de las personas.

Por otra parte, la ley clasifica a los datos sensibles como "especialmente protegidos", dentro de ellos podemos destacar: Los datos ideológicos; creencia religiosa, afiliación política, pertenencia a organizaciones de la sociedad civil. Los datos relacionados a la salud; historia clínica, enfermedades, consumo de sustancias tóxicas, información de carácter psicológico, psiquiátrico, incapacidades, etc.

Las características personales también son datos especialmente protegidos, tales como el tipo de sangre, el ADN y la huella dactilar. El color de piel, su origen étnico y racial, el color de iris, color de cabello, señas particulares, estatura, peso y discapacidades. La vida sexual, es decir la preferencia o no de un género y sus hábitos sexuales[38].

En simultáneo de la aprobación de la ley de protección de datos personales se dio también la aprobación de la ley 18.381 de Acceso a la Información Pública. Ambas legislaciones están controladas por la misma autoridad de aplicación, al igual que en el actual proyecto de ley argentino.

En octubre de 2018 fue promulgada la Ley de Rendición de Cuentas N°19.670, vigente desde enero de 2019, la cual contiene cuatro artículos que incorporan

[38] **Ley de Protección de Datos Personales y Hábeas data,** Senado y la Cámara de Representantes de la República Oriental del Uruguay.
https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html
Fecha de consulta: 23 de julio de 2019.

importantes modificaciones a la normativa de Protección de Datos Personales en Uruguay[39].

Dichos cambios tienen el objetivo de alinear la legislación nacional con los nuevos desarrollos en la materia, ofreciendo así mayores garantías a las personas para la protección de sus datos personales. Los cambios a la legislación sobre Protección de Datos Personales (introducidos por los artículos 37 a 40 de la Ley de Rendición de Cuentas) son los siguientes:

Ampliación del ámbito de aplicación de la Ley de Protección de Datos Personales:

Anteriormente, la Ley de Protección de Datos Personales N° 18.331 se aplicaba al tratamiento de datos personales en caso de que el responsable o encargado de una base de datos estuviera radicado y ejerciera su actividad en territorio uruguayo o si en el tratamiento de los datos se utilizaban medios situados en el país. Ahora, dicha normativa regirá también fuera de las fronteras del país en caso de que las actividades del tratamiento estén relacionadas con la oferta de bienes y servicios dirigidos a habitantes de Uruguay o que involucren el análisis de su comportamiento, o si así lo disponen normas de derecho internacional o un contrato.

Nuevas obligaciones para responsables y encargados de bases de datos:

A partir de la nueva legislación, cuando el responsable o encargado de una base de datos tome conocimiento de que se ha vulnerado la seguridad de dicha base, deberá informar de inmediato, conjuntamente con las medidas adoptadas, tanto al titular de los datos como a la URCDP, quien coordinará con el Centro Nacional de

[39] **Modificaciones a la normativa de Protección de Datos Personales en Uruguay**, Centro de Información Oficial.
https://www.impo.com.uy/bases/leyes/19670-2018
Fecha de consulta: 31 de julio de 2019.

Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy) los pasos a seguir.

Modificaciones al "principio de responsabilidad":

El artículo 39 de la Ley de Rendición de Cuentas sustituye el antiguo artículo 12 de la Ley 18.331 de Protección de Datos Personales. La nueva redacción impone modificaciones al "principio de responsabilidad", estableciendo que tanto el responsable como el encargado de una base de datos son responsables de la violación de las disposiciones de la ley. Asimismo, la normativa establece que responsables y encargados de bases de datos deben adoptar las medidas técnicas y organizativas que correspondan (privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, etc.) para asegurar su protección.

Creación de la figura del "delegado de protección de datos":

La normativa hoy vigente establece que las entidades públicas y las privadas que tratan grandes volúmenes de datos o datos sensibles como negocio principal deben incorporar obligatoriamente la figura del "delegado de protección de datos". Este tendrá entre sus funciones asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales; supervisar el cumplimiento y proponer las medidas pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia y actuar como nexo entre su entidad y la URCDP.

Bolivia

En Bolivia no existe una legislación específica que regule el derecho a la protección de los datos personales, ni tampoco el derecho de acceso a la información pública.

La Constitución Política del Estado, (como llaman a su Constitución Nacional), en su artículo 21, inciso 2 establece que los bolivianos y bolivianas “tienen derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad”,y en el artículo 130 describe el derecho constitucional que las personas tienen de “conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y la privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá imponer la Acción de Protección de Privacidad”.

En el mismo sentido, el artículo 18 del Código Civil establece que “nadie puede perturbar ni divulgar la vida íntima de una persona” y la Ley de Telecomunicaciones, en su artículo 55 establece que “los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias y usuarios salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma”[40].

La misma legislación, en el artículo 83, obliga a los proveedores a “brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley”.

Para que un ciudadano boliviano ejerza su derecho de protección de datos personales deberá interponer una Acción de Protección de Privacidad ante las cortes superiores distritales, la misma pasará a revisión al Tribunal Constitucional y recibirá un fallo que genera jurisprudencia vinculante.

En términos generales es apreciable cierta complejidad para acceder a éste derecho, que necesita de una proactividad alta por parte de cada ciudadano para en

[40] **Ley de Telecomunicaciones de la República de Bolivia,** 1995.
http://www.itu.int/ITU-D/treg/Legislation/Bolivia/ley_tlc.pdf
Fecha de consulta: 23 de julio de 2019.

términos individuales o colectivos ejercer su derecho de protección de datos personales.

Ante la falta de un órgano de control específico, la Defensoría del Pueblo de Bolivia emite pronunciamientos que generan influencia sobre diferentes autoridades, organismos o empresas que ante un reclamo o por propia iniciativa consideren que pueden estar afectando el derecho de ciudadanos, pero dichas posiciones no generarán una pena sobre los denunciados ni tienen capacidad de juzgar a los mismos por lo que su poder de protección es limitado.

Tabla comparativa de países.

Cuadro 2: Elaboración propia en base a datos recolectados según fuentes descriptas.

País	Ley vigente y año	Nombre de organo de control	Regula organizaciones públicas y privadas	Organo de control exclusivo	Depende de	Nivel de sanciones	Autoriza datos sencibles	Sin concentimiento del titular	Se está tratando proyecto de creación ó modificación	Delegado de protección de datos
Argentina	2001	Agencia de Acceso a la Información Pública	Sí	No, tambien acceso a la información	Presidencia de la Nación	Multas económicas 500 salarios minimos, suspención de bases de datos, carcel para responsable de bases (nueva ley)	Prohibido, salvo concentimiento expreso del titular (en proyecto ley nueva)	Todos: Nombre y apellido, DNI y dirección. Libre para: Seguridad, defensa, tareas del Estado,	Sí. Nueva ley	Sí, solo para públicos y privados de gran escala. En nueva ley
Brasil						2% de facturación o 13.5 millones de U$s				
Chile			Sí	No, tambien acceso a la información	Consejo de Trasnparencia			Fuentes de libre acceso legales limitadas y registradas por la autoridad	Sí y reforma constitucional	
Colombia	2012	Delegatura para la protección de Datos Personales	Sí	Sí	Superintendencia de Industria y Comercio	2000 salarios minimos, suspención temporal o defeinitiva de bases	Prohibido salvo excepciones	Datos de naturaleza pública, actividades del Estado, Casos urgencia médica, orden judicial, fines historicos, estadisticos o científicos	Sí	
UE						20 millones de euros ó 4% de facturación anual				
Uruguay	Ley 18.331/2018	Unidad Reguladora y de Control de Datos Personales (URCDP)	Sí	Sí	Autonomía técnica		Prohibido		No	Sí
Bolivia	No tiene / Pero está amparado por la Constitución Política del Estado, artículos 21 y	Cortes Superiores Distritales (Poder judicial)	A través de una Acción de Protección de Privacidad el ciudadano puede reclamar ante el Poder Judicial por bancos de datos	No tiene / Pero el derecho sería canalizado por el Poder Judicial y tambien en segundo nivel por la Defensoría del	No tiene	El Poder Judicial genera fallos que crean jurisprudencia vinculante	No especifica	No especifica	No	No

CAPÍTULO 3

PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA Y EL NUEVO PROYECTO DE LEY

Como hemos citado anteriormente en este trabajo, en nuestro país el derecho a la protección de Datos Personales está actualmente regulado por la Ley 25.326 de Protección de Datos Personales. Dicha ley define a los datos personales en su artículo 2 como “información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”.

El órgano de control de la normativa es la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente de Presidencia de la Nación, y actualmente incorporado por decreto dentro de la Agencia de Acceso a la Información Pública, una nueva institución que maneja tanto el derecho de protección de datos personales como el de acceso a la información pública, hasta el momento definido por el decreto 1172/03.

Esta decisión buscaría atenuar la tensión que existe entre ambos derechos y que mayoritariamente se dirimía en el ámbito del Poder Judicial al carecer de una relación formal. Según el prestigioso think tank argentino Asociación por los Derechos Civiles (ADC) “los conflictos interpretativos entre la protección de datos personales y el acceso a la información se resuelven a favor de la primera. Sobre 45 dictámenes analizados, en un 89 por ciento de los casos la DNPDP negó el acceso a los datos solicitados o, más comúnmente, estableció condiciones para ese acceso no previstas en el decreto de acceso a la información, como la existencia de un interés legítimo”.

La ley 25.326 regula el uso de los datos personales en archivos públicos y también privados. Este tipo de datos solo pueden ser recopilados con el consentimiento del titular y se le debe garantizar el uso confidencial de los mismos. Un principio importante de la ley vigente es el de finalidad, que determina que los datos no deben utilizarse para fines distintos a los que fueron reunidos.

En este sentido, al consultarle al especialista Eduardo Bertoni[41] sobre si esta ley es adecuada para proteger datos personales en el marco de la prácticas habituales de

[41] Eduardo Bertoni, Ex-Director de la Agencia de Acceso a la Información Pública (AAIP) (2017-2021). Actual representante ante el Instituto Interamericano de Derechos Humanos (IIDH). Entrevista, 30 de marzo 2020.

los usuarios de “volcar” datos en las redes, Bertoni expresa que *Si "volcamos" implica otorgar consentimiento, lo cual parece obvio, nuestra ley es suficiente y está adecuada a las legislaciones de otros países. El problema a veces es que no somos conscientes de que damos nuestro consentimiento al aceptar el uso de las aplicaciones.*

En el artículo 11 de la ley, está descrita la acción de *Cesión*, es decir cuando los titulares de los datos deciden darlos para determinado uso: “Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.”

La misma ONG, ADC, expone dos casos prácticos que respaldan esta relación de tensión entre el derecho de acceso a la información pública y el derecho de protección de datos personales.

El primero de los casos es el de CIPPEC contra el Estado Nacional: En este caso, la Asociación por los Derechos Civiles (ADC) patrocinó el reclamo del CIPPEC que había solicitado información sobre distribución de planes sociales y la misma había sido denegada alegando que conocer quiénes eran los beneficiarios de esos planes implicaba acceder a “datos sensibles”, que según la ley 25.326 son datos personales que “revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”. Según la DNPDP, “si bien el hecho de integrar una lista de beneficiarios de un plan social no es, en principio, información de carácter sensible per se, si el subsidio tiene su origen o fundamento en una enfermedad (dato relativo a la salud) podría revelar un dato sensible, circunstancia que configuraría en ese caso la excepción prevista en el citado artículo 16 del reglamento de Acceso a la Información Pública (decreto 1172/03)”. La Subsecretaría para la Reforma Institucional y el Fortalecimiento de la Democracia se sumó a esa interpretación de

la DNPDP, aunque reconoció que el acceso podría favorecer el control de la implementación de los planes sociales en cuestión[42].

En el segundo de los casos, la Dirección Nacional de Protección de Datos Personales ha considerado en numerosas oportunidades que el acceso a información sobre nómina de empleados del Estado requiere la demostración de un "interés legítimo" por parte de quien lo solicita, requisito que el decreto 1172/03 no establece pero sí la ley 25.326. Ello es así por la definición amplia de "datos personales" que establece la ley, que en la práctica restringe fuertemente el alcance del derecho de acceso a la información. Así, por ejemplo, la DNPDP condicionó a la existencia de un "interés legítimo" la entrega de información relativa al salario del vocero presidencial (1/10); sobre personas detenidas durante una ola represiva en la década del sesenta (4/09); información sobre personas condecoradas con motivo de los servicios prestados durante la Guerra de Malvinas (30/09); información sobre transferencias presupuestarias a organizaciones sin fines de lucro (38/09); nómina de autoridades de la Policía Federal Argentina (3/08); información sobre personas detenidas durante un conflicto que involucró a productores agropecuarios (5/08); sueldo de la Presidenta de la Nación (37/08); entre otros[43].

Como señaló el especialista en protección de datos, Eduardo Peduto, la ley nacional 25.326 que estudiamos en el presente trabajo guarda estrecha similitud con la ley 1845 de Protección de Datos Personales de la Ciudad de Buenos Aires, a excepción de que la ley nacional también aplica sobre el sector privado.

En el caso de la Ciudad de Buenos Aires, la Defensoría del Pueblo, ha sido designada órgano de control del asiento, uso y difusión de las bases de datos personales del sector público de la Ciudad de Buenos Aires garantizando el derecho al honor, la intimidad y la autodeterminación informativa. Los datos asentados deben ser exactos y bajo ningún concepto ser utilizados para un fin distinto a aquel por el que fueron obtenidos.

---

[42] Cfr. Nota 495/08 del Ministerio de Desarrollo Social, Secretaría de Coordinación y Monitoreo Institucional, del 9 de abril de 2008.
[43] Todos los números entre paréntesis corresponden a dictámenes de la Dirección Nacional de Protección de Datos Personales, disponibles en: http://www.jus.gob.ar/datos-personales.aspx

Esta garantía está especialmente orientada a la preservación y confidencialidad respecto de los denominados datos sensibles: origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o vida sexual.

Con el objeto de cumplir con las funciones asignadas, la Defensoría del Pueblo ha creado el Centro de Protección de Datos Personales. En línea con lo expresado por el especialista, toda persona que presuma o tenga la certeza de que sus datos figuran en alguno de los bancos de datos personales puede ejercer los siguientes derechos:

Derecho de información: Solicitar a la Defensoría del Pueblo, tomar conocimiento del Registro a su cargo. Derecho de acceso: Solicitar y obtener información de los datos referidos a su persona que se hallen en alguna o algunas bases de datos del sector público. Derecho de rectificación, actualización o supresión: Solicitar la rectificación o actualización de sus datos y, cuando corresponda, la supresión o la protección de confidencialidad.

En este sentido, Peduto destacó que la visión de la Dirección que preside trata estos temas como partes de un triángulo que debe tener cierta armonía entre cada extremo. Un extremo es el derecho a la Protección de Datos Personales, otro es el derecho de Acceso a la Información (pública) y un tercero es el derecho a la Privacidad.

En opinión de este especialista, la ley nacional de Protección de Datos Personales vigente tiene dos debilidades. Una es que al haber sido creada en el año 2000 no contempla mucho de lo que fue sucediendo con la evolución y el crecimiento de internet, por lo que falta que la normativa se explaye en esta materia y determine muchos aspectos de los datos personales en internet.

Otro aspecto a mejorar es que se suscribe al ámbito judicial y no contempla las denuncias administrativas que podrían efectuarse con muy buenos resultados. A su vez el acceso a la justicia es muchas veces restrictivo para las mayorías, lo cual muchas veces supone contratar una representación o asesoramiento legal, sumado

a que por cláusulas contractuales las empresas globales de internet, propietarias entre otras de Facebook, Instagram y Twitter, tienen base en EE.UU. y designan a los tribunales de California como el lugar para dirimir potenciales litigios o reclamos legales. Esto hace que el derecho a reclamar o defenderse sea difícil de ejercer para gran parte de los extranjeros o para personas con recursos medios o medios-bajos.

El cambio tecnológico de almacenamiento de contenidos también representa un llamado de atención para la protección de los datos personales según la óptica de Peduto. Las nuevas prácticas de alojamiento migran de dispositivos físicos offline a alojamientos online, en la “nube”. Pero ese alojamiento de datos tiene su sustento en hardware que mayoritariamente se encuentra físicamente en EE.UU. por lo que cualquier legislación o decisión política sobre esa información va a ser influenciada por dicho país.

La Unión Europea, por ejemplo, recomienda no alojar contenidos en servidores de EE.UU. por considerarlo un destino no seguro para la información de sus ciudadanos. En este sentido, otra disposición que se abordó es el requisito para todas las empresas de Unión Europea del rol de “delegado de protección de datos personales” dentro de cada compañía. Esto deberá ser ejercido por un empleado que estará registrado y mantendrá el vínculo con el órgano de control de cada país, según la legislación puesta en práctica desde mayo de 2018 para la Unión Europea.

Volviendo al caso de nuestro país, la variante institucional tiene cuestiones a reveer en la materia como es el caso de que la Agencia de Acceso a la Información Pública (AAIP) dependa del Poder Ejecutivo Nacional (PEN). De esta forma tal vez nunca podrá ejercer su rol con verdadera imparcialidad cuando le toque exigir o denunciar al PEN.

Otra observación que considera interesante contemplar el especialista es el hecho de que la ley de Acceso a la Información Pública (que resuelve la creación de la AAIP), crea la Agencia de Control con la estructura de lo que era la Dirección Nacional de Datos Personales, pero por su nombre y su estructura puede hacer presuponer que le dará más importancia al acceso a la información pública que a

protección de datos personales o la privacidad. Lo que para nuestro país puede resultar inverso nuestra tendencia donde la protección de Datos Personales fue precursora sobre los otros dos derechos.

Jerónimo Pardo, que actualmente trabaja en Google, se desempeñó en el área de Analytics de la empresa de Inteligencia en Redes Sociales Illuminati Lab, la misma se dedica al análisis de datos e información disponible en redes sociales para la producción de conocimiento.

Para este trabajo tuvimos la oportunidad de entrevistarlo y nos comentó que dentro de sus tareas en la empresa en Inteligencia en Redes Sociales, la principal es la “escucha” o listening, que trata de entender de qué se está hablando en redes sociales, especialmente si esto involucra a algún cliente de la compañía o sobre algún tema de interés de dichos clientes. Se estima que estos proyectos representan cerca del 70% del total de los ingresos económicos de la compañía y es por lo tanto la actividad principal.

Para el entrevistado, dos datos personales que son de mucho valor para las empresas son: el email y el número de teléfono, ya que ambos datos permiten dirigir campañas publicitarias a usuarios específicos, son los datos de entrada que pide tanto Facebook como Instagram, pertenecientes al mismo grupo empresario.

Pudimos entender a través de la consulta a este profesional que empresas de esta actividad manejan cientos de bases de datos personales que se reúnen, donde principalmente se destacan datos como: nombre y apellido ó usuario, teléfono, email, cantidad de seguidores y seguidos en el caso de Twitter. Muchas veces en Twitter, por ejemplo, no hay datos personales, sino nombres de usuarios por lo tanto no pueden ser estos usuarios relacionados con una persona de existencia real.

Pero sobre la obtención, aparentemente se da a través de recursos legales ya que es el usuario el que voluntariamente o por desconocimiento acepta los términos y condiciones de la red social y comprarte esta información o bien provienen de una fuente de acceso público sin restricciones como es Twitter. Luego estos datos son aprovechados con fines comerciales.

Es importante destacar que los datos almacenados en la empresas, para no incumplir la ley, no deberían tener relación con una persona determinada o determinable.

Los archivos de datos, no siempre son archivos manipulables individualmente, alojados en un disco físico, sino que muchas veces son bases de datos alojadas en la nube, hosteadas en algún servidor de las compañías que no tienen un respaldo en hardware o bien no están disponibles de manera individual.

A través de la experiencia de Jerónimo dimos cuenta de la importancia a la hora de creación de un nuevo archivo de datos, y de que exista un protocolo, para que cada trabajador no cree a discreción archivos nuevos y diseñarlos al efecto de la tarea que le fue encomendada. De modo que los archivos figuren respetando las normativas y disposiciones internas de la compañía.

Aquellos archivos que no se utilizan más deben ser correctamente eliminados o cancelados. Evitando un almacenamiento masivo y siguiendo un criterio de eliminación. Si bien puede facilitar trabajo a futuro, no es una buena práctica la preservación ante futuras oportunidades de uso de dichos archivos.

Los archivos en estas compañías muchas veces son utilizados bajo lo que la ley considera “uso publicitario o comercial” al ser usados para campañas de email marketing o campañas publicitarias dirigidas a través de redes sociales.

Por otra parte los datos personales recabados en algunas ocasiones pueden ser para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, lo que en ese punto es un servicio con el respaldo legal considerado en la ley. Pero en la mayoría de los casos no es así ya que predominan los clientes de naturaleza privada.

Conocer la experiencia de Jerónimo Pardo fue valioso para nuestra investigación. Podemos decir que lo más prioritario en que deben hacer foco las compañías es en lo relativo a datos sensibles en algunos proyectos, específicamente cuidar que no

haya archivos donde se reúna y archive datos bajo el criterio de “opiniones políticas” u otros datos considerados “datos sensibles”. En redes sociales los usuarios muchas veces los exponen en sus biografías de cada perfil expresando su ideología u opinión política, o bien lo dan a conocer por la acción de “seguir” o “gustar” de determinados referentes políticos.

Otro aspecto que el analista consideró importante son las herramientas de análisis de datos, que si bien los paquetes de datos abiertos que entrega Twitter, por ejemplo, son para todas las herramientas los mismos, los software de análisis dan un aporte significativo para relacionar y extraer los datos y poder construir información, contexto y sentido al volumen de datos. Algunos de los programas más conocidos que utilizan son: Springler, Social Studio, Social Backers, Social Metrix (argentino), entre otros.

Finalizando la entrevista Jerónimo dijo estar considerablemente de acuerdo con que el valor de la Inteligencia en Redes Sociales está dado por el análisis masivo de datos, es allí donde radica el sentido de la producción de conocimiento para las organizaciones de esta naturaleza.

Nuevo proyecto de ley

Durante la presidencia de Mauricio Macri, el gobierno envió al Congreso, a través de la Agencia de Acceso a la Información Pública (AAIP), en septiembre de 2018 un proyecto de ley que buscaba derogar la actual ley 25.326 de Protección de Datos Personales y proponer a lo largo de 95 artículos, una nueva ley para reemplazarla.

Cabe mencionar que el proyecto perdió estado parlamentario el 29 de febrero de 2020.

Este proyecto girado al Congreso por la AAIP planteó, en principio, mayores controles y restricciones sobre el manejo de datos de los ciudadanos, crea mecanismos de protección para datos sensibles, nuevas sanciones para quienes no se adecuen o violen la normativa, crea la figura del *Delegado de Protección de*

Datos Personales y el ya conocido en nuestro país registro *No llame*, entre otros temas.

Según opinó el ex-titular de la AAIP, dependiente de Jefatura de Gabinete, Eduardo Bertoni[44], el proyecto tiene en cuenta ideas de las leyes europeas, de un perfil más restrictivo junto con ideas basadas en las legislaciones norteamericanas, donde los controles son un poco más moderados.

Como novedad se incorpora la obligación de que las organizaciones reguladas notifiquen cuando existan incidentes de seguridad en las bases de datos personales dentro de las 72 horas y en consecuencia la obligación de realizar una evaluación de impacto sobre los potenciales daños que dicho incidente podría provocar sobre los derechos de los titulares de los datos.

El proyecto obliga a adoptar medidas proporcionales a las modalidades y finalidades del tratamiento de los datos, su contexto, su tipo y categoría de datos tratados. También deben informar sobre el riesgo que dicho tratamiento pueda representar sobre los derechos del titular.

Los titulares, de aprobarse este proyecto en el futuro, tendrán derecho de oponerse a que sus datos sean objeto de una decisión tomada en base a un tratamiento automatizado. Esto plantea un punto interesante de cara al crecimiento exponencial de la Inteligencia Artificial.

Para la AAIP, este proyecto contempla muchos de los desafíos que las nuevas tecnologías le impusieron al rol de la protección de la privacidad.

Otros puntos destacados son que, el responsable del tratamiento debe informar al titular de los datos las finalidades del tratamiento de sus datos, antes de recolectarlos. También informar la identidad y los datos de contacto del responsable del tratamiento, los medios de los que dispone para ejercer sus derechos y poner en conocimiento al titular si dar sus datos es obligatorio o una facultad que se reserva,

[44] Eduardo Bertoni, Ex-Director de la Agencia de Acceso a la Información Pública (AAIP) (2017-2021). Actual representante ante el Instituto Interamericano de Derechos Humanos (IIDH).

y en el mismo sentido deberá informar qué consecuencias podría tener si da sus datos.
Sobre los datos sensibles, aquellos que determinan nuestra ideología, nuestra creencia religiosa, preferencias sexuales, opinión política, etc, seguirá siendo prohibido su tratamiento, excepto que el titular de su consentimiento expreso, o bien que sea una necesidad vital para el titular y éste se encuentre física o legalmente incapacitado.

Dentro del articulado se mencionan los derechos sobre la posible transferencia internacional de datos personales, en un contexto de flujo global de datos e información a través de internet, este apartado tiene un significado mucho más relevante y actual. Se permitirá la transferencia internacional solo con el consentimiento expreso del titular, si a su vez el país u organismo proporciona un nivel de protección adecuado, si Argentina mantiene un tratado o bien si de la transferencia de los datos dependieran temas vitales de la salud como la prevención, tratamiento o diagnóstico médico.

Por otra parte, el derecho de acceso a los titulares será dado previa acreditación de su identidad, a quienes se les deberá suministrar los datos que se tienen de ellos para el tratamiento de forma clara, exenta de codificaciones y en ese caso acompañada de una explicación, en un lenguaje accesible al conocimiento medio de la población.

La figura del Delegado de Protección de Datos Personales será obligatorio para los casos de autoridades u organismos públicos o si se realizan tratamiento de datos a gran escala. Por otro lado se crea el registro *No llame,* que prohíbe a las compañías contactar a titulares de datos que se registren en el mismo, ofreciendo publicidad, oferta, venta o regalo de bienes o servicios no solicitados.

Para aquellas organizaciones que no cumplan con la legislación se extenderán multas y sanciones que contemplan la suma de hasta quinientos salarios mínimos, suspensión de las actividades relacionadas con el tratamiento de los datos hasta por seis meses, suspensión definitiva de actividades si una vez cumplido el plazo no hubieran adoptado medidas correctivas.

Al haber sido presentado durante febrero de 2018, el proyecto perdió estado parlamentario. Si bien su principal impulsor fue, Eduardo Bertoni, (quien siguió al frente de la Agencia de Acceso a la Información Pública hasta enero de 2021), el gobierno de Alberto Fernández, no retomó, hasta el momento de cierre de esta tesis (marzo 2021), el impulso político al proyecto de ley.

Para Bertoni, los Estados con fines de seguridad pública, en ocasiones, recolectan datos personales de redes sociales. Pero esta tensión entre el derecho a la protección de los datos personales y el derecho a la seguridad pública, queda muchas veces resuelto en la ley, tanto en la Argentina como en el nuevo Reglamento de Protección de Datos de Europa ya que hay cierta información que de acuerdo a la ley se puede recolectar sin consentimiento y hay información que no puede ser recolectada.

En el caso de las empresas privadas que recolectan y analizan datos personales con fines comerciales, si hay consentimiento no hay problema. Pero si hay recolección con consentimiento y se utiliza para un fin distinto, se está fuera de la ley y en el mismo sentido si hay recolección sin consentimiento por fuera de las excepciones que da la ley, se está en contra de la ley de Protección de Datos Personales.

Cristina Caamaño[45] destacó que “para evitar que la producción de Inteligencia (por ejemplo en redes sociales) vulnere el derecho de protección de datos personales, hay que cumplir con la ley, sin descuidar que la inteligencia es una actividad estatal y que la premisa es que el Estado no puede violar el Estado de Derecho”.

Con ese fin desde la AFI “se elaboró un borrador de reforma legislativa que crea los mecanismos de control para que toda tarea de reunión de información sea congruente con una directiva de Inteligencia y que si esa tarea tensiona alguno de los derechos de los ciudadanos y las ciudadanas sean autorizadas y monitoreadas por un juez”, comentó la interventora.

[45] Cristina Caamaño, Interventora de la Agencia Federal de Inteligencia (AFI). Entrevista realizada el 21 de marzo de 2021.

CAPÍTULO 4

DESAFÍOS PARA GESTIÓN DE DATOS PERSONALES EN LA INTELIGENCIA ESTRATÉGICA DE ARGENTINA

En esta sección se presentarán los principales desafíos a medio y largo plazo que enfrenta la Argentina en materia de gestión de datos personales en las próximas décadas. Estos desafíos han sido identificados en función del relevamiento de fuentes efectuado para la investigación, así como de las reflexiones que se desprenden de las mismas y complementados con aportes provenientes de las entrevistas realizadas a expertos en la materia.

Desafíos a mediano plazo

Cuando hablamos de los desafíos a mediano plazo para la inteligencia estratégica nos estamos refiriendo a los escenarios futuros que en los próximos diez a quince años se verán reflejados en nuestras democracias actuales.

Es importante entender el rol que el análisis de información y datos producen en la realidad de las sociedades modernas. La velocidad con la que los sucesos se van a reconfigurar serán un desafío. El escenario actual, de múltiples legislaciones alrededor del mundo vigentes, dan cuenta de un momento de importancia para aplicar políticas públicas en la materia y de la relevancia que las sociedades democráticas y modernas le dan al tema.

Tanto en nuestro país, como en la región y en el mundo, las normativas sobre datos personales son diversas. A lo largo de la investigación se ha registrado esa diversidad y matices que, a pesar de compartir algunos valores esenciales, como la protección de los derechos de la ciudadanía y la promoción de la transparencia, muestran brechas y puntos en común entre los diferentes estados soberanos.

Es importante remarcar, tal como lo señaló David Omand[46], que los encargados de tomar decisiones políticas inevitablemente tienen un enfoque a más corto plazo que los funcionarios que brindan evaluaciones debido a las demandas del ciclo de elecciones políticas. El pensamiento genuinamente estratégico requiere la

[46] David Omand, Ex Director del Government Communications Headquarters (GCHQ), organismo responsable de la recolección de inteligencia de señales (SIGINT) en Reino Unido, entre 1996 y 1997. Entrevistado el 17 de abril de 2020.

capacidad de pensar como estadista, no como político. Por lo tanto, aunque las evaluaciones de inteligencia pueden ser genuinamente estratégicas, esbozando posibles desarrollos a largo plazo en los asuntos internacionales, son las advertencias a corto plazo de posibles crisis por delante las que reciben mayor atención y son más valoradas cuando ayudan a los gobiernos a evitar problemas.

Los desafíos a mediano plazo, además, tienen que ver con la interpretación de las diferentes normativas, la viabilidad de aplicación de cada una de ellas y también sobre la capacidad que los Estados tengan para adaptar estas legislaciones a los escenarios reales y, también virtuales, que se nos presenten en cada momento, donde la variable clave será la velocidad de cambio.

Otro de los principales desafíos que se nos plantean hasta aquí, tiene que ver con la formación y el conocimiento, y en ese sentido con la capacidad de nuestra comunidad para tomar decisiones sobre estos derechos que sin dudas estarán en constante tensión en los próximos años y afectarán a toda la población mundial. El desafío interpretativo de esta temática global estará asociado con la capacidad de interpretar las diferentes legislaciones en el contexto de cada país soberano.

Es por eso que este trabajo plantea preguntas sobre la capacidad que tendremos como sociedad para discernir y decidir sobre estos derechos.

Una dirección que parece la más sólida es la de toma de decisiones plurales, multisectoriales e interdisciplinarias, donde se pueda tener en cuenta un abanico amplio de intereses y de actores, y de esta forma comprender de una manera más integral los próximos puntos en debate.

Para el especialista Alejandro Salomón, quien fue director de la Escuela Nacional de Inteligencia - Agencia Federal de Inteligencia (AFI) - (2015-2019), las redes sociales tienen mucha información útil para la producción de inteligencia, y desde el Estado se brinda a los analistas la formación específica para aprovechar ese recurso y otros recursos tecnológicos, como el Big Data. Desde ya que en la actualidad un analista de inteligencia es mucho más útil que sepa de tecnología a que sepa hacer un seguimiento callejero u otros métodos más arcaicos de recolección de información

que se promovía en el pasado y que por un lado eran mucho más violentos e invasivos y hoy son considerados totalmente obsoletos en gran medida.

Quizás por nuestros rasgos culturales, en Argentina, se replican discursos de diferentes actores políticos que sostienen, al menos desde la teoría, el camino único de “nunca” vulnerar el derecho a la privacidad de las personas.

Desde la óptica de esta tesis, creemos que no es cierto considerar que la privacidad pueda y deba ser respetada siempre. Y para ello podríamos como sociedad transitar un camino de sinceramiento sobre las políticas en esta materia que para nuestra opinión es el camino de promover la afectación de la privacidad “en consenso”. Esta propuesta invita a renunciar a la evasión y a la censura sobre el “cuando” y “como” el Estado debe violar la privacidad de una persona para protejer un derecho de mayor jerarquía.

Para la sociedad, saber que algunas privacidades no serán respetadas, sería un mensaje de mayor responsabilidad y verosimilitud con la realidad por parte de las autoridades. Sería deseable que este mensaje sea propuesto desde una política pública de consenso mayoritario y con plena transparencia.

Hay algunos problemas bien visibles sobre el rol de la Inteligencia del Estado y los decisores políticos. Desde el lado de la Agencia, uno de los sesgos más señalados, en algunos sectores, es realizar el trabajo pensando que están al servicio del presidente. Eso no es así, están al servicio del Estado, y de los intereses del Estado. Esto es realmente muy diferente. Como ejemplo se me ocurre que si la Agencia reúne información sobre los intereses de los bonistas para proveer inteligencia que ayude a una mejor toma de decisiones con respecto al pago de la deuda de nuestro país, sería una función lógica y útil a los intereses del Estado. Ahora bien, la reelección de un presidente, es un tema político partidario o personal del presidente, la Agencia no debe intervenir en ese asunto. Por eso no es correcto decir que la Agencia responde al presidente, sí responde pero solo sobre aquellos intereses estatales, no personales ni político partidarios.

Desde la óptica de la autoría de esta tesis, creemos que el pasado (y en algunos casos el futuro de largo plazo) puede ser un buen insumo para la difusión de la imagen de la Agencia Federal de Inteligencia. La visión, misión y valores organizacionales se explicarían mejor hacia afuera y hacia adentro pudiendo contar un relato sobre el trabajo y la producción de la agencia con ejemplos concretos que se hayan sucedido en el pasado y que no representen hoy una violación del secreto.

En algunas agencias del extranjero, esta política de transparencia, pero sobre todo de comunicación de la imagen, está ampliamente desarrollada mediante la llamada “desclasificación” de información, donde algunos informes o trabajos de las agencias tienen un vencimiento posterior al cual se le modifica la calificación de seguridad a los documentos que toman estado público y pasan a ser de libre acceso a la comunidad.

Del mismo modo, prospectivas a muy largo plazo, también pueden ser una forma de comunicar la visión del organismo reforzando la imagen de la agencia sin perjudicar proyectos en curso que podrían verse afectados si determinada información se hace pública.

Ambas propuestas, que guardan un mismo fin, tendrían efectos interesantes para avanzar en una nueva cultura donde la frontera entre la seguridad nacional, la privacidad, el acceso a la información y el uso político de los organismos del Estado, deje de sumar páginas gravosas que contradicen su objetivo funcional de servicio público.

Del otro lado, los decisores políticos muchas veces llegan con total desconocimiento sobre qué es la inteligencia y que debería hacer. Si no saben los decisores que se supone que son personas medianamente informadas, qué podemos esperar de la comunidad en general. El desconocimiento es total. Entonces, volviendo a los decisores, desde ese desconocimiento es muy complejo que consigan conducir o requerir funciones que sean realmente interesantes y eficientes para los intereses del país. Por otra parte también hay productos de inteligencia de muy baja calidad que de alguna manera desmotivan a los decisores políticos a proveerse de ese recurso, no todos los productos tienen baja calidad, pero aquellos que sí,

deslegitiman el rol de todo el organismo y entonces el decisor busca otras fuentes para tomar las decisiones de su posición. Quizás recurre al ámbito académico o científico o de algún otro tipo. En este sentido la responsabilidad es compartida, del político de no conocer la función de la inteligencia y de algún sector del organismo de no estar a la altura de la función que debe cumplir.

Otro de los mitos que se deben romper, según la visión de esta tesis, es el ideal de que la acción de la inteligencia del Estado no debería tener nunca efectos sobre lo político. Quien proponga este resultado no está a la altura de conducir un organismo de esta naturaleza, y políticamente utiliza un discurso tan engañoso como peligroso.

La inteligencia estatal, muchas veces puede influir, aunque no sea su fin principal, sobre la política nacional, sobre los partidos y las organizaciones políticas. Y claro que en eso se juega un rol institucional de mucha sensibilidad.

Ejemplos de esta influencia pueden verse en los casos en que funcionarios políticos se involucran en el narcotráfico. Allí la tarea de producir conocimiento sobre las organizaciones del narco que tienen los organismos de inteligencia van a influir sobre el arco político de un gobierno.

El impacto político que un funcionario involucrado de forma personal en algún delito federal puede ocasionar al gobierno es muy difícil de predecir, pero según sea su posición en el esquema formal o del poder real del gobierno, las consecuencias políticas y sociales pueden ser sustanciales. También sería justo que, por más que el servicio no debe condicionar el accionar del poder judicial, si debe valorar y comunicar los efectos que decisiones penales podrían implicar sobre la realidad social de la comunidad.

En suma, los delitos de las personas deben ser juzgados y penados, y la influencia que la persecución del delito acarree sobre lo político, no puede ser la prioridad. Es cierto que esos casos tendrán efectos a corto plazo quizás hasta perjudiciales para la sociedad, pero ¿no mejorarán la cultura política en el largo plazo?, ¿no llegarán mejores personas a los lugares de conducción si no hay lugar para narcopolíticos, por ejemplo?. Por otra parte, quizás de guante blanco, ¿qué lugar juegan los

aportantes “en negro” de las campañas electorales que después reclaman la devolución de su generosidad?.

El político o funcionario que delinque se convierte en delincuente, desde ese momento dejó los honores de representación de la comunidad, para representar intereses diferentes. No debe contar con inmunidad judicial, fueros o privilegios, usando al pueblo como rehén para no ser juzgado por los delitos que pudo haber cometido.

Volviendo a la opinión de Salomón, sobre la formación del recurso humano de los organismo de inteligencia consideró que: todo agente sobre todo un analista debe tener una formación muy, pero muy sólida en lógica. Nadie puede desempeñar su función profesional sin tener muchísima robustez en ese ámbito de la ciencia. La lógica brinda las herramientas para que el analista consiga desempeñar su función con mayor objetividad, y menores sesgos, le dará herramientas para que eventualmente identifique esos sesgos y pueda volcarlos dentro del análisis. El consumidor del producto de inteligencia debe tener acceso a comprobar cómo se llegó a determinada conclusión, y la lógica brinda de la mano de los métodos de análisis una forma científica de justificar aquello que se prospecta sobre determinado hecho o fenómeno.

Es decir que para este rol no se puede usar la intuición, o una percepción que no esté suficientemente constatada. Es por eso que analizar información en grupo puede dar mayor ecuanimidad pero siempre y cuando no haya una mayoría con un sesgo muy marcado que condicionen la opinión de una minoría. Los sesgos van a estar y hay que registrarlos para conseguir un producto de mayor calidad.

En palabras de David Omand[47], ”Se necesita una variedad de habilidades, probablemente no todas se encuentren en una sola persona. Así que el trabajo en equipo es esencial. La capacidad de comprender la tecnología de las redes sociales, incluida la tecnología publicitaria que la impulsa. Conocimiento de la psicología humana y cómo las personas se comportan (mal) en línea. Habilidades

[47] David Omand, Ex Director del Government Communications Headquarters (GCHQ), organismo responsable de la recolección de inteligencia de señales (SIGINT) en Reino Unido, entre 1996 y 1997. Entrevistado el 17 de abril de 2020.

lingüísticas relevantes (incluido el argot del grupo que es el objetivo y habla en internet). Sensibilidad a la posibilidad de engaño y falsificaciones. Conocimiento profundo del grupo objetivo (criminal, terrorista, etc.)".

La Agencia Federal de Inteligencia y el sistema en general carecen no sólo de una buena imagen pública, sino también de una legitimidad política, debido a múltiples factores y uno de ellos es una desmedida cultura del secreto. El camino para mejorar esto sin dudas es comenzar a transparentar mucho más las funciones de la agencia y conservar en secreto lo profesionalmente necesario.

El mejor camino para que la producción de conocimiento en redes sociales no vulnere el derecho de protección de datos personales debe estar dado por el fin ético que tenga la reunión de información. Recolectar información que ayude a combatir los delitos que afectan a la comunidad, por ejemplo con el fin de desarticular una banda delictiva vinculada al narcotráfico, la venta ilegal de armas, al terrorismo o cualquier delito federal, es una acción positiva que busca proteger los intereses del Estado y de los argentinos. Reunir información bajo estos fines es una acción permitida por la ley de protección de datos personales, ya que serán datos que se recaben para el ejercicio de funciones propias de los poderes del Estado y para ello la ley prevé que no se necesita consentimiento por parte del dueño de los datos personales.

Desafíos del largo plazo

Para profundizar sobre los desafíos a largo plazo, entrevistamos a Mariana Márques, quien es Directora de Justicia y Política Internacional de la ONG Amnistía Internacional y fue responsable del informe "El debate público limitado. Trolling y agresiones a la libre expresión de periodistas y defensores de DD.HH en Twitter Argentina" publicado en Marzo de 2018.

Dicho informe demuestra cómo se vulnera, de forma organizada y clandestina, la libre expresión y el derecho de protección de los datos personales de diferentes referentes de DD.HH. y periodistas en Argentina en la red social Twitter.

La persona u organización clandestina, mencionadas en el informe como “Ciber Tropas”, producen conocimiento en base a “datos sensibles”, que luego utilizan para la toma de decisiones y ejecución de sus acciones en Twitter. De hecho, ser referente del colectivo de DD.HH. en un país, es sin lugar a dudas pertenecer a un grupo ideológico y político, y esto constituye un “dato sensible” de cada persona.

Mariana Márques opinó sobre la complejidad de regular el uso de datos personales por parte de estas organizaciones clandestinas, en que lo principal es exigir a las compañías dueñas de las redes sociales que tengan políticas activas sobre aquellas cuentas que tienen comportamientos que vulneren la libertad de expresión de otras. Otra iniciativa podría ser dar de baja aquellas cuentas que es evidente que actúan como robots, repitiendo contenido, agraviando sistemáticamente a determinados actores ejerciendo acoso, asumiendo un rol más activo desde las compañías.

Facebook e Instagram, que son de la misma empresa, tienen políticas más robustas en materia de protección de datos personales y están más comprometidas en este aspecto que Twitter. Un ejemplo de ello es que Facebook pide a los usuarios su identidad real y te permite crear una sola cuenta por persona, mientras que Twitter es más laxo disponiendo hasta cinco cuentas registradas con un mismo email y/o usuario. También es reconocible que Facebook, en muchos casos, buscando proteger datos personales o privacidad, incurre en censuras.

También es un hecho que por el diseño funcional de Twitter, se promueve indirectamente la interacción, y en consecuencia, la agresión entre usuarios.

Sobre el tema del anonimato en Internet, Amnistía no considera al momento promover alguna legislación que genere una identidad virtual, o un método que permita regular las interacciones y que pueda haber responsables por cada hecho u opinión en la red. Por el contrario, la ONG con base Argentina ve con buenos ojos que exista libertad y desregulación, para que los usuarios no se vean siempre individualizables y que esto genere una autocensura. A su vez, el anonimato muchas veces permite géneros discursivos como la sátira que enriquecen la libertad de pensamiento y cuestionan al poder concentrado de los discursos dominantes.

Sobre los casos que estudiaron en el informe nos comentó que la operatoria de estos grupos se inicia en la función de “figuras habilitadoras”, que son usuarios reales representativos en la red que inician una crítica a un usuario, identificandolo públicamente como el objetivo de hostigamiento para la “Ciber Tropa” en la comunidad en Twitter. Sobre dicho usuario la “Ciber Tropa” ejercerá el acoso mediante ataques discursivos, limitando así la opinión de la víctima sobre determinada temática.

Estos ataques discursivos en oportunidades incluyen como herramienta la acción, ya descrita en este trabajo, conocida como *Fake News.* La táctica consiste en crear una noticia falsa sobre el usuario “blanco” que sirva para degradar su honor (vulnerando su derecho al honor) o su estándar ético, buscando mostrar contradicción en sus valores personales o la incursión en algún delito normado por la ley.

Tal como desarrollamos en el apartado sobre noticias falsas, éstas son de especial relevancia para ésta tesis por el hecho de que casi siempre contienen la categoría de “datos sensibles” que dispone la Ley Nacional de Datos Personales, buscando exponer al usuario blanco y a su vez ganar verosimilitud e impacto en las repercusiones de la acción.

Como sugerencias de parte de Amnistía Internacional, Mariana Marques consideró que lo más importante es la educación a los usuarios, que sean conscientes de que estas operaciones existen, dado que en muchas oportunidades los usuarios genuinos participan sin saber, de buena fe o reproducen contenido falso que puede perjudicar el nombre y honor de otra persona. Hay una tarea pendiente por parte del Estado y las instituciones de la comunidad en generar concientización en la comunidad de redes sociales.

Las empresas, todas, y las de redes sociales también, son responsables de proteger los derechos humanos. Amnistía reconoce que hay problemas en este sentido y que todos los actores deben comprometerse más para evitar las violaciones a los DD.HH. en su ámbito.

Para Amnistía, el rol de las campañas políticas en redes sociales merece un capítulo aparte en esta discusión. Ya en varios países los partidos políticos que compiten en elecciones democráticas abiertas celebran lo que se denomina un "acuerdo de no violencia online" buscando mitigar el nivel de agresiones entre los actores que pugnan por un cargo y entre los usuarios de la red social en general.

Casos como el de Cambridge Analitica con Facebook, dispararon las alertas en las comunidades más involucradas en las nuevas tecnologías, sobre lo que el uso legal pero inadecuado de las redes sociales pueden representar en los escenarios electorales.

La visión a de la Agencia Federal de Inteligencia

Durante la entrevista que se le realizó a la actual interventora de la agencia, Cristina Caamaño, consideró qué aspectos consideran y valoran los decisores políticos de la AFI. "Si bien la Agencia Federal de Inteligencia se encuentra en un proceso de refundación institucional, estamos construyendo las capacidades para que su función sea la producción de inteligencia estratégica y el trabajo con otros organismos nacionales e internacionales en materia de prevención del terrorismo".

"Hoy, estamos viendo los primeros resultados y las máximas autoridades nacionales comenzaron a referir que los informes que realizamos son de utilidad al momento del diseño de políticas públicas. Obviamente, no puedo dar a conocer ni el tema ni el contenido, pero sí que fue un proceso que iniciamos al comienzo de la Intervención, en paralelo con la enorme tarea de hacer ingresar al Estado de Derecho a la AFI, lo cual no fue sencillo".

Consultada sobre cómo debe ser la formación de un analista de inteligencia, Caamaño opinó que "el analista debe especializarse en un tema puntual, de modo de no iniciar el camino cada vez que aborda una temática específica. El trabajo del analista es un eslabón del proceso de producción de inteligencia y debe ceñirse a las necesidades de inteligencia que originaron el requerimiento de información. En

ese sentido, además de la formación específica sobre la producción de inteligencia estratégica, el analista debe mantenerse actualizado en su disciplina y en la temática específica a la cual se dedica".

"No sirve un analista que sepa un poco de todo, por el contrario lo necesario es que sepa mucho de algo. Por eso, el proceso de formación necesita de tiempo, diría que de años. Nosotros nos encontramos con una AFI casi sin capacidad de análisis, ya que se encontraba dedicada al espionaje ilegal".

Por otra parte, la interventora a cargo de la AFI comentó que "la Escuela Nacional de Inteligencia tenía un muy bajo nivel académico. Actualmente, nos encontramos en proceso de certificar los programas y los títulos con el Ministerio de Educación, ya que descubrimos que los programas no contaban con la aprobación oficial y que, nos llamó aún más la atención, en muchos casos los certificados se extendían con el nombre supuesto, lo que significaba que no servían para sumar a un CV como antecedente".

La sociedad virtual

La virtualidad de nuestras vidas hoy es un fenómeno fuera de discusión, en este sentido, prevemos que tomarán mayor protagonismo los derechos y obligaciones que se ponen en tensión para consolidar nuevos y más avanzados estándares de convivencia en las sociedades. Surgirán nuevos medios de comunicación y de relacionamiento virtuales y reales que plantearán nuevos desafíos y a través de los cuales transitarán, invariablemente, datos personales.

La consulta y la opinión técnica, legal y experta mantendrá mayores espacios en común con la opinión horizontal de la comunidad a través de las mismas redes sociales y a través de las organizaciones del tercer sector, cada vez más involucradas e influyentes en el campo. Este camino posiblemente reducirá los márgenes para caer en visiones parciales y de afectaciones injustas sobre las mayorías.

A lo largo de este trabajo fuimos comprendiendo de forma más acertada como la capacidad legislativa encuentra su mayor dificultad, en el tiempo que demandan los procesos, y la modificación del escenario para el que legislan. Por eso la capacidad de adaptación a la velocidad de internet y de las necesidades sociales modernas es cada vez más limitada al punto de tornar ineficiente casi cualquier medida que por vía legislativa tradicional, se le intente regular.

Ante este escenario que plantea el desafío del manejo del tiempo para la toma de decisiones sería importante contemplar alternativas administrativas que puedan ejercer un rol a la hora de decidir sobre los derechos y obligaciones de los sujetos y de los diferentes actores que hacen al uso de los datos personales y a la aplicación de la inteligencia estratégica, preservando las libertades individuales y las autonomías y soberanías de los diferentes países.

Habida cuenta que las tecnologías permiten hoy la opinión y el flujo de datos de manera más sencilla también se abren numerosos desafíos en el área electoral y de participación ciudadana, donde los procesos electorales y plebiscitarios del futuro encontrarán la posibilidad de elegir de forma virtual sobre alternativas. El desafío de gestionar estos mecanismos tomando la opinión de las mayorías de forma directa puede representar mejoras sustanciales en el ejercicio de la democracia.

De la mano de este planteo, otro de los desafíos que vemos como un emergente después del estudio de los diferentes fenómenos, es el que tiene que ver con la identidad digital. Para este planteo se abrirá un debate sobre la libertades del anonimato y el derecho a la identidad.

Si pudiésemos vincular cada identidad de una persona física con su identidad virtual de manera identificable y determinable en internet podríamos otorgar de mayor transparencia al entorno virtual. Sin embargo, si esta verificación de la entidad virtual de las personas pasa a ser una obligación legal, podría abrir nuevos escenarios que restrinjan las libertades personales.

El anonimato en internet tiene también un sentido favorable hacia la libertad de opinión. En algunos Estados totalitarios tener determinadas opiniones no son

compatibles con la posibilidad de asumir legal y públicamente la autoría de las mismas, y esto tiene que ver con la posibilidad cierta de recibir represalias por parte de estos Estados autoritarios poniendo en riesgo los bienes económicos, la libertad personal e incluso la vida.

Probablemente habrá países donde las libertades personales, el desarrollo político y democrático moderno le permita a los ciudadanos emitir opiniones sobre diferentes aspectos de la vida social, cultural y política de manera libre y sin sufrir por esto persecuciones ni represiones. Pero posiblemente sigan coexistiendo con países y culturas donde esto no sea una posibilidad.

Desarrollar un marco de respeto a las decisiones soberanas de cada país y cada cultura plantea un desafío interpretativo y de convivencia con el que las próximas generaciones deberán convivir.

Es por eso que la posibilidad de dotar de una transparencia total a las comunicaciones en internet es un escenario que generaría beneficios para algunos y grandes perjuicios para otros según su contexto. Y esa transparencia nunca debería traslucir los datos personales que ponemos a disposición consentida de diferentes organizaciones.

Sería deseable que esta demanda de la sociedad y de las organizaciones del tercer sector interpretada por los cuerpos legislativos, encuentre también su cauce en el Poder Judicial con mayores iniciativas para que los cambios inminentes en las legislaciones se consoliden en el tiempo como una política pública de Estado, que trascienda los diferentes gobiernos con la más alta aprobación y efectividad posible.

Servicios de inteligencia y datos personales: recomendaciones de la ONU

Los servicios de inteligencia desempeñan un papel fundamental en la protección de los Estados y sus poblaciones contra las amenazas a la seguridad nacional, incluido el terrorismo. Gracias a estos servicios los Estados pueden cumplir su obligación de

salvaguardar los derechos humanos de todos los individuos bajo su jurisdicción. De ahí que un funcionamiento eficaz y la protección de los derechos humanos puedan ser objetivos mutuamente complementarios de los servicios de inteligencia.

La Organización de las Naciones Unidas ha desarrollado un trabajo sustantivo en cuanto a recomendaciones para los servicios de inteligencia.

En 2010, el Consejo de Derechos Humanos, de la Asamblea General de Naciones Unidas publicó el documento *"Marcos jurídicos e institucionales para promover los derechos humanos y el respeto por el estado de derecho en la labor de los servicios de inteligencia"*[48].

Las buenas prácticas a las que se refiere el documento abordan los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión.

Como se observará, una cantidad significativa de recomendaciones se refieren a temas vinculados con la protección de datos personales.

En base al alcance de cada una de ellas y en función del objetivo de la presente investigación se ha realizado un análisis individual de cada una que se ofrece de modo sintético. Se profundizó en las recomendaciones con mayor relación al tema de esta tesis.

[48] Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo* Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión https://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46_sp.pdf

Buenas prácticas

1. No involucrarse en seguridad ciudadana: La recopilación, análisis y difusión de información pertinente para la protección de la seguridad nacional es una tarea fundamental de la mayor parte de estos servicios, y muchos Estados limitan la función de sus servicios de inteligencia a esta tarea. Esto supone una buena práctica, porque impide que los servicios de inteligencia se dediquen a actividades relacionadas con la seguridad que ya son de la incumbencia de otros organismos públicos y que, si corrieran por cuenta de los mencionados servicios, podrían poner en peligro los derechos humanos.

2. Definir los mandatos del servicio a través de una ley nacional que sea de público conocimiento: La ciudadanía tiene que tener acceso a comprender con rigor y precisión cuales son las amenazas que aborda el servicio, a través de leyes y políticas públicas sin definiciones generalistas o ambiguas o que se presten a múltiples interpretaciones.

3. Facultades para terrorismo, sólo para terrorismo:

Esta recomendación sugiere que el poder legislativo debe hacer una enumeración exhaustiva de las facultades y competencias de los servicios de inteligencia para favorecer la transparencia y permitir que la población prevea cuáles de esas facultades podrían utilizarse en su contra. Esto es especialmente importante, porque muchas de las facultades conferidas a los servicios de inteligencia encierran el potencial necesario para vulnerar los derechos humanos y las libertades fundamentales. Por otra parte tener definiciones precisas por ejemplo en Terrorismo, ayuda a una mejor coordinación internacional, estandarizando la definición de grupos y actividades terroristas para posibilitar la cooperación y un abordaje global más eficiente, dadas las características, especialmente internacionales de esta amenaza.

4. Publicidad:

Algunas actividades del organismo pueden coartar Derechos Humanos, por esto resulta importante que no haya reglamentos paralelos a las leyes públicas en materia de Inteligencia y en el caso de que se necesiten reglamentaciones específicas siempre deben ser públicas o basarse en leyes vigentes a las que el público tenga acceso.

5. Dentro de la Constitución Nacional y de las normativas internacionales sobre DDHH:

Toda actividad debe estar dentro de estos parámetros, como cualquier otro organismo estatal. Ninguna autoridad podrá solicitarle que vayan en contra de estos límites.

6. Supervisión de una institución civil:

Si bien muchos países cuentan con controles internos, ejecutivos, parlamentarios y judiciales de sus servicios de inteligencia, es importante que ese trabajo combinado sea integrado por al menos una institución civil de prestigio y con una independencia del poder ejecutivo y del propio servicio. Este control integral debe contemplar todos los aspectos de la labor de los servicios de inteligencia, con inclusión de su observancia de la ley, la eficacia y eficiencia de sus actividades, su situación financiera y sus prácticas administrativas.

7. Las instituciones de supervisión deben contar con facultades, recursos y conocimientos técnicos para iniciar sus propias investigaciones.

También es preciso que tengan acceso completo a la información, a los funcionarios y a las instalaciones que sean útiles para cumplir con su trabajo. Se les debe garantizar pleno acceso a documentos y archivos como así también se les debe permitir convocar a cualquier miembro del servicio para que testimonie bajo juramento. Gracias a estas facultades, los supervisores pueden examinar eficazmente las actividades de los servicios de inteligencia e investigar en detalle los posibles incumplimientos de la ley.

8. Aplicar sanciones a los miembros de las instituciones de supervisión:

Aquellas que no cumplan con la cadena de confidencialidad de la información y de los datos personales sobre los que tengan acceso. Debiendo tomar además protocolos y medidas institucionales que protejan dichos datos. Tener en cuenta que el revelar información confidencial a veces se da de forma deliberada y otras por inadvertencia. Se pueden usar mecanismos de control antes de dar acceso a sus miembros, acuerdos de confidencialidad y fundamentalmente capacitación, que concientice a cada trabajador sobre el valor de la información que maneja y del por qué de sus cuidados.

9. Derecho a denunciar a los organismos de inteligencia:

Se recomienda que se garantice el derecho de denunciar ante un tribunal o ante una institución de supervisión (por ejemplo la Defensoría del Pueblo), a toda persona que crea que sus derechos han sido vulnerados por parte de acciones ilegales de un servicio de inteligencia con el fin de acceder a la protección de sus derechos, a la reparación y a la plena compensación por los daños sufridos.

10. Que las instituciones que tramitan denuncias tengan la facultad jurídica necesaria para dictar órdenes reparatorias de cumplimiento obligatorio:

Producto de las investigaciones sobre las denuncias recibidas. Las mismas deberán trabajar permanentemente para mantener independencia de los servicios y del poder ejecutivo. Promoviendo la transparencia y una gestión ética y equitativa de sus recursos.

11. Prohibir la discriminación por “datos sensibles”:

De modo que no se promueva o se vaya en contra de los intereses de cualquier grupo étnico, religioso, político. Los Estados deben asegurar que las actividades de sus servicios de inteligencia se basan en el comportamiento de los individuos, y no en su etnia, religión u otro criterio análogo. Algunos Estados han prohibido

explícitamente a sus servicios de inteligencia la constitución de archivos individuales, sobre criterios de datos sensibles.

12. Prohibir involucramiento en actividades político-partidarias:

Tomar las medidas necesarias para que los servicios no promuevan o protejan los intereses de cualquier grupo político, religioso, lingüístico, étnico, social o económico. Un ejemplo de esto es la prohibición de que los empleados de los servicios de inteligencia sean miembros de partidos políticos. También es recomendable que la duración del mandato del director/a del servicio esté estipulado por disposiciones jurídicas, como así también se especifiquen los motivos para su destitución.

13. Prohibir la afectación de la libertad de expresión, asociación o reunión de las personas:

Estos derechos son fundamentales para el funcionamiento de una sociedad libre, en el que participan los partidos políticos, los medios de comunicación y la sociedad civil. Por consiguiente, se recomienda a los Estados adoptar disposiciones para reducir la medida en que los servicios de inteligencia pueden elegir como blanco de sus operaciones (o la medida en que se les puede pedir que lo hagan) a personas o grupos dedicados a estas actividades.

14. Los Estados son internacionalmente responsables de las actividades de sus servicios:

Ya sea de forma directa o a través de un contratista privado, los Estados deben asumir la plena responsabilidad de control sobre las actividades en el extranjero de sus servicios e independientemente de quién sea el blanco de un hecho internacionalmente ilícito. Dichas políticas de control deben ajustarse a promover el respeto por las normativas internacionales de Derechos Humanos y las disposiciones legales soberanas del país donde se desempeñen.

15. Las excepciones a la ley no pueden nunca vulnerar el derecho internacional o los derechos humanos:

De haber autorizaciones específicas para incumplir una ley nacional, las mismas deben ser de carácter excepcional y limitadas a través de otra ley que regule dicha autorización. Cual sea el caso, ninguna autorización por ley podrá permitir a un servicio de inteligencia vulnerar los derechos humanos o el derecho internacional.

16. Prever sanciones penales y civiles para quienes incumplan la ley:

Aquellos miembros o personas que actúen en nombre del servicio y que transgredan la legislación nacional o la normativa internacional de los derechos humanos, deben ser sancionados penal o civilmente según el caso. También deben ser extendidos estos procedimientos judiciales para aquellos jefes que den una orden violatoria de derechos a un subalterno.

17. Protección para empleados que se nieguen a obedecer órdenes violatorias a los Derechos Humanos:

No solo una protección, sino también debe ser una exigencia para todos los trabajadores del sistema de inteligencia nacional. Este tipo de normativas es más habitual dentro de las Fuerzas Armadas y las Fuerzas de Seguridad, se recomienda extender su disposición también en los servicios de inteligencia y contratistas privados si los hubiera.

18. Protección legal para trabajadores que denuncien hechos ilícitos:

Por la naturaleza de la actividad, frecuentemente trabajadores del servicio pueden detectar antes que la comunidad en general hechos ilícitos cometidos por su propio organismo, como violaciones a los derechos humanos, malversaciones financieras u otras infracciones a la ley. Es por esto especialmente que se recomienda al Estado que a través de su legislación dote a los trabajadores de los servicios de suficiente respaldo legal e institucional ante denuncias voluntarias y de buena fe. Si los procedimientos internos para denuncias de esta índole no son suficientes, se

recomienda la intervención de un organismo independiente que investigue los hechos y si la denuncia del trabajador tomara estado público, se recomienda arbitrar los medios para su adecuada protección laboral, legal y física.

19. Establecer por ley programas de formación y conducta adecuada:

En algunos Estados el ministerio a cargo del servicio decide hacer públicos los contenidos del programa de formación, o bien de un código deontológico, como gesto de responsabilidad política. También se recomienda que este programa de formación sea sometido a un examen pormenorizado de las instituciones de supervisión.

20. Aquellas medidas que coarten derechos y libertades deben cumplir estos criterios:

a) Que estén contempladas en leyes de acceso público y que respeten las normas internacionales de derechos humanos. b) Que sea estrictamente necesario para cumplir con el mandato legal del servicio. c) Que guarden proporción con el objetivo, disminuyendo al mínimo aquellos efectos desfavorables sobre los derechos de las personas. d) Nunca vulnerar elementos esenciales de derechos humanos o normas imperativas de derecho internacional. e) Que exista un sistema bien definido y completo para autorizar, y supervisar la aplicación de aquellas medidas que coarten los derechos humanos. f) Que aquellas personas que hayan sido blanco, siempre tengan derecho de presentar denuncias ante instituciones independientes con el fin de acceder a una reparación efectiva si le correspondiera.

21. La legislación debe fijar qué tipo de medidas de recolección de información les son permitidas aplicar a los servicios:

También los objetivos permisibles de la recopilación, las clases y actividades de personas sobre las que sí se puede recopilar, qué grado de sospecha justifica la recolección, durante qué plazos y el protocolo de los procesos mediante los que se auditará dicha recopilación. Tener todos estos factores definidos de forma clara a

través de una ley nacional reduce a un mínimo los abusos sobre el uso que el Estado le atribuye al servicio de inteligencia.

22. Una institución externa e independiente al servicio debe auditar aquellas medidas de recolección que coartan de manera significativa los derechos humanos:

Esta institución auditora debe tener poder de revisar, suspender o terminar la medida de reunión de información. También se recomienda que en especial estas medidas de gran suspensión de derechos, sea autorizada por el propio poder ejecutivo, además de por el propio servicio y la institución independiente auditora.

23. Transparencia sobre qué datos personales sí puede retener el servicio:

Más allá de que la Ley Nacional de Protección de Datos Personales prevé el uso autorizado de cualquier dato personal en virtud de las necesidades del Estado, la recomendación es que el criterio de utilización, retención, supresión y revelación de datos personales se instrumente, en el caso de los servicios, mediante una ley nacional pública específica sobre la que toda la comunidad tenga acceso. Allí debería estar determinado qué tipo de datos personales y bajo qué circunstancia gozan de uso autorizado por parte del servicio de inteligencia.

24. Obligación de actualización o supresión de datos personales:

Aquellos datos personales que ya no sean utilizados para el fin que la ley autoriza deben ser suprimidos asegurando un procedimiento seguro sobre la eliminación de dicha información. Con la misma frecuencia de tiempo, aquellos datos personales que sí deban permanecer archivados por motivos funcionales, deben ser actualizados, verificando así su pertenencia y su correlación con el dueño de los datos. También deben mantenerse almacenados aquellos datos que sean necesarios por razones de supervisión tanto por las instituciones de control como por el poder judicial.

25. Determinar una institución independiente como auditora de los datos personales que utiliza el servicio:

La misma deberá tener acceso a todos los archivos con los que trabaja el servicio y estar facultada para ordenar la revelación de los datos a las personas afectadas o bien ordenar la destrucción de los datos en los archivos de forma permanente.

26. El servicio debe justificar ante una institución independiente cuando decide no dar a conocer un dato personal ante el reclamo de su dueño:

Si un ciudadano reclama saber si tienen sus datos personales en archivos del servicio, se le deberá informar fehacientemente que datos tiene justificando su uso proporcional y necesario. El dueño tendrá derecho a actualizarlos y corroborarlos. Toda excepción a esta regla, es decir si el servicio por motivos funcionales decide negar el acceso a la información a su dueño, deberá justificarlo antes la autoridad de auditoría independiente.

27. Los servicios no están autorizados para ejercer facultades de arresto y detención de personas:

Estas actividades deben quedar reservadas para las fuerzas de seguridad pública en virtud de su mandato constitucional.

28. Si se autorizan las facultades de arresto y detención a miembros del servicio debe ser a través de leyes de público conocimiento:

Se recomienda una normativa muy clara al respecto. Los servicios de inteligencia no pueden privar de la libertad a individuos por la simple razón de que necesitan información. Ejercer la facultad de arresto obraría para casos razonables donde por ejemplo un individuo haya cometido o esté por cometer un delito concreto grave. Todo hecho de esta índole deberá ser sometido a examen judicial para corroborar su legitimidad.

29. Está prohibido aplicar tortura o tratos inhumanos:

Así tengan autorizado hacer detenciones en casos excepcionales, éstas nunca podrán ser a través de tratos degradantes o tortuosos, debiendo siempre atenerse a las normas internacionales de derechos humanos.

30. Está prohibido que los servicios tengan instalaciones de detención propia o a través de terceros:

Esta prohibición debe figurar en la legislación nacional. En los casos que tengan permitido el ejercicio de una detención en un caso excepcional la persona deberá ser trasladada a un centro regular de detención.

31. El intercambio de información entre agencias debe estar regulado por una legislación nacional:

Ya sea entre organismos de inteligencia de un mismo país o entre organismos de Estados extranjeros. Dichas operaciones deben estar bien descritas y definidas en la legislación, donde se explicite las condiciones de reunión, entidades autorizadas y demás consideraciones para proteger la información sensible y los intereses del país, sobre todo cuando esta información incluye datos personales.

32. Los intercambios de información con agencias extranjeras deben ser firmados por el poder ejecutivo:

Esta práctica se recomienda que esté además contemplada en una legislación nacional.

33. El servicio debe evaluar previamente los antecedentes del receptor de la información en materia de DDHH y Protección de Datos Personales:

Esta práctica tiene el fin de que la información enviada al servicio extranjero sea pertinente para el acuerdo establecido, reduciendo el riesgo de que la información se utilice para fines diferentes que los declarados.

34. Las instituciones independientes de supervisión del servicio pueden revisar los acuerdos de intercambio de información:

También deben poder hacerlo sobre cualquier otra información enviada a servicios extranjeros. De esta forma se le da un respaldo legal contemplando que el intercambio se haya ajustado a derecho, sobre todo cuando dicha información contenga datos personales.

35. Los servicios tienen prohibido recurrir a servicios extranjeros si esta solicitud incumple con las normativas nacionales o de control institucional:

Cuando pidan a servicios de inteligencia extranjeros que lleven a cabo actividades en su nombre, los Estados exigirán a estos servicios que observen la misma normativa jurídica que regiría si las actividades las llevaran a cabo sus propios servicios de inteligencia.

Este documento sugiere a los servicios de inteligencia no discriminar la información reunida bajo criterios de pertenencia a determinadas ideologías o religiones, por ejemplo como lo indica la recomendación N°11. También, tal como lo describe la recomendación N°21 se pide ser muy transparentes y precisos sobre qué tipo de datos personales pueden ser recolectados y cuáles de ellos almacenados. Debe haber absoluta claridad sobre lo permitido y lo prohibido, como se indica en la práctica N°23.

Otro aspecto que incluye el documento, en la práctica N° 24, y que muchas legislaciones sobre datos personales así lo sugieren, es el de la obligación de actualización o supresión de datos personales.

Por otra parte, en la práctica N°25, se indica la importancia de que haya una institución independiente como auditora de los datos personales que utiliza el servicio. Acá será clave la idoneidad y la ética que pueda brindar a su función de auditoría la organización que se convoque. Dado que por las características de la función del servicio, los dueños de los datos personales no van a tener conocimiento sobre el manejo de sus datos por el servicio y es donde cobra una importancia

sustancial el rol que pueda cumplir la organización a cargo de la auditoría, que será muchas veces el único ente de contralor que vele por el derecho de protección de los datos personales de la ciudadanía.

Asimismo, en la práctica N°26, se recomienda que el servicio justifique ante dicha institución independiente, cuando decide no dar a conocer un dato personal ante el reclamo de su dueño. Es una instancia muy interesante que pondrá en juego decisiones que pueden afectar tanto al secreto como al derecho de protección de datos personales.

Cuando se realicen envíos de información a otras agencias, tanto la institución que audite al servicio en esta materia como el plantel profesional del servicio, según la práctica N°33, se deberán tomar medidas para evaluar previamente los antecedentes en materia de DDHH y Protección de Datos Personales del receptor de la información. Considerando acuerdos (sugiere la práctica N°34) que protejan los derechos de los ciudadanos como así también los intereses nacionales que puedan estar en juego por compartir esta información.

CONCLUSIONES

El presente trabajo buscó echar luz sobre un fenómeno de creciente relevancia en lo concerniente a la protección de datos personales: el avance de las tecnologías de la información y comunicación (TICs), en especial en relación al desarrollo de las redes sociales en sus múltiples usos, y las implicaciones y condicionantes en materia de regulaciones.

La investigación comenzó con una descripción del estado de situación del fenómeno de las TICs en relación al uso de redes sociales y su impacto en la protección de datos personales. Seguidamente se indagó sobre la situación del marco de regulaciones a nivel nacional.

Posteriormente se presentó un relevamiento de las tendencias regulatorias en la región de Latinoamérica, así como en Europa (a partir de la normativa) y en los Estados Unidos. Con relación a esto, se observa un cambio de época en relación a la protección de los datos personales caracterizado por la búsqueda de ampliación de derechos, fundamentalmente protagonizado desde el poder legislativo y organizaciones de la sociedad civil de cada país, con acompañamientos por parte de los poderes ejecutivos. En algunos casos con mayor intensidad (como es el caso de la Unión Europea) y en otros con impulsos más resistidos (como son los casos de Venezuela y Brasil).

Seguidamente se presentaron los aspectos más sobresalientes del proceso de regulación en Argentina, su estado de situación y sus avances.

Por último, este trabajo buscó identificar los desafíos más apremiantes en materia de regulación de datos personales frente al avance de las TICs

Complementariamente, este trabajo se nutrió de relevantes aportes provenientes de entrevistas realizadas a expertos de gran renombre, tanto a nivel nacional como internacional. Se caracterizaron los aspectos más relevantes de entrevistas realizadas a especialistas.

Tendencias

Tal como se observa, la tendencia global en tecnologías de la información implica un aumento de los flujos de comunicación a nivel exponencial. Esto, dado en el contexto del uso de redes sociales (o social media), presenta un gran desafìo a la gestión de la protección de los datos personales.

Como se destacó al inicio, la inteligencia, entendida como la producción de conocimiento para la toma de decisiones, es un recurso estratégico para las organizaciones que determinará el crecimiento económico, el progreso democrático (sobre todo en el sector público) y el mayor acceso a derechos para nuestra comunidad. Desaprovechar este recurso significaría ceder un potencial determinante para las organizaciones, no obstante, dicho desafío implica esfuerzos en el área legal, ética y metodológica.

Con respecto a las tendencias regulatorias, se identifica un aumento de la gravedad de las sanciones que estipulan las leyes, política que de resultar efectiva sin dudas será de gran ayuda para determinar el éxito de las nuevas legislaciones sobre protección de datos personales, y una motivación para inculcar el cambio cultural que está haciendo falta dentro de la mayoría de las organizaciones.

En base a las entrevistas efectuadas a actores del sector, en general, los entrevistados creen que la regulación no va a ser suficiente para proteger los datos personales. Siempre puede haber registros o archivos no controlados, sin declarar a la autoridad de aplicación y en gran medida el control sobre ellos se dificulta ante la imposibilidad de auditar todos los sistemas informáticos de una organización. Por esto la importancia de promover cambios culturales y políticas internas que premien los buenos usos y castiguen los malos, siendo los referentes de cada organización quienes deben liderar desde el ejemplo las buenas prácticas.

Proyecto de ley

Durante la presidencia de Mauricio Macri, el gobierno envió al Congreso, a través de la Agencia de Acceso a la Información Pública (AAIP), en septiembre de 2018 un

proyecto de ley que buscaba derogar la actual ley 25.326 de Protección de Datos Personales y proponer a lo largo de 95 artículos, una nueva ley para reemplazarla.

Cabe mencionar que el proyecto perdió estado parlamentario el 29 de febrero de 2020.

Este proyecto girado al Congreso por la AAIP planteó, en principio, mayores controles y restricciones sobre el manejo de datos de los ciudadanos, crea mecanismos de protección para datos sensibles, nuevas sanciones para quienes no se adecuen o violen la normativa.

Como novedad se incorpora la obligación de que las organizaciones reguladas notifiquen cuando existan incidentes de seguridad en las bases de datos personales dentro de las 72 horas y en consecuencia la obligación de realizar una evaluación de impacto sobre los potenciales daños que dicho incidente podría provocar sobre los derechos de los titulares de los datos.

El proyecto obliga a adoptar medidas proporcionales a las modalidades y finalidades del tratamiento de los datos, su contexto, su tipo y categoría de datos tratados. También deben informar sobre el riesgo que dicho tratamiento pueda representar sobre los derechos del titular.

Los titulares, de aprobarse este proyecto, tendrán derecho de oponerse a que sus datos sean objeto de una decisión tomada en base a un tratamiento automatizado. Esto plantea un punto interesante de cara al crecimiento exponencial de la Inteligencia Artificial.

Dentro del articulado se mencionan los derechos sobre la posible transferencia internacional de datos personales, en un contexto de flujo global de datos e información a través de internet, este apartado tiene un significado mucho más relevante y actual. Se permitirá la transferencia internacional solo con el consentimiento expreso del titular, si a su vez el país u organismo proporciona un nivel de protección adecuado, si Argentina mantiene un tratado o bien si de la

transferencia de los datos dependieran temas vitales de la salud como la prevención, tratamiento o diagnóstico médico.

Por otra parte, el derecho de acceso a los titulares será dado previa acreditación de su identidad, a quienes se les deberá suministrar los datos que se tienen de ellos para el tratamiento de forma clara, exenta de codificaciones y en ese caso acompañada de una explicación, en un lenguaje accesible al conocimiento medio de la población.

Para aquellas organizaciones que no cumplan con la legislación se extenderán multas y sanciones que contemplan la suma de hasta quinientos salarios mínimos, suspensión de las actividades relacionadas con el tratamiento de los datos hasta por seis meses, suspensión definitiva de actividades si una vez cumplido el plazo no hubieran adoptado medidas correctivas.

La figura del Delegado de Protección de Datos Personales será obligatorio para los casos de autoridades u organismos públicos o si se realizan tratamiento de datos a gran escala.

Por otra parte, en el caso de nuestro país, el proyecto de ley que se estaba tratando no considera un Delegado de Protección de Datos Personales para organizaciones que traten datos a media o baja escala. Lo cual si bien guarda un criterio de proporcionalidad a su vez expone a mayor vulnerabilidad aquellos datos personales que sean manejados por organizaciones de este tamaño. También es difuso el criterio sobre qué organizaciones tratan datos a gran escala y cuáles no.

Sobre los incidentes de seguridad a los que se refiere el proyecto también existe una “zona gris”, ya que el único medio que tiene la autoridad de aplicación para tomar conocimiento sobre un incidente, es la notificación del propio regulado. Y como es esperable, reconocer una falla en el control de los archivos puede significar un punto bajo para la imagen de la organización, y que esto no favorezca los casos de denuncias voluntarias.

En este escenario es válido preguntarse si un texto estático y concluyente como lo es el de una ley puede acompañar la dinámica antes descrita. Si bien toda ley es modificable, el proceso burocrático de los cuerpos legislativos sumados a los momentos políticos siempre variables, nos dan la pauta de la baja probabilidad de que una adaptación razonable suceda con la inmediatez esperada.

Para que los procesos de protección de datos personales corran con mayor suerte dependerán de autoridades de aplicación lo más independientes y autónomas posibles y esto se logrará en la medida que la política pública que determine la autonomía de éste organismo cuente con un consenso generalizado de la sociedad, de los poderes del Estado, de los partidos políticos, ONG,s etc.

Otra conclusión a la que llegamos es que el avance de la tecnología desafía la capacidad regulatoria de la ley y su velocidad de adaptación. Esta característica fue mencionada en más de una oportunidad durante las entrevistas realizadas y los textos analizados. El rasgo de permanente cambio y evolución de las tecnologías informáticas y de la comunicación parecen no tener un techo y siempre encuentran nuevos procesos y soluciones que superan las hipótesis más ambiciosas.

En este sentido, una deuda a saldar en los próximos tiempos será el mecanismo de elección de los directores o jefes de los organismos de control. Si la elección es vía decreto del poder ejecutivo, o mediante acuerdos partidarios en las cámaras legislativas, la autonomía de los organismos de control se verá seriamente afectada.

Creemos que la regulación aplicada desde 2018 por la Unión Europea podría llegar a ser el prototipo de legislación sobre el que debemos tomar ejemplo, pero a su vez será de radical importancia capitalizar la experiencia europea dándole un seguimiento permanente a la aplicación y a su grado de efectividad.

"Que la democracia y los derechos humanos no sean un techo para la producción de inteligencia, sino una plataforma desde donde partir"[49].

[49] Cristina Caamaño, Interventora de la Agencia Federal de Inteligencia (AFI). Entrevista realizada el 21 de marzo de 2021.

FUENTES Y BIBLIOGRAFÍA

Libros y artículos:

Omand, David*,* Introducing Social Media Intelligence (SOCMINT)*, in Jamie Bartlett & Carl Miller, Intelligence and National Security,* Editorial Routledge, England and Wales, 2012.

Heuer Jr., Richards, How does analysis of competing hypotheses (ACH) improve intelligence analysis?, Pherson Associates, 2005.

Heuer Jr., Richards, Psychology of Intelligence Analysis, Center for the study of intelligence, Central Intelligence Agency, 1999.
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Lowenthal, Mark M., Intelligence: From Secrets to Policy, Editorial CQ Press; 7th edition, 2017.

Bartlett, Jamie, Policing in an information age, *in Carl Miller, Jeremy Crump & Lynne Middleton,* Editorial Demos, 2013.
https://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365

Bartlett, Jamie, The state of the art : a literature review of social media intelligence capabilities for counter - terrorism, *& Carl Miller,* Editorial Demos, 2013.
https://www.demos.co.uk/files/DEMOS_Canada_paper.pdf

Bartlett, Jamie, The state of the art : a literature review of social media intelligence capabilities for counter - terrorism, *& Carl Miller,* Editorial Demos, 2015.
https://www.demos.co.uk/wp-content/uploads/2015/09/State_of_the_Arts_2015.pdf

Miller, Carl, The promise of Social Media, Demos Website, 2014.
https://quarterly.demos.co.uk/article/issue-1/the-promise-of-social-media/

Bartlett, Jamie, @metpoliceuk how twitter is changing modern policing, *& Carl Miller,* Demos Website, 2013.
https://www.demos.co.uk/files/_metpoliceuk.pdf?1371661838

Omand, David, A balance between security and privacy online must be struck, *in Jamie Bartlett & Carl Miller,* Editorial Demos, 2012.
https://www.demos.co.uk/wp-content/uploads/2017/03/intelligence-Report.pdf

Bruneau, Thomas, Intelligence and democratization the challenge of control in new democracies, *& Kenneth Dombroski,* Institutional Archive of the Naval Postgraduate School, 2000.
http://hdl.handle.net/10945/47008

Hammond, Philip, National Cyber Security Strategy 2016-2021, UK Government, 2016.
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf

FBI, Request for Information: Social Media Application, Department of Justice, Washington, DC, 2012.
https://www.fbo.gov/utils/view?id=7f9abf0ff0fdba171d1130ddf412aea3

Guillard, Julia, Strong and Secure: A Strategy for Australia's National Security, *Department of the Prime Minister and Cabinet*, Commonwealth of Australia; Canberra, 2013.
https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf

Kaplan, Andreas M., Users of the World, Unite! The Challenges and Opportunities of Social Media, *& Michael Haenlein*, Business Horizons, 2010.
http://michaelhaenlein.eu/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf

Stobbe, Antje, How companies are tapping the benefits of Web 2.0, Digital Economy and Structural Change, Deutsch Bank Research, 2010.
https://pdfs.semanticscholar.org/4774/7ec672d1f3eb4c0d699411d09f3ed7a9c67b.pdf

Best, Richard, Open Source Intelligence (OSINT): Issues for Congress, *& Alfred Cumming,* Congressional Research Service, Congressional Research Service, Washington DC, 2007.
https://fas.org/sgp/crs/intel/RL34270.pdf

Fleisher, Craig S., Using open source data in developing competitive and marketing intelligence, European Journal of Marketing, 2008.
https://www.emeraldinsight.com/doi/abs/10.1108/03090560810877196

Golden, James, OSINT and the Pharmaceutical Enterprise, In: Bio IT World, Cambridge Healthtech Institute, 2007.
http://www.bio-itworld.com/issues/2007/nov/insights-outlook-osint/

Lankes, David R., Credibility on the internet: Shifting from Authority to Reliability, Journal of Documentation, 2008.
https://www.emeraldinsight.com/doi/abs/10.1108/00220410810899709

FBI, National Gang Threat Assessment, National Gang Intelligence Center, Washington, 2011.
https://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment

Bastian, M., Gephi: an open source software for exploring and manipulating networks, *in S. Heymann and M. Jacomy,* In: International AAAI Conference on Weblogs and Social Media, 2009.
http://www.aaai.org/ocs/index.php/ICWSM/09/paper/download/154/1009

Barnes, R., Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement, Network Working Group, internet Engineering Task Force. 2015.
https://www.rfc-editor.org/rfc/pdfrfc/rfc7624.txt.pdf

Electronic Frontier Foundation, The International Principles on the Application of Human Rights to Communications Surveillance, 2014. https://en.necessaryandproportionate.org

Ferrari, Verónica, State Communications Surveillance and the Protection of Fundamental Rights in Argentina, *& Daniela Schnidrig,* The Electronic Frontier Foundation, 2016.
https://necessaryandproportionate.org/files/argentina_en_august2016_1.pdf

OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (The Privacy Guidelines). 2013.
https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Omand, David, Understanding Digital Intelligence and the Norms That Might Govern It, GCIG Paper, CIGI and Chatham House. 2015.
https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf

Bazzell, Michael, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, Inteltechniques.com, Fifth edition, 2017.

Fedotov, Yury, Uso de internet con fines terroristas, Oficina de las Naciones Unidas contra la droga y el delito, Viena, Austria, 2013.

https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Leyes y convenios internacionales:

Declaración Universal de los Derechos Humanos, *Asamblea General de las Naciones Unidas*, 10 de diciembre de 1948.
http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Declaración Americana de los Derechos y Deberes del Hombre, *IX Conferencia Internacional Americana*, en Bogotá, Colombia, 1948.
http://www.infoleg.gob.ar/?page_id=1000

Pacto Internacional de Derechos Civiles y Políticos, *Asamblea General de las Naciones Unidas,* 16 de diciembre de 1966.
http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), *Organización de los Estados Americanos (OEA),* 22 de noviembre de 1969.
https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Convención sobre los Derechos del Niño, *Naciones Unidas,* 20 de noviembre de 1989.
http://www.un.org/es/events/childrenday/pdf/derechos.pdf

Ley Nacional de Protección de Datos Personales Nº25326, *El Senado y Cámara de Diputados de la Nación Argentina,* INFOLEG, Ministerio de Justicia y Derechos Humanos de la Nación, 2000.

Ley de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires N°1845, *Legislatura de la Ciudad Autónoma de Buenos Aires*, Centro de Documentación Municipal (CEDOM), 24 de noviembre de 2005.

Ley de Rectificación de Datos Personales de la Ciudad Autónoma de Buenos Aires N°4496/13, *Legislatura de la Ciudad Autónoma de Buenos Aires*, Centro de Documentación Municipal (CEDOM), 14 de mayo de 2013.

Ley de Defensa Nacional N°23.554, *El Senado y Cámara de Diputados de la Nación Argentina,* INFOLEG, Ministerio de Justicia y Derechos Humanos de la Nación, Abril de 1988.
http://servicios.infoleg.gob.ar/infoleginternet/anexos/20000-24999/20988/texact.htm

Ley de Inteligencia Nacional N°25.520, *El Senado y Cámara de Diputados de la Nación Argentina,* INFOLEG, Ministerio de Justicia y Derechos Humanos de la Nación, Noviembre de 2001.
http://servicios.infoleg.gob.ar/infoleginternet/anexos/70000-74999/70496/norma.htm

Ley de Seguridad Interior Ley Nº 24.059, *El Senado y Cámara de Diputados de la Nación Argentina,* INFOLEG, Ministerio de Justicia y Derechos Humanos de la Nación, Diciembre 1991.
http://servicios.infoleg.gob.ar/infoleginternet/anexos/0-4999/458/texact.htm

Otros artículos

El derecho a la privacidad en la era digital, *Naciones Unidas*, 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/%20RES/69/166&referer=/english/&Lang=S

Reglamento General de Protección de Datos (RGPD), Unión Europea, 2016. https://ec.europa.eu/info/law/law-topic/data-protection_en

Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *David Kaye,* United Nations General Assembly: Human Rights Council, 2017. http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22300&LangID=E

Regulaciones Globales

Data Protection Act (Reino Unido) https://www.gov.uk/data-protection

ANEXO I - ENTREVISTAS

Entrevistados

David Omand, Ex Director del Government Communications Headquarters (GCHQ), organismo responsable de la recolección de inteligencia de señales (SIGINT) en Reino Unido, entre 1996 y 1997.

Mariana Marques, Directora de Política y Justicia Internacional, Amnistía Internacional Argentina.

Eduardo Peduto, Director del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la CABA.

Jerónimo Pardo, Responsable del área Analytics de Illuminati Lab. Actualmente Account Manager en Analytical and Insights team de Google.

Hugo García, Jefe de la Central de Inteligencia Criminal, Prefectura Naval Argentina.

Roberto Uzal, Director de la maestría en Ciberdefensa y Ciberseguridad (UBA).

Alejandro Salomón, Ex director de la Escuela Nacional de Inteligencia, en Agencia Federal de Inteligencia (AFI), 2015-2019.

Eduardo Bertoni, Ex-Director de la Agencia de Acceso a la Información Pública (AAIP) (2017-2021). Actual representante ante el Instituto Interamericano de Derechos Humanos (IIDH).

Cristina Caamaño, Interventora de la Agencia Federal de Inteligencia (AFI).

Entrevistas

DAVID OMAND

Ex Director del *Government Communications Headquarters (GCHQ),* organismo responsable de la recolección de inteligencia de señales (SIGINT) en Reino Unido, entre 1996 y 1997.

Nota: La entrevista a David Omand fue realizada en idioma inglés. Se transcribe, en esta sección, en idioma original. Las inserciones realizadas en el cuerpo de la investigación han sido debidamente traducidas al español.

P: According to your experience in the public service. What aspects do you think political decision makers value the most in relation to the production of strategic intelligence and why?.

R: My experience is that political decision makers inevitably have a shorter term focus than the officials providing assessments because of the demands of the political election cycle. Genuinely strategic thinking requires an ability to think as a statesman not a politician. So although intelligence assessments can be genuinely strategic outlining possible long term developments in international affairs it is the shorter term warnings of possible crises ahead that get most attention, and are most valued when they help governments steer clear of trouble.

P: What attributes and training should the officials and workers of the offices that analyze information from social networks related to terrorism and organized crime have?

R: A range of skills are needed, probably not all to be found in one person. So teamwork essential. The ability to understand the technology of social media, including the ad tech that drives it. Knowledge of human psychology and how people (mis)behave online. Relevant language skills (including the argot of the group that is the target and internet-speak. Sensitivity to the possibility of deception and fakes. Deep knowledge of the target group (criminal, terrorist, etc).

P: In your experience, how can current governments mediate the tension that exists between the collection of information on social networks by different State agencies and the right to protection of personal data that citizens enjoy?

R: Governments have to start out by respecting the privacy rights of citizens, and recognising that intrusions must be necessary for defined purposes (national security, prevention and detection of serious crime) and the degree of intrusion must be proportionate to the harm it is hoped to prevent. In the UK we express this as 3Rs:

Rule of law: Up to date law to regulate intrusive intelligence gathering, providing transparency for the citizen as to the effect of the law, and with legal sanctions for misuse. An independent Court considers any complaints made by citizens or civil society groups.

Regulation with the Secretary of State (Foreign Secretary for overseas and Home Secretary domestically) personally signing bulk warrants subject to judicial review by a senior judge acting as Commissioner, who with a team of inspectors ensures the work of the agencies remains within the law. Requests for communications data are now granted by an independent office under the Commissioner. Parliamentary oversight continues by the Intelligence and Security Committee of Parliament which has been given enhanced powers to secure evidence from the agencies.

Restraint, requiring that the use by security and intelligence agencies of the coercive powers of the state to investigate the private lives of others be justified as both necessary and proportionate. Assessing proportionality has to be done by carrying out a balancing exercise in which the potential for harm to others of operations are set against the harms to the public that they are designed to avert, for example from engaging the privacy rights of those not the subject of investigation set against the saving of life and damage to property from stopping terrorist and cyber-attacks. There needs to be a reasonable belief in the value of the activity, on the basis of experience or specific research, to justify the level of ethical risk that may be involved.

P: What role do you think the private sector should have in relation to social networks, states and users?

R: Complicated! Depends on which part of the private sector. But the main message is that governments must be able to ensure the rule of law is upheld and that evidence of criminality can be obtained, which means private sector operators working with democratic governments to find ways in which with proper legal authorisation/warrants information can be passed to the authorities - part of the 3R approach.

EDUARDO PEDUTO

Jefe del Centro de Protección de Datos Personales, Defensoría del Pueblo de la Ciudad de Buenos Aires.

La ley nacional 23.326 que estudiamos en el presente trabajo guarda estrecha similitud con la ley 1845 de Protección de Datos Personales de la Ciudad de Buenos Aires, a excepción de que la ley nacional también aplica sobre el sector privado.

En el caso de la Ciudad de Buenos Aires, la Defensoría del Pueblo, ha sido designado órgano de control del asiento, uso y difusión de las bases de datos personales del sector público de la Ciudad de Buenos Aires garantizando el derecho al honor, la intimidad y la autodeterminación informativa. Los datos asentados deben ser exactos y bajo ningún concepto ser utilizados para un fin distinto a aquel por el que fueron obtenidos.

Esta garantía está especialmente orientada a la preservación y confidencialidad respecto de los denominados datos sensibles: origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o vida sexual.

Con el objeto de cumplir con las funciones asignadas, la Defensoría del Pueblo ha creado el Centro de Protección de Datos Personales. Para la realización de éste trabajo tuvimos la oportunidad de entrevistarnos con su director, el Licenciado Eduardo Peduto quien nos informó que toda persona que presuma o tenga la certeza de que sus datos figuran en alguno de los bancos de datos personales puede ejercer los siguientes derechos:

Derecho de información: Solicitar a la Defensoría del Pueblo, tomar conocimiento del Registro a su cargo. Derecho de acceso: Solicitar y obtener información de los datos referidos a su persona que se hallen en alguna o algunas bases de datos del sector público. Derecho de rectificación, actualización o supresión: Solicitar la

rectificación o actualización de sus datos y, cuando corresponda, la supresión o la protección de confidencialidad.

Peduto destacó que la visión de la dirección que preside trata estos temas como partes de un triángulo que debe tener cierta armonía entre cada extremo. Un extremo es el derecho a la Protección de Datos Personales, otro es el derecho de Acceso a la Información (pública) y un tercero es el derecho a la Privacidad.

En opinión de este especialista, la ley nacional de Protección de Datos Personales vigente tiene dos lados flacos. Uno es que al haber sido creada en el año 2000 no contempla mucho de lo que fue sucediendo con la evolución y el crecimiento de internet, por lo que falta que la normativa se explaye en esta materia y determine muchos aspectos de los datos personales en internet.

Otro aspecto a mejorar es que se suscribe al ámbito judicial y no contempla las denuncias administrativas que pueden efectuarse con muy buenos resultados. A su vez el acceso a la justicia es muchas veces restrictivo para las mayorías que muchas veces supone contratar una representación o asesoramiento legal sumado a que por cláusulas contractuales las empresas globales de internet, propietarias entre otras de Facebook, Instagram y Twitter, tienen base en EE.UU. y designan a los tribunales de California como el lugar para dirimir potenciales litigios o reclamos legales. Esto hace que el derecho a reclamar o defenderse sea difícil de ejercer para gran parte de los extranjeros o para personas con recursos medios o medios-bajos.

El cambio tecnológico de almacenamiento de contenidos también representa un llamado de atención para la protección de los datos personales según la óptica de Peduto. Las nuevas prácticas de alojamiento migran de dispositivos físicos offline a alojamientos online, en la “nube”. Pero ese alojamiento de datos tiene su sustento en hardware que mayoritariamente se encuentra físicamente en EE.UU. por lo que cualquier legislación o decisión política sobre esa información va a ser influenciada por dicho país.

La Unión Europea, por ejemplo, recomienda no alojar contenidos en servidores de EE.UU. por considerarlo un destino no seguro para la información de sus ciudadanos. Otra disposición que se abordó es el requisito para todas las empresas de Unión Europea del rol de “delegado de protección de datos personales” dentro de cada compañía. Esto deberá ser ejercido por un empleado que estará registrado y mantendrá el vínculo con el órgano de control de cada país, según la legislación puesta en práctica desde mayo de 2018 para Unión Europea.

Volviendo al caso de nuestro país, la variante institucional tiene cuestiones a reveer en la materia como es el caso de que la Agencia de Acceso a la Información Pública (AAIP) dependa del Poder Ejecutivo Nacional (PEN), de esta forma nunca podrá ejercer su rol con verdadera imparcialidad cuando le toque exigir o denunciar al PEN.

Otra observación que considera interesante contemplar el especialista es el hecho de que la ley de Acceso a la Información Pública (que resuelve la creación de la AAIP), crea la agencia de control con la estructura de lo que era la Dirección Nacional de Datos Personales, pero su nombre y su estructura puede hacer presuponer que le darán más importancia al acceso a la información pública que a protección de datos personales o la privacidad. Lo que para nuestro país puede resultar a contramano de nuestra historia donde la protección de Datos Personales fue precursora sobre los otros dos derechos.

HUGO GARCÍA

Jefe de Inteligencia Criminal, Prefectura Naval Argentina.

El Departamento Central de Inteligencia Criminal, de la Prefectura Naval Argentina tiene responsabilidad sobre tareas de inteligencia en la Prefectura Naval Argentina y acompañan el accionar institucional desde sus orígenes históricos en 1756, cuando se estableciera la primera Capitanía de Puerto, con funciones eminentemente policiales relacionadas con la seguridad de la navegación o en el ámbito portuario.

Para este trabajo nos resultó muy interesante poder entrevistar al jefe del área Hugo García quien marcó la génesis del departamento en una disposición del 12 de marzo de 1951, cuando el entonces Prefecto Nacional Marítimo daba lugar a la creación de la División Informaciones y Seguridad, que luego de sucesivas transformaciones dio origen al actual organismo.

La Dirección de Inteligencia Criminal, interviene en la colección, análisis e integración de la información de interés en el área jurisdiccional de la fuerza. Dentro de las principales actividades se incluyen la producción de inteligencia criminal sobre las acciones de toda índole que puedan vulnerar la operatividad de los puertos y las vías navegables, así como la salvaguardia de los intereses marítimos, fluviales, pesqueros y portuarios de la Nación.

La dinámica alcanzada en el proceso de integración entre los países miembros del MERCOSUR generó, desde el punto de vista policial, la necesidad de implementar una modalidad de trabajo impuestas por otras comunidades.

En ese sentido, se intensificó el intercambio de información e inteligencia criminal con organismo nacionales y de los países involucrados, con la finalidad de llevar a cabo un seguimiento constante de las organizaciones criminales cuya magnitud constituya un real peligro para la sociedad.

Según Hugo García todos los miembros del departamento que preside están totalmente informados y tienen pleno conocimiento de la ley de Protección de Datos Personales, desde su publicación en el Boletín Oficial de la Nación.

En ese marco consultamos si la organización posee archivos que contengan datos personales, a lo que respondieron que no. Asegurando que no recaba datos personales, ni datos personales sensibles en general.

Sin embargo cuando Prefectura recibe instrucción de reunir información en virtud de sus funciones de Seguridad Interior, Hugo García consideró que se utiliza información proveniente de redes sociales siempre mediante un pedido de una autoridad del Poder Judicial de la Nación. De modo que la actividad de recolección de datos personales sería en estos términos una práctica legal según la actual ley.

JERÓNIMO PARDO

Responsable de Analytics, Illuminati Lab Social Intelligence. Actualmente, Account Manager en Google.

Jerónimo Pardo, se desempeña en el área de Analytics de la empresa de Inteligencia en Redes Sociales Illuminati Lab, la misma se dedica al análisis de datos e información disponible en redes sociales para la producción de conocimiento.

Dentro de sus tareas la principal es la “escucha” o listening, que trata de entender de qué se está hablando en redes sociales, especialmente si esto involucra a algún cliente de la compañía o sobre algún tema de interés de dichos clientes. Se estima que estos proyectos representan cerca del 70% del total de los ingresos económicos de la compañía y es por lo tanto la actividad principal.

MARIANA MÁRQUES

Directora de Justicia y Política Internacional de la ONG Amnistía Internacional.

Entrevistamos a Mariana Márques, quien es Directora de Justicia y Política Internacional de la ONG Amnistía Internacional. Mariana es la responsable del informe “El debate público limitado. Trolling y agresiones a la libre expresión de periodistas y defensores de DD.HH en Twitter Argentina” publicado en Marzo de 2018.

Dicho informe demuestra cómo se vulnera, de forma organizada y clandestina, la libre expresión y el derecho de protección de los datos personales de diferentes referentes de DD.HH. y periodistas en Argentina en la red social Twitter.

La persona u organización clandestina, mencionadas en el informe como “Ciber Tropas”, producen conocimiento en base a “datos sensibles”, que luego utilizan para la toma de decisiones y ejecución de sus acciones en Twitter. De hecho ser referente del colectivo de DD.HH. en un país, es sin lugar a dudas pertenecer a un grupo ideológico y político, y esto constituye un “dato sensible” de cada persona.

Mariana opinó sobre la complejidad de regular el uso de datos personales por parte de estas organizaciones clandestinas, en que lo principal es exigir a las compañías dueñas de las redes sociales que tengan políticas activas sobre aquellas cuentas que tienen comportamientos que vulneren la libertad de expresión de otras.

Otra iniciativa podría ser dar de baja aquellas cuentas que es evidente que actúan como robots, repitiendo contenido, agraviando sistemáticamente a determinados actores ejerciendo acoso, asumiendo un rol más activo desde las compañías.

Facebook e Instagram que son de la misma empresa tienen políticas más robustas en materia de protección de datos personales y están más comprometidas en este aspecto que Twitter. Un ejemplo de ello es que Facebook pide a los usuarios su identidad real y te permite crear una sola cuenta por persona, mientras que Twitter

es más laxo disponiendo hasta cinco cuentas registradas con un mismo email y/o usuario. También es reconocible que Facebook, en muchos casos, buscando proteger datos personales o privacidad, incurre en censuras.

También es un hecho que por el diseño funcional de Twitter, se promueve indirectamente la interacción y en consecuencia, la agresión entre usuarios.

Sobre el tema del anonimato en internet, Amnistía no considera al momento promover alguna legislación que genere una identidad virtual, o un método que permita regular las interacciones y que pueda haber responsables por cada hecho u opinión en la red. Por el contrario la ONG con base Argentina ve con buenos ojos que exista libertad y desregulación, para que los usuarios no se vean siempre individualizables y que esto genere una autocensura, a su vez el anonimato muchas veces permite géneros discursivos como la sátira que enriquecen la libertad de pensamiento y cuestionan al poder concentrado de los discursos dominantes.

Sobre los casos que estudiaron en el informe nos comentó que la operatoria de estos grupos se inicia en la función de “figuras habilitadoras”, que son usuarios reales representativos en la red que inician una crítica a un usuario, identificandolo públicamente como el objetivo de hostigamiento para la “Ciber Tropa” en la comunidad en Twitter. Sobre dicho usuario la “Ciber tropa” ejercerá el acoso mediante ataques discursivos, limitando así la opinión de la víctima sobre determinada temática.

Estos ataques discursivos en oportunidades incluyen como herramienta la acción, ya descrita en este trabajo, conocida como *Fake News.* La táctica consiste en crear una noticia falsa sobre el usuario blanco que sirva para degradar su honor (vulnerando su derecho al honor) o su estándar ético, buscando mostrar contradicción en sus valores personales o la incursión en algún delito normado por la ley.

Tal como desarrollamos en el apartado sobre noticias falsas, éstas son de especial relevancia para ésta tesis por el hecho de que casi siempre contienen la categoría de “datos sensibles” que dispone la Ley Nacional de Datos Personales, buscando

exponer al usuario blanco y a su vez ganar verosimilitud e impacto en las repercusiones de la acción.

Como sugerencias de parte de Amnistía Internacional, Mariana consideró que lo más importante es la educación a los usuarios, que sean conscientes de que estas operaciones existen, dado que en muchas oportunidades los usuarios genuinos participan sin saber, de buena fe o reproducen contenido falso que puede perjudicar el nombre y honor de otra persona. Hay una tarea pendiente por parte del Estado y las instituciones de la comunidad en generar concientización en la comunidad de redes sociales.

Las empresas, todas, y las de redes sociales también, son responsables de proteger los derechos humanos. Amnistía reconoce que hay problemas en este sentido y que todos los actores deben comprometerse más para evitar las violaciones a los DD.HH. en su ámbito.

Para Amnistía, el rol de las campañas políticas en redes sociales merece un capítulo aparte en esta discusión. Ya en varios países los partidos polìticos que compiten en elecciones democráticas abiertas celebran lo que se denomina un “acuerdo de no violencia online” buscando mitigar el nivel de agresiones entre los actores que pugnan por un cargo y entre los usuarios de la red social en general.

Casos como el de Cambridge Analitica con Facebook, dispararon las alertas en la comunidad más involucrada en las nuevas tecnologías sobre lo que el uso legal pero inadecuado de las redes sociales pueden representar en los escenarios electorales de la actualidad.

ALEJANDRO SALOMÓN

Ex director de la Escuela Nacional de Inteligencia - Agencia Federal de Inteligencia (AFI) - (2015-2019).

¿Qué conocimiento cree útil producir desde el Estado, en base a la información de redes sociales?

Las redes sociales tienen mucha información útil para la producción de inteligencia, y desde el Estado se brinda a los analistas la formación específica para aprovechar ese recurso y otros recursos tecnológicos, como el Big Data. Desde ya que en la actualidad un analista de inteligencia es mucho más útil que sepa de tecnología a que sepa hacer un seguimiento callejero u otros métodos más arcaicos de recolección de información que se promovía antes y que por un lado eran mucho más violentos e invasivos y hoy son considerados totalmente obsoletos en gran medida.

¿Qué aspectos considera que valoran los decisores políticos y por qué?

Hay algunos problemas bien visibles sobre el rol de la Inteligencia del Estado y los decisores políticos. Desde el lado de la Agencia, el error en algunos sectores empieza cuando creen que están al servicio del presidente. Eso no es así, están al servicio del Estado, de los intereses del Estado. Esto es realmente muy diferente. Como ejemplo se me ocurre que si la Agencia reúne información sobre los intereses de los bonistas para proveer inteligencia que ayude a una mejor toma de decisiones con respecto al pago de la deuda de nuestro país, sería una función lógica y útil a los intereses del Estado. Ahora bien la reelección de un presidente, es un tema político o personal del presidente y la Agencia no debe intervenir en ese asunto, por eso no es correcto decir que la Agencia responde al presidente, sí responde pero solo sobre aquellos intereses estatales no personales ni políticos.

Del otro lado, los decisores políticos muchas veces llegan con total desconocimiento sobre qué es la inteligencia y que debería hacer. Si no saben los decisores que se

supone que son personas medianamente informadas, que podemos esperar de la comunidad en general. El desconocimiento es total. Entonces, volviendo a los decisores, desde ese desconocimiento es muy complejo que consigan conducir o requerir funciones que sean realmente interesantes y eficientes para los intereses del país. Por otra parte también hay productos de inteligencia de muy baja calidad que de alguna manera desmotivan a los decisores políticos a proveerse de ese recurso, no todos los productos tienen baja calidad, pero aquellos que sí deslegitiman el rol de todo el organismo y entonces el decisor busca otras fuentes para tomar las decisiones de su posición. Quizás recurre al ámbito académico o científico o de algún otro tipo. En este sentido la responsabilidad es compartida, del político de no saber la función y de algún sector de no estar a la altura de la función que debe cumplir.

¿Cómo debe ser la formación de un analista de inteligencia y qué cambios considera que serían positivos hacer desde el Estado?

Bueno, todo agente sobre todo un analista debe tener una formación muy, pero muy sólida en Lógica. Nadie puede desempeñar su función profesional sin tener muchísima robustez en ese ámbito de la ciencia. La lógica brinda las herramientas para que el analista consiga desempeñar su función con mayor objetividad, y menores sesgos, le dará herramientas para que eventualmente identifique esos sesgos y pueda volcarlos dentro del análisis. El consumidor del producto de inteligencia debe tener acceso a comprobar cómo se llegó a determinada conclusión, y la lógica brinda de la mano de los métodos de análisis una forma científica de justificar aquello que se prospecta sobre determinado hecho o fenómeno.

Es decir que para este rol no se puede usar la intuición, o una percepción que no esté suficientemente constatada. Es por eso que analizar información en grupo puede dar mayor ecuanimidad pero siempre y cuando no haya una mayoría con un sesgo muy marcado que condicionen la opinión de una minoría. Los sesgos van a estar y hay que registrarlos para conseguir un producto de mayor calidad.

La Agencia Federal de Inteligencia y el sistema en general carecen no sólo de una buena imagen pública, sino también de una legitimidad política, debido a múltiples factores y uno de ellos es una desmedida cultura del secreto. El camino para mejorar esto sin dudas es comenzar a transparentar mucho más las funciones de la agencia y conservar en secreto lo profesionalmente necesario.

¿Cuál cree que sería el mejor camino para que la producción de conocimiento en redes sociales no vulnere el derecho de protección de datos personales?

El criterio ético desde ya que está dado por el fin que tenga la reunión de información. Recolectar información que ayude a combatir los delitos que afectan a la comunidad, por ejemplo con el fin de desarticular una banda delictiva vinculada al narcotráfico, la venta ilegal de armas, al terrorismo o cualquier delito federal, es una acción positiva que busca proteger los intereses del Estado y de los argentinos. Reunir información bajo estos fines es una acción permitida por la ley de protección de datos personales, ya que serán datos que se recaben para el ejercicio de funciones propias de los poderes del Estado y para ello la ley prevé que no se necesita consentimiento por parte del dueño de los datos personales.

EDUARDO BERTONI

Ex-Director de la Agencia de Acceso a la Información Pública (2017-2021). Actual representante ante el Instituto Interamericano de Derechos Humanos (IIDH).

Teniendo en cuenta que en el uso de redes sociales los ciudadanos volcamos muchas veces datos personales y datos personales sensibles: **¿Considera suficientes las normativas de protección para garantizar los derechos de los ciudadanos?**

RTA: Si "volcamos" implica otorgar consentimiento, lo cual parece obvio, nuestra ley es suficiente y está adecuada a las legislaciones de otros países. El problema a veces es que no somos conscientes de que damos nuestro consentimiento al aceptar el uso de las aplicaciones.

Los Estados con fines de seguridad pública, en ocasiones, recolectan datos personales de redes sociales. **¿Cómo se debería mediar en esta tensión entre el derecho a la protección de los datos personales y el derecho a la seguridad pública?.**

RTA: Hay cierta información que de acuerdo a la ley que se puede recolectar sin consentimiento. Y hay información que no puede ser recolectada. Eso está resuelto en la ley, tanto en la Argentina como en el nuevo Reglamento de Protección de Datos de Europa.

¿Y en el caso de las empresas privadas que recolectan y analizan datos personales con fines comerciales?

RTA: Si hay consentimiento no hay problema. Si hay recolección con consentimiento y se utiliza para un fin distinto, se está fuera de la ley. Si hay recolección sin consentimiento por fuera de las excepciones que da la ley, se está en contra de la ley.

¿Cuándo y cómo considera que se le dará tratamiento al proyecto de ley que se trabajó desde la AAIP para actualizar la ley de protección de datos personales argentina?.

RTA: El proyecto perdió estado parlamentario el 29 de febrero de 2020.

ROBERTO UZAL

Director de la maestría en Ciberdefensa y Ciberseguridad - UBA

¿Qué rol considera que ocupan las redes sociales en materia de Ciberdefensa y Ciberseguridad?

El rol de las redes sociales relacionado a la Ciberdefensa y la Ciberseguridad, es esencial. Han habido y hay múltiples campañas comunicacionales llamémoslas, insidiosas, con el fin de influir por ejemplo en la opinión de un electorado, a través del uso de técnicas de Data Analytics.

La fuente de ingresos de datos muchas veces proviene de las bases que disponen las redes sociales. Estos grandes agregados de datos, a los que se acceden de forma a veces lícita a veces no, son un insumo clave que segmentado y dirigido, son usados lamentablemente para la concreción de estas operaciones sobre la comunidad.

Algo similar pasa con las bases de datos de clientes bancarios o de tarjetas de crédito, desde donde estas organizaciones de ciber fraude se alimentan para montar sus acciones. El caso de Cambridge Analytica es un ejemplo de la capacidad de incidencia en la opinión pública a través del procesamiento de grandes volúmenes de datos, la segmentación y el uso de esta información.

Una característica que debemos tener en cuenta al referirnos a Ciberdefensa es la complejidad que toma el factor territorial. Ya no podemos hablar de territorio tal cual lo entendimos hasta hace algunas décadas, las fronteras se borran y todo forma parte de una misma cosa, por lo que la aplicación de las soberanías y la protección de los intereses de cada nación va a tener que adaptarse a este nuevo escenario, sin lugares y sin distancias. No todos los Estados e instituciones lo entienden porque continúan basando algunos criterios de acción en la ocurrencia territorial de los fenómenos.

Los delitos de Ciberdefensa, como puede ser la intrusión de un Estado sobre algún activo estratégico de otro Estado a través de internet, también ven afectado el factor tiempo. Las acciones de esta especie se desarrollan en pocos segundos y los sistemas de los Estados para proteger estos activos deben resolver la intrusión también en una brevedad similar, para conseguir neutralizar efectivamente el ataque.

Para conocer quien realizó el ataque, se debe resolver la atribución, es decir la fuente de la agresión y para ello los sistemas trabajan desandando el camino que el atacante realizó, son decisiones que deben tomarse en fracciones de segundos y para lo cual el Estado va necesariamente a violar la jurisdicción de algunos Estados amigos por los que haya pasado el agresor. Esto no está bien visto, pero es un nuevo problema.

¿Puede haber vulneración de (derecho de protección de) datos personales en acciones de Ciberdefensa o de Ciberseguridad?

Bueno para reducir esto, es muy útil la elaboración de una matriz de riesgo, que no es otra cosa que listar los blancos más tentadores para un posible ciberagresor y este listado puede incluir una correspondencia en valores monetarios y sociales, es decir la afectación económica y social de suceder el evento sobre un determinado activo. Este análisis sumado a un eje que incluya la probabilidad de que estos hechos ocurran, nos puede ayudar mucho a focalizar los esfuerzos en ciberdefensa y a su vez a disminuir cualquier vulneración innecesaria sobre datos personales u otros derechos individuales.

En este sentido, la Corte Suprema de los Estados Unidos, emitió una acordada donde declaró que su jurisdicción era global en cuanto a “ciber felonías” y le otorgó especialmente al Federal Bureau of Investigation (FBI) jurisdicción global en materia de ciberdelitos. Es decir que en relación a la aplicación del Derecho de Protección de Datos Personales u otros derechos emparentados, cuando una acción del FBI vulnere derechos de ese tipo en países aliados de los Estados Unidos, será una acción legal, al menos para ese país. Este tipo de decisiones políticas refuerzan la idea de que lo geográfico carece de sentido cuando nos referimos a cibercrímenes.

Repasando el escenario mundial, sabemos que China tiene un gran desarrollo en Ciberdefensa, pero también pesan sobre ellos algunas sospechas sobre cómo han podido acceder a conocimiento científico tecnológico, que a otras naciones les costó un desarrollo de años, en tiempos marginales. Como el caso de Editas Medicine, una compañía promocionada por el MIT de EEUU que investiga modificaciones en el ADN para conseguir combatir mejor algunas enfermedades. China llegó a resultados más avanzados poco tiempo después de que Editas Medicine tuviera sus primeros resultados después de mucho tiempo de desarrollos.

Rusia por su parte, también es otra de las potencias mundiales en materia de Ciberdefensa. Una muestra de ello se da cuando Putin estaba a cargo de la KGB, el Director de Tecnología Informática de ese organismo era el dueño de una de las empresas más importantes en la materia, nada menos que Eugene Kaspersky, dueño de Kaspersky Lab. Conocido por ser uno de los antivirus más populares del mundo.

Irán, después de haber sufrido ciberataques en su planta nuclear de la ciudad de Natanz, comenzó a desarrollar un alto nivel de medidas empoderando su equipo de ciberdefensa y en la actualidad es considerado una potencia en la materia.

¿Qué tipo de delitos comete el Ciber Crimen Organizado Trasnacional?

Los delitos son diversos, dependiendo cual sea el interés del ciberagresor. Si persigue un interés económico, podrá tratar de vulnerar la seguridad de un banco o usuarios de cuentas bancarias para transferir fondos, o realizar ciber extorsiones amenazando con el manejo de cierta información sensible. Robar conocimiento científico tecnológico, etc.

Si el interés es geopolítico, o religioso y se busca generar un hecho terrorista, o la afectación vital de una comunidad, ahí el blanco del ciberagresor puede ser una de las industrias críticas de la comunidad como puede ser afectar una planta potabilizadora y con esto la salud de la comunidad, afectar una central nuclear

convirtiendo en arma una instalación o solo cortando el suministro. Los blancos son tan variados como motivaciones haya.
Aunque suene contradictorio, los principales problemas relacionados a la seguridad en internet no vienen de internet, sino de la variante humana en el uso de internet. Estos problemas que se producen por acción del hombre y la mujer en el uso de redes sociales por ejemplo, son las que afectan los derechos de la sociedad en general.

Puntualmente cuando se omiten algunos aspectos éticos en el uso de internet. No necesariamente por parte de Estados, y si es por parte de los Estados, peor aún. Pero cuando ese factor humano es desviado del que debería ser, el daño hacia los derechos de las personas, y sus datos personales se ven amenazados de forma exponencial.

Creo que hay que hacer foco en el factor humano, entender de un modo más acabado las diferentes personalidades que hay en una sociedad y que en determinados lugares de decisión afectan sustancialmente nuestros derechos. Es ahí donde veo la brecha más amplia y el flanco más vulnerable en lo que hace a la ciberseguridad y la ciberdefensa.

CRISTINA CAAMAÑO

Interventora de la Agencia Federal de Inteligencia (AFI).

¿Qué conocimiento cree útil producir desde el Estado, en base a la información de redes sociales como fuente de información? ¿cómo ve a Argentina en ese aspecto en relación a otros países?.

El fenómeno de las redes sociales abrió un abanico muy interesante, pero también complejo en términos de derechos.

Cuando una persona publica en alguna red social contenidos personales debe entender que esa información queda a disposición por un período de tiempo indeterminado. Sin embargo, las redes sociales, y ahora opino como fiscal jubilada, pueden aportar información para reconstruir el contexto de determinadas personas o hechos puntuales.

A su vez, las redes sociales son utilizadas como canales orgánicos de instituciones públicas y privadas para comunicar temas de interés en su materia.

El Estado es un conjunto complejo de agencias. Es muy difícil pensar qué tipo de conocimiento útil se puede producir de manera uniforme. No es lo mismo pensar a la Agencia Federal de Inteligencia que, por decir algo, al PAMI. No es lo mismo pensar a las redes sociales como una fuente de información o como un canal de comunicación institucional.

Lo importante es el respeto de las garantías constitucionales de las personas. El Estado, con la excusa de la seguridad nacional, no puede violar los derechos de los ciudadanos.

Nosotros nos encontramos con prácticas absolutamente ilegales al momento de asumir la Intervención. Las fuimos denunciando penalmente. Una parte de la información recopilada tenía como fuente a las redes sociales. Inmediatamente,

ordené detener todo tipo de tarea de reunión de información sobre ciudadanos, que representaba uno de los eslabones de las prácticas de inteligencia ilegal.

¿Qué aspectos considera que valoran los decisores políticos de la AFI y por qué?

La Agencia Federal de Inteligencia se encuentra en un proceso de refundación institucional. Estamos construyendo las capacidades para que su función sea la producción de inteligencia estratégica y el trabajo con otros organismos nacionales e internacionales en materia de prevención del terrorismo.

Hoy, estamos viendo los primeros resultados. Las máximas autoridades nacionales comenzaron a referir que los informes que realizamos son de utilidad al momento del diseño de políticas públicas. Obviamente, no puedo dar a conocer ni el tema ni el contenido. Fue un proceso que iniciamos al comienzo de la Intervención, en paralelo con la enorme tarea de hacer ingresar al Estado de Derecho a la AFI, lo cual no fue sencillo.

¿Cómo debe ser la formación de un analista de inteligencia?

El analista debe especializarse en un tema puntual, de modo de no iniciar el camino cada vez que aborda una temática específica. El trabajo del analista es un eslabón del proceso de producción de inteligencia y debe ceñirse a las necesidades de inteligencia que originaron el requerimiento de información.

En ese sentido, además de la formación específica sobre la producción de inteligencia estratégica, el analista debe mantenerse actualizado en su disciplina y en la temática específica a la cual se dedica.

No sirve un analista que sepa un poco de todo. Es necesario que sepa mucho de algo. Por eso, el proceso de formación necesita de tiempo, diría que de años.

Nosotros nos encontramos con una AFI casi sin capacidad de análisis, ya que se encontraba dedicada al espionaje ilegal.

Y además, la Escuela Nacional de Inteligencia tenía un muy bajo nivel académico. Nos encontramos en proceso de certificar los programas y los títulos con el Ministerio de Educación. Descubrimos que los programas no contaban con la aprobación oficial y que, nos llamó aún más la atención, en muchos casos los certificados se extendían con el nombre supuesto, lo que singificaba que no servían para sumar a un CV como antecedente.

¿Cómo evitar que la producción de Inteligencia (por ejemplo en redes sociales) vulnere el derecho de protección de datos personales?

Hay que cumplir con la ley. La inteligencia es una actividad estatal. El Estado no puede violar el Estado de Derecho. Esa es nuestra premisa.

Para ello, elaboramos un borrador de reforma legislativa que crea los mecanismos de control para que toda tarea de reunión de información sea congruente con una directiva de Inteligencia y que si esa tarea tensiona alguno de los derechos de los ciudadanos y las ciudadanas sean autorizadas y monitoreadas por un juez.

¿Qué mensaje le dejaría a las próximas generaciones sobre la política pública en Inteligencia? ¿qué cosas quedan por mejorar?

En primer lugar, que estudien. Que se mantengan en constante actualización.

Y que no acepten premisas según las cuales se puede violar la ley. La democracia y los derechos humanos no son un techo para la producción de inteligencia, sino una plataforma desde donde partir.