Organización Civil - ONG
Grupo de Mujeres de la Argentina
Foro de VIH Mujeres y Familia (GMAF)

"Elaboración del documento – Convención Global de Ciberdelincuencia"

I - Presentación

Agradecemos por nuestra presencia en esta reunión virtual, integrando el Comité intergubernamental de Expertos ad hoc de expertos (AHC) - como organización civil, comprometida socialmente en el ámbito nacional e internacional, para Llevar a cabo un Estudio Integral sobre Ciberdelincuencia, conjuntamente con representante de los Estados.

Es por ello que tomando en cuenta que el Presidente del Comité ha preparado un documento[1] borrador como base para la segunda lectura en la próxima 4ª[2] y 5ª sesión de la AHC, **para apoyar la elaboración de una Convención de las Naciones Unidas eficaz y respaldada universalmente**, para "**Combatir el Uso de las Tecnologías de la Información y las Comunicaciones para Fines Delictivos punibles",** anticipamos que, al respecto daremos nuestro apoyo a tal iniciativa con nuestras recomendaciones.

Nos sentimos reconfortados por el hecho de la concurrencia a éste documento final, en el cual se encuentran participando distintos actores de la comunidad internacional, para elaborar una Convención de la ONU sobre la lucha contra el delito cibernético.

Entendemos que, é**l mismo, debe consolidarse desde los estándares e instrumentos internacionales y tomando en cuenta las normativas del derecho interno de cada sujeto internacional, y regional, para lograr combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos.**

[1] Naciones Unidas AC 291/16 Asamblea General Distr. General 7 noviembre 2022
[2] Cuarta en la sesión Viena, 9-20 de enero de 2023

Dra. Martha I. Miravete Cicero – Presidenta del Grupo de Mujeres de la Argentina – Foro de VIH Mujeres y Familia – email denunciasddhh@gmail.com - Twetter: @gmaddhh web: www.grupodemujeres.org.ar
Participaron: Dra. Natalia Torres, Dra. Daiana Ibave, Mg. Ester Hublich, Sr. Ashur Nufuri, Ing Hugo Corral

II – Análisis

Nuestra organización, se ha conformado hace 20 años[3], siendo la voz de muchas y muchos sobrevivientes, que han vivido distintos hechos de violencia en nuestro país y en el mundo.

Desde el 2006 somos una organización consultora de la OEA y en el 2014 de Naciones Unidas – ECOSOC, hasta la fecha.

A sabiendas de la situación de nuestro país, de la región y el mundo, en el contexto en análisis, en el cual se encuentra la sociedad con un alto índice de vulnerabilidad (sujetos nacionales e internacionales), registramos y monitoreamos casos por **el mal uso de las tecnologías de la información y las comunicaciones con fines delictivos.**

Y es por ello que nos hemos comprometimos en visibilizar, colaborar y recomendar sobre la problemática que implica no solo la existencia del ciberdelito sino la universalización de este tipo de conducta y su impacto en el mundo actual.

A raíz del conocimiento de las causas, hemos logrado establecer, por ejemplo, que muchas personas jóvenes se han quitado la vida (suicidio), por la extrema presión a la que son sometidos en prácticas que aparentan ser un simple trabajo coordinado, y terminan configurando delitos que incluso en las legislaciones internas de los Estados parte no figuran como tales; como así también hemos analizado casos de sujetos internacionales que han sido difamados, **con el claro objetivo de influir y manipular información, creando otro suceso alternativo y paralelo en redes sociales, que provoque confusión y engaño, por el solo hecho de desprestigiar a la persona o la descalificación de políticos descreditando su trabajo,** y así contribuir a debilitar las políticas públicas generadas ad hoc.

Un ejemplo preciso de ello, son las **"fake news",** que es información creada como si fuese real con la intención de desinformar. El objetivo es manipular a las masas por diferentes portales de

[3] 19 de agosto 2002 – IGJ 780/02 - Argentina

noticias: prensa, radio, televisión y redes sociales, para lograr un engaño en la sociedad con fines políticos o ideológicos.

Ahora bien, nos preguntamos porque no existe una regulación de las redes sociales, en monitorear estos espacios de empresas privadas, las que son usadas de manera ilícita, las cuales muchas veces son usadas con falsas identificaciones y grupos que exponen impunemente sus delitos realizados.

Creemos que debe existir una regulación, sanción económica y penalización, tomando en cuenta medidas procesales para que la comunidad internacional regule, y ello será así si se transforma en una Convención Internacional, pues lamentablemente muchos casos analizados trascendieron las fronteras de los Estados, convirtiéndose así en un delito Transnacional, utilizando las tecnologías de la información y las comunicaciones con fines delictivos.

Por ello hacemos hincapié en lo siguiente:

A. **<u>Con respecto a la resolución 74/247 del 2019, aprobada por la Asamblea General, decimos</u>**:

Nos preocupa que empresas privadas de redes sociales y sus usuarios vivan hostigamiento y difamación, ya que se utilizan informaciones privadas o falsas para difamarlos.

Como dijimos anteriormente, espacios como las redes sociales, son usados con falsas identidades para desprestigiar a las personas, o hasta realizar incentivos de violencia hacia la sociedad.

Otro ejemplo es:

- la **ciber-violencia de género**, **el ciberacoso,** los insultos y amenazas, la obtención de datos y contraseñas para acceder de forma indebida a los perfiles personales de las víctimas, compartir contenido íntimo para extorsionar a la víctima (**sexting**).
- El "**grooming o child grooming**" el acoso sexual a niños, niñas y adolescentes a través de medios digitales, para establecer contacto con fines sexuales. En el cual es un conducta de una persona deliberadamente iniciadas por una persona mayor con el objetivo de contactar a un niño, niña y/o adolescente y así ganarse su confianza, estableciendo un vínculo emocional.

Siendo estos espacios redes sociales, en el cual las empresas son las responsables de estos sitios, es que deben tomarse medidas de Alerta temprana, como una forma de control para que esto no ocurra.
Ahora bien, con respecto a cuál debería ser el área de Estado que deba realizar el seguimiento y monitoreo, ¿en cada Estado?, ése dispositivo estatal debería ser un ente regulador, autárquico, descentralizado, como sucede en nuestro país[4], donde observamos que existen varios organismos[5] que se ocupan y monitorean estos hechos[6].

B. Con respecto al Hackeo de información privada

El hackeo y compra de datos personales y de organismos del Estado, son usados con fines delictivos, violándose así el Derecho a la información privada – Habeas Data. Esto es utilizado para coaccionar y hostigar al usuario de otra empresa para la venta de un producto, pero también otras empresas utilizan esta información para no aceptar a la persona como empleada por tener problemas de salud (por ejemplo).

Hemos visto que son varios los hechos ocurridos en los últimos años, sobre la obtención ilícita de datos personales, daremos ejemplos sobre los cuales hay que tener en cuenta para una regulación nacional e internacional al respecto.

Un ejemplo es la empresa Globo[7] en el cual fue Hacheada su base de datos incluye los datos de 5.790.564 pedidos de clientes, 21.379 datos empleados y 37.509 mensajeros.
Otro ejemplo en nuestro país, es la base de datos del **Registro Nacional de las Personas (RENAPER)**[8] y también sobre **Datos de IOSFA[9] – Instituto de Obra Social de las Fuerzas**

[4] En agosto del 2022, se realizó una reunión en el cual participaron, el Comité de la Convención sobre Cibercrimen del Consejo de Europa; del Instituto de Estudios de Seguridad de la Unión Europea; del proyecto EU Cybernet; de la Organización de Estados Americanos; de INTERPOL; del Global Forum on Cyber Expertise; del Operation Underground Railroad; y la embajadora para Asuntos Cibernéticos del Ministerio Federal de Relaciones Exteriores de Alemania. Desde el sector privado participaron integrantes de empresas como Microsoft, Oracle, Eset, Fortinet, Intel, Meta, Whatsapp, Chainalisys, Maltego, Voyager Labs y Grayshift. Mientras que de nuestro país expusieron representantes de la Fundación Argentina de Prevención de Lavados de Activos; de la Asociación de Bancos; de la Asociación de Fiscales y funcionarios del Ministerio Público Fiscal de la Nación. Además, participaron ministros y ministras de las provincias de Córdoba, Entre Ríos, Río Negro, Santa Fe, Tierra del Fuego; funcionarios; fiscales y agentes de las fuerzas de seguridad de más de 16 provincias, así como de funcionarios del gobierno nacional. Pero ninguna organización civil comprometida en la temática.
[5] https://www.argentina.gob.ar/justicia/convosenlaweb/denuncia
[6] https://www.argentina.gob.ar/noticias/se-realizo-la-primera-conferencia-cumbre-sobre-asuntos-ciberneticos
[7] https://www.xataka.com/seguridad/datos-personales-cinco-millones-pedidos-glovo-estan-a-venta-que-ocurre-duro-hackeo
[8] https://eleconomista.com.ar/tech/hackean-renaper-hablo-hacker-asegura-tener-copia-datos-planea-venderlos-filtrarlos-n47003
[9] https://www.eldisenso.com/informes/hacker-pone-a-la-venta-datos-del-renaper-de-45-millones-de-argentinos/

Armadas y de Seguridad, datos de 1.193.316 afiliados pertenecientes a la Gendarmería, Ejército, Prefectura Naval, Armada y Fuerza Aérea.

RECOMENDACIONES

Al respecto, decimos que es importante:

a- Comprometer a las empresas de Telecomunicaciones para realizar alertas tempranas en el contexto de la seguridad internacional, pues ello conduce a una mejor cooperación de todos los actores sociales en la prevención de estos delitos tecnológicos de la información y de la comunicación.

b – Deben adoptarse medidas para prevenir el delito transnacional, como el tráfico de personas, tráfico de drogas, la adulteración de documentos públicos sobre la identidad de las personas – documentos apócrifos, hackeo de datos personales y de organismos del Estado.

c- Proteger a la sociedad, a los sujetos internacionales y a la comunidad internacional de estos delitos trasnacionales de tráfico de información a través del ciberdelito, comprometiéndonos convencionalmente para reducir éstos actos delictivos.

Con respecto a los temas de particular interés incluiremos para esta reunión:

- **Alcance de las disposiciones sobre tipificación y obtención de pruebas electrónicas;**

En Argentina, la problemática no se profundizado lo que afecta la vigencia de garantías de la población que reside en el país.

Hasta ahora el sistema ha intentado solucionar el problema posterior a los hechos que ocurren día a día[10], por lo que no se ha logrado implementar Alertas Tempranas, más tomando en cuenta las nuevas tecnologías que cada día cambian y su repercusión en el mundo del delito cibernético.

Lo que trae aparejado diversos inconvenientes que ha demostrado en varios casos la incapacidad del sistema para brindar una respuesta adecuada que violenta el derecho a la intimidad.

Lamentablemente, no se ha logrado el compromiso real desde el sistema de Estado, ya que suele confundir la vigencia del derecho constitucional con la certeza del elemento probatorio, que son cuestiones diferentes.

Uno de los Poderes del Estado (el Legislativo), el cual tiene la responsabilidad de aprobar una normativa sobre la problemática en análisis, adolece o no tiene asistencia de

[10] ley penal, lo que permitió la tipificación del *cibercrimen,* prevista en la Ley de delitos informáticos, nº 26.388

profesionales capacitados a ésta temática, por lo que debería ser prioritario capacitar a los funcionarios y profesionales, específicamente en el tema y **el control de convencionalidad.**

Con respecto al Poder Judicial - puede acceder a un sistema informático pero no va acompañado a la normativa vigente, ya que la investigación debe ser ordenada por un juez - Constitución Nacional - art 116, acompañado por las exigencias formales establecidas por el legislador para acceder a determinados ámbitos de intimidad - Constitución Nacional artículo, 18), para que aporte una motivación suficiente que establezca el grado de intrusión, criterios de proporcionalidad en la disposición de la medida, y lograr una eficacia de la medida sin violentar o restringir el derecho a la intimidad u otros más allá de lo necesario.

Ésta medida debe tener en cuenta cuáles son los requisitos que la medida debe abarcar, como así también, tener cuenta la extensión y gravedad de dicha intrusión.
La afectación de la tecnología en la intimidad de los ciudadanos, obliga a una regulación muy rigurosa, bien podemos decir que el concepto de la Corte Federal Constitucional Alemana, reconoce un nuevo derecho fundamental constituido por la garantía a la confidencialidad e integridad de la información en sistemas informáticos como una derivación del derecho a la personalidad y la dignidad. Resulta relevante advertir el grado de amplitud (en virtud de algunos medios tecnológicos o en algunos casos en particular) de la injerencia a la intimidad.

- **Medidas procesales y garantías de los derechos humanos**

La **regulación normativa en muchos otros casos no resulta obligatoria desde el punto de vista constitucional**, pero sí resulta una buena decisión de política criminal regular el acceso a sistemas informáticos con reglas claras que respeten el derecho a la intimidad si se encontrara comprometido, que unifique la regulación del acceso del Estado a comunicaciones en general y los sistemas informáticos, así como regular la cadena de custodia.

La regulación en derecho procesal penal, debe ser de carácter general a los sistemas informáticos, estableciendo limitaciones jurídicas, temporales y que aporten certezas a los elementos probatorios incorporados, que permita al proceso penal adaptarse a nuevos medios posibles día a día.

No resulta ajena a **nuestra recomendación desde el enfoque de los Derechos Humanos**, el hecho de recurrir a una herramienta fundamental en el control del poder discrecional del Estado, **que avanza sobre o soslaya, la plena vigencia del Derecho Internacional de**

los Derechos Humanos; y en ése sentido nos referimos al **CONTROL DE CONVENCIONALIDAD.**

Es indudable la necesidad de contar con una Convención internacional que regule de forma univoca el tratamiento y la creación de mecanismos para la prevención y lucha efectiva contra el denominado ciberdelito.

Con la asistencia de una **IA (Inteligencia Artificial),** que se proyecta y desarrolla a pasos agigantados, los ciberdelincuentes encuentran en la intangibilidad del espacio virtual, nuevas formas para provocar delitos que en general no son sometidos al poder punitivo de los Estados, y ello también se debe a la enorme brecha tecnológica que afecta a la mayoría de los mismos y resguarda a unos pocos.

Dra. Martha Inés Miravete Cicero
@gmafddhh – www.grupodemujeres.org.ar

ANEXO

- Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina, publicado en Derecho Penal y Procesal Penal, editorial Abeledo Perrot, Bs As - 2013
- Tecnología informática: ¿un nuevo desafío para el proceso penal?, XXV Congreso Nacional de Derecho Procesal Penal, Editor Rubinzal.
- El acceso transfronterizo de datos y las técnicas de acceso remoto a datos informáticos: nuevos desafíos de la prueba digital en el proceso penal, su tesis doctoral presentada en Córdoba en mayo 2017, recientemente editada Ad-Hoc.
- Ley El 4 de Junio del año 2008 el Congreso Nacional sancionó la **Ley 26.388 de delitos informáticos que modificó el Código Penal** para incluir como conductas típicas la falsificación de documentos electrónicos (CP, art. 77 y 292); ofrecimiento y distribución de pornografía infantil – la tenencia solo fue tipificada cuando tiene fines inequívocos de distribución o comercialización- (CP, art. 128); conductas vinculadas a la violación de secretos y la privacidad que incluyen el acceso ilegítimo a sistemas informáticos ajenos, la intercepción de correspondencia electrónica y otras formas de comunicación, la revelación de secretos y los delitos relacionados con la protección de datos personales (CP, arts. 153, 153 bis, 155, 157 y 157 bis); fraude informático (CP, art. 173, inc. 16); daño informático (CP, arts. 183 y 184); interrupción de comunicaciones (CP, art. 197) y la destrucción de pruebas contenidas en soportes informáticos (CP, art. 255). Sobre los antecedentes de la Ley 26.388 y los problemas dogmáticos de los tipos penales sancionados, ver. Pablo Palazzi, *Los delitos informáticos en el Código Penal. Análisis de la Ley 26.388*, editorial Abeledo Perrot, Buenos Aires, 2009

Dra. Martha I. Miravete Cicero – Presidenta del Grupo de Mujeres de la Argentina – Foro de VIH Mujeres y Familia – email denunciasddhh@gmail.com - Twetter: @gmaddhh web: www.grupodemujeres.org.ar
Participaron: Dra. Natalia Torres, Dra. Daiana Ibave, Mg. Ester Hublich, Sr. Ashur Nufuri, Ing Hugo Corral