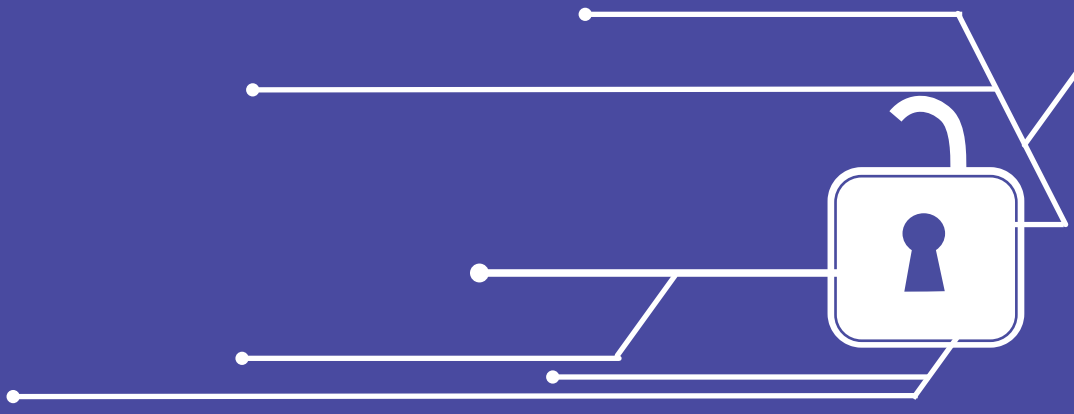
Observatorio Centroamericano de Seguridad Digital

- Informe anual 2017 -



Fundación Acceso, 2018

Observatorio Centroamericano de Seguridad Digital - Informe 2017

Elaborado por: Sara Fratti

Revisado por: Tanya Lockwood

En colaboración con: Alejandro Durón, Gema Jiménez y David Oliva

Índice

D. EL SALVADOR

E. NICARAGUA

F. Bibliografía

A. Introducción

El Observatorio Centroamericano de Seguridad Digital (OSD) surgió en el año 2016 como una iniciativa de Fundación Acceso.

El objetivo general del OSD es registrar y analizar incidentes de seguridad digital de personas defensoras de derechos humanos que estén ejerciendo su defensoría en Guatemala, Honduras, El Salvador y/o Nicaragua.

Para alcanzar este objetivo, Fundación Acceso visita y da seguimiento a las personas u organizaciones defensoras de DDHH que reportan un incidente a su seguridad digital, lleva un registro de los incidentes reportados y elabora el presente informe anual con la información recolectada.

Con esto se busca fortalecer los mecanismos de seguridad de defensoras y defensores de DDHH, posicionar el tema de la seguridad digital como un componente clave de la seguridad integral, fortalecer el análisis de la seguridad integral de defensores/as de DDHH en Centroamérica y apoyar potenciales litigios estratégicos con información basada en análisis jurídico e informático.

Durante los meses de registro y análisis del Observatorio (junio – noviembre 2017) registramos 24 casos de Honduras, Nicaragua y Guatemala. En el caso de El Salvador, se recibieron dos casos, sin embargo estas no pudieron ser analizados debido a la falta de respuesta en la comunicación por parte de las organizaciones / personas defensoras afectadas. Por esta razón, el capítulo de El Salvador carecerá de casos analizados pero se mantendrá el capítulo con sus apartados de contexto legal.

A.1. Derechos humanos en Internet

Es importante destacar que el derecho a la privacidad e intimidad se encuentra reconocido el Derecho Internacional, en el artículo 12 de la Declaración Universal de los derechos humanos[1], en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[2], así como en el artículo 11 de la Convención Americana de derechos humanos[3]. En los cuales se reafirma el derecho a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, así como a obtener la protección jurídica pertinente a nivel nacional.

1. Organización de Naciones Unidas. **Declaración Universal de derechos humanos.** Disponible en: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf
2. Organización de Naciones Unidas. **Pacto Internacional de Derechos Civiles y Políticos**. Disponible en: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx
3. Organización de Estados Americanos. **Convención Americana de derechos humanos**. Disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

El derecho a la privacidad además de ser un elemento importante para la consolidación de sociedades democráticas, es esencial para el ejercicio de otros derechos fundamentales como el libre acceso a la información, libertad de expresión y libertad de asociación y manifestación. Los cuales resultan aún más necesarios de proteger en el contexto de la defensa de derechos humanos, como consecuencia se requiere un análisis interseccional del marco jurídico internacional y nacional con esta importante labor que trasciende a la esfera digital.

En la última década y, principalmente tras las revelaciones de Edward Snowden, es de conocimiento público, derivado de esas y otras filtraciones posteriores, que los gobiernos de todo el mundo, incluyendo varios de América Latina, han adquirido diferentes mecanismos y software para la vigilancia masiva de las comunicaciones. Estas herramientas de vigilancia están dirigidas principalmente a personas opositoras, defensoras de derechos humanos y activistas de diferentes causas, con la finalidad de intimidar y censurar sus causas, por la naturaleza de la información que pueden obtener.

Claramente, la utilización de los mecanismos de vigilancia atenta contra los estándares internacionales en materia de derechos humanos consagrados en diferentes tratados y legislaciones, principalmente la legalidad, debido proceso, necesidad y proporcionalidad, entre otros. Los gobiernos están utilizando diferentes herramientas de vigilancia digital sin control alguno, como nuevas estrategias de represión social.

Los principios antes mencionados, forman parte del catálogo de los *Principios Internacionales sobre la Aplicación de los derechos humanos sobre la Vigilancia de las Comunicaciones*[4] desarrollados por un grupo de organizaciones de sociedad civil, entre ellas Electronic Frontier Foundation, Article 19, Privacy International, entre otras.

Estos principios ampliamente desarrollados también funcionan como una guía de buenas prácticas para los gobiernos que deciden actualizar su marco jurídico relacionado a la vigilancia de las comunicaciones, para que garanticen los derechos humanos. Los 13 principios desarrollados son un análisis basado en estándares internacionales (interamericanos[5] y universales) y cómo se deben aplicar a la vigilancia de las comunicaciones. Sirven como guía para que los gobiernos tengan un marco normativo y de control al momento de realizar actividades de vigilancia masiva, además permiten que la sociedad civil posee mecanismos de fiscalización frente a posibles arbitrariedades. En este sentido, la Corte Interamericana de derechos humanos ha determinado que una de las causas directas del monitoreo de las comunicaciones de las y los defensores de derechos humanos,

4. Electronic Frontier Foundation (2014). **Necesarios y Proporcionados: Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones**.
Disponible en: https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

5. Electronic Frontier Foundation y Derechos Digitales (2016). **Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones y el Sistema Interamericano de Protección de derechos humanos.** Disponible en: https://necessaryandproportionate.org/files/2016/08/23/iachr-sp-agosto2016.pdf

sin la observación de los requisitos legales, causa temor y altera el normal ejercicio del derecho de asociación.[6] Lo cual es perjudicial para la actividad de defensa de los derechos humanos en la región.

A pesar que la mayoría de Constituciones de los países centroamericanos de alguna manera reconocen la privacidad e intimidad como derechos inherentes, los legisladores de las Asambleas y Congresos olvidan estos preceptos constitucionales al momento de presentar y aprobar proyectos de legislación ordinaria. La Electronic Frontier Foundation desarrolló una serie de recomendaciones[7] para los gobiernos de América Latina, incluida Centroamérica, en la que detalla las disposiciones legislativas sobre vigilancia masiva de las comunicaciones que deben ser derogadas o reformadas, y en qué sentido. Específicamente en el sentido que las legislaciones sobre Internet no deben incluir definiciones vagas que puedan permitir posteriores vulneraciones desproporcionadas de los derechos fundamentales.

Michel Frost, Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas en sus informes ha demostrado gran preocupación sobre los diferentes mecanismos que utilizan los gobiernos para restringir la libertad de expresión y otros derechos fundamentales en Internet. Considera que Internet es una de las plataformas más relevantes que facilitan el acceso a la información y a exigir la transparencia. Sin embargo, los gobiernos realizan diferentes actividades, desde limitar el acceso a Internet hasta remoción de contenido, pasando por implantación de spyware, todo con la finalidad de censurar las voces de defensores y defensoras de derechos humanos.

En este sentido, una de sus preocupaciones principales se refiere al efecto que estos mecanismos han tenido en las y los defensores de derechos humanos, ya que utilizan las tecnologías, como Internet y las redes sociales para promover el respeto a los derechos fundamentales. Los gobiernos se han dedicado a presentar acusaciones de difamación contra defensoras y defensores, incluso inician campañas de desprestigio y acoso, con la finalidad de reprimir sus opiniones.

Por su parte David Kaye, Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión de las Naciones Unidas, también ha señalado en sus Informes anuales que los gobiernos últimamente tienden a controlar, limitar o vigilar el derecho a la libertad de expresión en Internet. Incurren en prácticas como interferir las conexiones, interceptar comunicaciones privadas, generalmente con asistencia de actores del sector privado de las telecomunicaciones, como los proveedores de servicios de Internet. Además, con técnicas como el

6. Comisión Interamericana de derechos humanos (2016). **Informe Criminalización de defensoras y defensores de derechos humanos**. Disponible en: https://www.oas.org/es/cidh/informes/pdfs/criminalizacion2016.pdf

7. Electronic Frontier Foundation (2016). **Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica**. Disponible en: https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016_es_0.pdf

filtrado de contenido, censura, priorizar contenidos o aplicaciones, vulnerando la Neutralidad de la Red, una de las invariantes de Internet.

Edison Lanza, Relator Especial para la Libertad de Expresión de la Comisión Interamericana de derechos humanos, ha expresado que Internet es una herramienta que facilita que las personas busquen, reciban y difundan información, potencializando el ejercicio del derecho a la libertad de expresión en sus comunidades. Sin embargo, ha señalado diferentes prácticas de violencia e intimidación hacia periodistas y personas defensoras derechos humanos en la región. Por ejemplo, mecanismos de vigilancia masiva, censura estatal e incluso ataques cibernéticos. También enfatizó que "los Estados prevengan, protejan e investiguen las agresiones que se comentan en detrimento de quienes informan a través de Internet.[8] Así mismo ha enfatizado que la protección de la libertad de expresión en Internet también debe aplicarse a códigos, protocolos, hardware e infraestructuras de telecomunicaciones.

Amnistía Internacional en su informe anual[9] (2017) enfatizó gran preocupación sobre los mecanismos desproporcionados que utilizan los gobiernos para acosar e intimidar a las personas que se dedican a la defensa de los derechos humanos y el rol que juegan las nuevas tecnologías en este ámbito. Se ha comprobado que diferentes gobiernos han adquirido diferentes clases de software, como malware y spyware, para vigilar a las y los defensores de derechos humanos. Además se dedican a realizar campañas de difamación, propagando noticias falsas a través de las redes sociales en contra de personas activistas y defensoras.

Front Line Defenders en su informe anual[10] (2016) también expresó su preocupación en relación a las malas prácticas que están adoptando los gobiernos para silenciar y perseguir a las personas defensoras de derechos humanos. La utilización de herramientas digitales para restringir el acceso a Internet y aplicaciones, también el bloqueo de contenidos e incluso pagar a personas (destacando los perfiles falsos en redes sociales) para que difundan rumores y calumnias, así como la adquisición de software y herramientas de vigilancia masiva que generalmente es utilizada en contra de activistas, opositores/as y defensores y defensoras.

8. Comisión Interamericana de derechos humanos (2017). **Informe Zonas Silenciadas: regiones de alta peligrosidad para ejercer la libertad de expresión.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ZONAS_SILENCIADAS_ESP.pdf Pág. 122.

9 Amnistía Internacional (2017). I**nforme annual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/

10. Front Line Defenders (2016). **Annual Inform Human Rights Defenders at risk in 2016**. Disponible en: https://www.frontlinedefenders.org/en/resource-publication/2016-annual-report

A.2. ¿Qué es un incidente de seguridad digital?

En el marco de las actividades del Observatorio Centroamericano de Seguridad Digital se registran los casos ocurridos a personas defensoras de DDHH en Centroamérica relacionados con su información y/o comunicación digital almacenada, en movimiento y en servicios.

En consecuencia, con base en lo establecido por la Organización de las Naciones Unidas, se entiende que defensor/a de derechos humanos es un individuo, grupo e institución de quienes se tenga referencia que luchen por la defensa de derechos humanos de los pueblos y las personas, y, en el contexto de este proyecto, que ejerzan su labor en Guatemala, Honduras, El Salvador y/o

Nicaragua, sin importar su género, edad, lugar de procedencia, antecedentes profesionales o de ningún otro tipo[11]. Además, en el marco del Sistema Interamericano de Protección de derechos humanos (SIDH), la Comisión Interamericana de derechos humanos (CIDH) reconoce la existencia de el derecho a defender los derechos humanos de las personas defensoras.[12]

Por otra parte, incidente se refiere a cualquier evento adverso (verificado o en sospecha) relacionado con la información (incluyendo datos y metadatos) y/o comunicación digital.

Para que esta información y/o comunicación se considere digital debió ser creada, procesada y comunicada por los dispositivos electrónicos computacionales de la actualidad, y que puede estar almacenada, transmitida o puede encontrarse en un servicio en línea o en cualquiera de las aplicaciones que se utilizan para acceder a ellos (como correo electrónico, redes sociales, blogs y medios independientes en línea).

Cuando se identifica un incidente que no cumple con estos criterios para ser registrado por el Observatorio, desde Fundación Acceso se brinda la atención técnica necesaria, en caso que la información que pudo estar comprometida o en el caso que sea un incidente de otra variable de la seguridad, ya sea física, legal o psicosocial, con la finalidad de referir el caso con organizaciones aliadas u otras instancias, nacionales o regionales que trabajen ese tema en particular.

A.3. Tipología de incidentes

Los incidentes se catalogan con base en la siguiente tipología:

Ataques LAN[13]: Bloqueo del tráfico de datos que circula en la red local, interrupción de las conexiones entre las computadoras de la red, denegación de acceso de servicios y generación de tráfico en la red. Un ejemplo es el de reconfigurar los routers o modems para bloquear determinadas páginas.

Ataques remotos: Toma de control del equipo o extracción de información del mismo de forma remota, logrando el acceso mediante una conexión a Internet o a una red. Los ataques remotos aprovechan vulnerabilidades del módem[14] o del sistema operativo.

11. Organización de Naciones Unidas. **Resolución 53/144 del 8 de marzo de 1999**. Disponible en: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

12. Comisión Interamericana de derechos humanos. **Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas.** Disponible en: https://www.cidh.oas.org/countryrep/Defensores/defensoresindice.htm

13. LAN en inglés significa Red de Área Local y se refiere al conjunto de computadoras ubicadas en un espacio determinado (como las oficinas de una organización), que pueden compartir archivos entre ellas y también pueden compartir salida a la Internet.

14. El Módem es el aparato proporcionado por el proveedor del servicio de Internet. Convierte la información digital generada por las computadoras en frecuencias de sonido para ser transmitidas por una red telefónica, es decir, el aparato por medio del cual las computadoras se conectan a Internet.

Ataques Web: Toda ataque a los servicios de Internet que utilizamos y el monitoreo de los mismos. Estos pueden ser los servicios de blogs, noticias, radios en línea, nuestros sitios web, bloqueo de nuestro canal de Youtube, otros así como el monitoreo de nuestro comportamiento a partir de los sitios que visitamos.

> Una de las principales técnicas informáticas para este tipo de ataque es DDoS (ataque de denegación de servicios), que es un ataque a la red que causa que un servicio o recurso sea inaccesible. También entran en esta categoría la censura de determinados sitios web por parte del Proveedor del Servicio de Internet (ISP), el monitoreo de tráfico, robo de identidad en la Web, suplantación de sitio web, aparición de publicaciones no autorizadas en el sitio Web, cambios en el Servidor de Nombres de Dominio (DNS), inadecuada actualización y respaldo del sitio Web.

Compromiso de cuentas: Ésta es una categoría especial que debería estar contenida en "Ataques a Web" pero que específicamente trata de craqueo de nuestras credenciales para acceder a los servicios que utilizamos. Se decide separar por la cantidad de incidentes de éste tipo que normalmente se dan[15].

> Una de las principales técnicas informáticas para este ataque es el Phishing[16] o suplantación de identidad, caracterizado por intentar adquirir información confidencial de forma fraudulenta, particularmente las contraseñas de cualquier cuenta de correo electrónico, de suscripciones en Internet, de redes sociales, de administración de Hosting y sitios Web, cuentas bancarias, tarjetas de crédito, etc.

Malware[17] o software malicioso: Cualquier tipo de software[18] que se ejecuta en los dispositivos para interrumpir las operaciones y recolectar información sensible sin consentimiento del usuario/a administrador/a. También se pueden instalar simultáneamente, pero de manera oculta como complementos extras de algunos programas aparentemente legítimos, legales, sin mala fe o sin terceras u ocultas intenciones.

Uno de los malware más peligrosos es el conocido como spyware[19] o programa espía el cual recopila información almacenada en el dispositivo y la transmite a una entidad externa sin consentimiento del usuario administrador. Los programas instalados en celulares que realizan escuchas telefónicas, o incluso que activan vídeo y audio también son considerados malware.

15. Recomendación del equipo de Access Now a partir de su experiencia con el Help Desk. https://www.accessnow.org/linea-de-ayuda-en-seguridad-digital/
16. Ed Skoudis. Phone phishing: The role of VoIP in phishing attacks.
17. Definición de Malware obtenida de techterms.com http://techterms.com/definition/malware
18. Se entiende Software como cualquier componente no tangible, por medio del cual se ejecutan determinadas instrucciones o rutinas que permiten utilizar un dispositivo.
19. FTC Report (2005). Disponible en: http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

Observatorio Centroamericano de Seguridad Digital

Momentos de Intervención:

1 Contacto Inicial

Ya sea por llamada telefónica, video-llamada, e-mail, mensaje de texto, mensajería instantánea, o personalmente. Se decide si puede o no ser un incidente, y si el/la técnico/a asistirá o no al lugar (1° Módulo del reporte)

2 Verificación

Técnico/a asiste al lugar para definir si efectivamente es un incidente o si es un falso positivo (2° Módulo del reporte)

3 Pre-diagnóstico

Si efectivamente es un incidente, se realiza una nueva visita al lugar con el/la abogado/a y se realiza un pre-diagnóstico, se define una estrategia (en conjunto con el/la defensor/a u organización de DDHH) y se decide si solo se registra o si es un posible caso jurídico (3° Módulo del reporte)

4 Implementación de Estrategias

Abogado/a y técnico/a realizan las acciones de la estrategia a la que se comprometieron durante la estrategia (4° Módulo del registro)

5 Peritaje Especializado

Abogado/a y técnico/a deciden si es necesario hacer un peritaje especializado para el que se necesita apoyo externo (Se agrega un 5° Módulo al registro con las acciones a tomar)

6 Resultados Peritaje

Resultados del peritaje (Se agrega un 6° Módulo al registro con los resultados del peritaje)

FUNDACIÓN Acceso

Pérdida de hardware: Robo, hurto, destrucción, o extravío del equipo. Un ejemplo de esto es la destrucción de equipo en un allanamiento ilegal.

Retención de hardware: Equipo incautado, confiscado y/o retenido por parte de agentes del Estado, con o sin orden legal, con o sin justificación legítima.

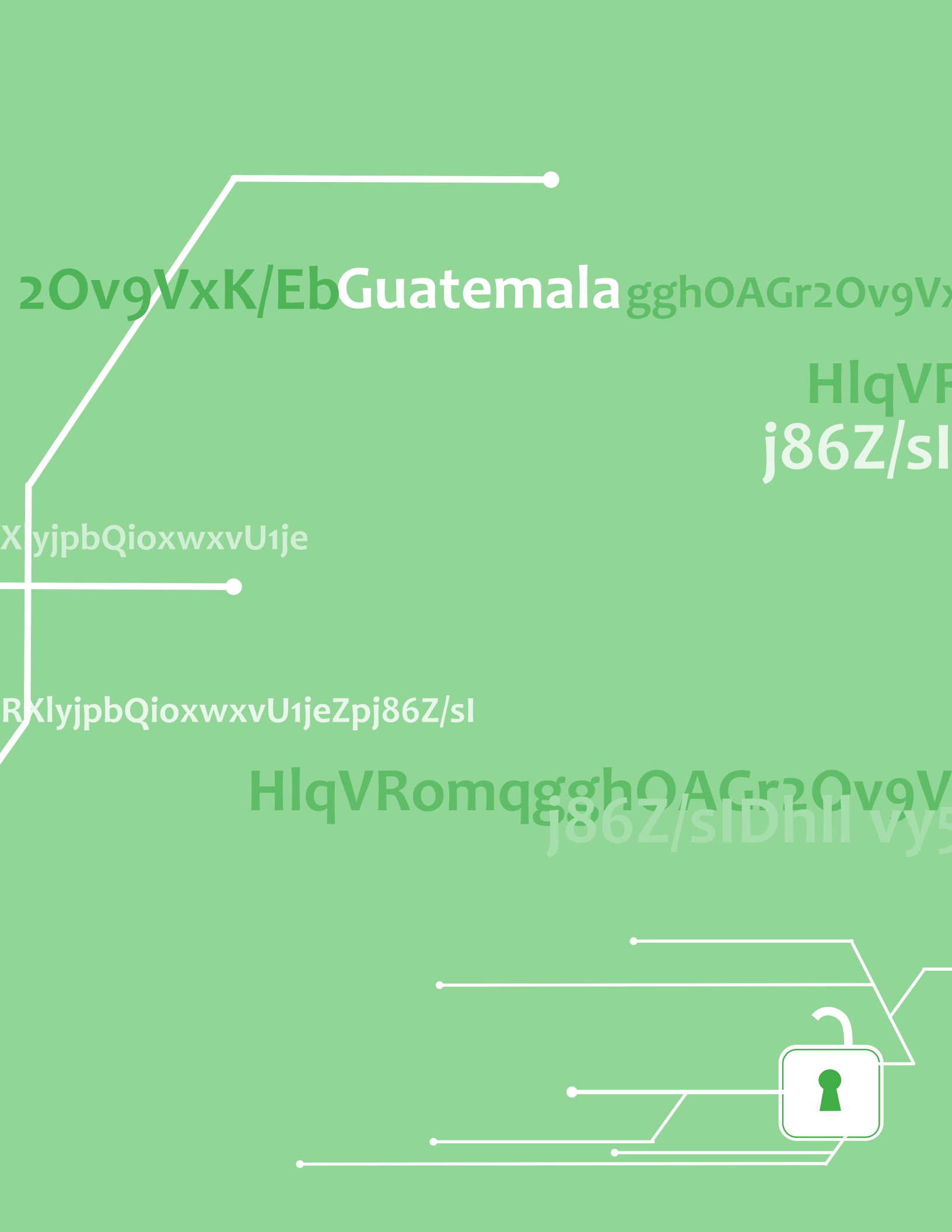
A.4. Procedimiento para el registro de incidentes

Al momento que el equipo de Fundación Acceso tiene conocimiento sobre un posible incidente de seguridad digital se procede al registro del mismo, además de prestar el servicio técnico necesario para proteger la información digital de la persona u organización.

Se inicia con la obtención del consentimiento informado para asegurarse que la persona usuaria está enterada de la intervención que se realizará sobre su equipo. Posteriormente se obtiene su autorización para realizar la inspección técnica (dependiendo del tipo de incidente que se trate, esto puede llevar desde horas hasta algunas semanas).

Durante el período que dure la inspección, la persona técnica encargada debe llenar una bitácora donde registra todas las acciones llevadas a cabo en el equipo, con el fin de demostrar que en su intervención se han realizado únicamente aquellas acciones dirigidas a determinar el origen del problema que presenta el equipo. Por último se registra la finalización de la inspección y devolución del equipo, donde constan las conclusiones de la inspección y posibles acciones de seguimiento.

Los casos registrados para este año del Observatorio han sido producto del conocimiento y de la relación que el equipo de la Fundación Acceso tiene con diversas organizaciones y personas que trabajan en la defensa de los derechos humanos en Guatemala.


2Ov9VxK/EbGuatemalagghOAGr2Ov9Vx
HlqVR
j86Z/sI
XlyjpbQioxwxvU1je
RXlyjpbQioxwxvU1jeZpj86Z/sI
HlqVRomqgghOAGr2Ov9V
j86Z/sIDhII vy5

B. CAPÍTULO GUATEMALA

B.1. Contexto Legal: Internet y Derechos Humanos en Guatemala

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[20] , en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[21], sin embargo, la legislación penal existente en relación a la protección del derecho a la privacidad digital aún no se encuentra regulada.

En este sentido, desde el 2009 la Iniciativa 4090, que dispone aprobar la Ley de Protección de Datos Personales[22] posee dictamen favorable y se encuentra pendiente del tercer debate en el Pleno del Congreso desde el año 2010, previo a su aprobación. La existencia de un marco jurídico en materia de protección de datos personales favorecería a una adecuada protección de la privacidad en línea de las y los defensores de derechos humanos, ya que tendrían mecanismos para ejercitar sus derechos frente al gobierno o empresas.

Durante el transcurso del año 2017, se han presentado un catálogo de iniciativas de ley en el Congreso de la República que de una u otra manera pueden perjudicar en el ejercicio de diferentes derechos humanos en Internet, especialmente para las personas defensoras en el país.

La iniciativa 5230[23] que dispone aprobar la reforma al Decreto Número 17-73 del Congreso de la República, Código Penal, reforma específicamente el inciso d) del artículo 274, la cual regula el delito de difamación, incluyendo dentro del tipo penal la creación de "banco de datos, una cuenta o usuario en una red social virtual o software social o de un registro informático, con datos que puedan afectar la intimidad, honorabilidad, o dignidad de las personas", exceptuando el caso regulado en el artículo 35 de la Constitución sobre la libre emisión del pensamiento, imponiendo una pena de prisión de 4 a 8 años. Sin embargo, esta iniciativa fue presentada con el objeto de proteger la dignidad, honorabilidad e intimidad de las personas, sin embargo la finalidad principal

20. Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

21. Ibíd. Pág 175.

22. Congreso de la Repúbica de Guatemala. **Iniciativa 4090, Ley de Protección de Datos Personales**. Disponible en: http://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf

23. Congreso de la República de Guatemala. **Iniciativa 5230.** Disponible en: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=2636

es evitar que la ciudadanía se manifieste en redes sociales en contra de los actos de corrupción que realizan a funcionarios y funcionarias públicos de turno. En este sentido, este proyecto en algún momento puede ser un peligro para la libertad de expresión en Internet. Además, las personas defensoras no podrán sentirse seguras emitiendo su opinión en redes sociales. Esta iniciativa ya posee dictamen favorable por la Comisión de Legislación y Puntos Constitucionales, actualmente se encuentra pendiente de tercer debate en el Pleno del Congreso.

La iniciativa 5239 que dispone aprobar la Ley Contra Actos Terroristas[24], ya posee dictamen favorable por la Comisión de Gobernación y se encuentra pendiente de ser conocida en el Pleno del Congreso. En términos generales este proyecto tiene como finalidad criminalizar las protestas ciudadanas[25]. Regula el delito de "terrorismo cibernético o ciberterrorismo" con prisión de 10 a 20 años. Además, se establece que se promoverá una red de inteligencia para controlar el movimiento de presuntos terroristas, sin embargo, no determina los estándares mínimos para este control y posible vigilancia masiva.

La iniciativa 5254 que dispone aprobar la Ley contra la Ciberdelincuencia[26], ya posee dictamen favorable y se encuentra pendiente de Dictamen por la Comisión de Gobernación. Sin embargo, el contenido de este proyecto carece de enfoque de derechos humanos y criminaliza conductas que en algún momento podrían afectar la actividad de las personas usuarias y de la labor de defensoría y/o denuncia de violación a derechos humanos.

Por otro lado, desde el lado del gobierno el desarrollo de políticas públicas en relación a la temática de Internet y Tecnologías de la Información y Comunicación, en el transcurso del año se han desarrollado algunos proyectos que deben ser mencionados por el posible impacto, positivo o negativo, para las personas defensoras en Guatemala.

Desde la Superintendencia de Telecomunicaciones (SIT), con el apoyo de otras entidades gubernamentales, se desarrolló la agenda digital denominada Nación Digital[27]. La cual posee como ejes de acción la utilización de las Tecnologías de la Información y Comunicación en la salud, educación, seguridad, desarrollo y transparencia. Sin embargo, esta agenda aún carece de objetivos reales y concretos, hasta el momento se desconocen los sectores o entidades que participarán en su ejecución y tampoco tiene un eje de protección de derechos humanos en Internet.

24. Congreso de la República de Guatemala. **Iniciativa 5239**, Ley contra Actos Terroristas. Disponible en: http://www.congreso.gob.gt/iniciativa-de-ley-de**talle/?id=3607**

25. Prensa Libre. Una peligrosa propuesta de ley. Disponible en: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley

26, Congreso de la República de Guatemala. **Iniciativa 5254**, Ley contra la Ciberdelincuencia. Disponible en: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf

27. Nación Digital. https://www.naciondigital.gob.gt/

El Ministerio de Gobernación, a través del IV Viceministerio de Tecnologías de la Información y Comunicación, con el apoyo de la Organización de Estados Americanos (OEA), han promovido la elaboración de la Estrategia Nacional de Ciberseguridad[28]. Esta Estrategia en términos generales pretende generar y coordinar una hoja de ruta a mediano y largo plazo para diseñar e implementar acciones para proteger la seguridad nacional frente a la ciberdelincuencia. En este proceso, que aún continúa, se han convocado a diferentes sectores (instituciones gubernamentales, del sector justicia, sector privado, academia, comunidad técnica y sociedad civil) para su elaboración. Sin embargo, el actual borrador de la Estrategia carece de un enfoque de derechos humanos, además la protección de la privacidad en línea y datos personales no es una prioridad en este proyecto.

Esto último es necesario destacar, ya que la creación de políticas públicas relacionadas a Internet y las nuevas tecnologías requiere de un elemento de reconocimiento a nivel nacional de estándares mínimos de protección de derechos fundamentales en el contexto digital. La falta de participación de organizaciones que se dedican a la defensa de derechos humanos también es perjudicial, ya que la elaboración de esta Estrategia debe involucrar a sectores claves. Además, es muy preocupante que las políticas públicas contenidas únicamente sean elaboradas bajo el enfoque de "seguridad nacional", lo cual puede perjudicar el actuar de las personas defensoras, principalmente por la tradición que tiene el gobierno de catalogar a estas organizaciones como grupos desestabilizadores o terroristas. Además, es un peligro en el sentido que la estrategia sea aprobada como actualmente se encuentra, ya que será la base para el desarrollo e implementación de futuras políticas públicas relacionadas con ciberseguridad.

Durante este año han existido importantes avances en materia de discusión alrededor de temáticas sobre Internet y derechos humanos. Por un lado, la organización internacional The World Wide Web Foundation elaboró un proceso colaborativo y descentralizado para promover el diálogo alrededor de los derechos humanos en línea entre diferentes sectores de la sociedad civil, denominado la Carta de Derechos de Internet en Guatemala[29].

La Alliance for Affordable Internet (A4AI) se encuentra promoviendo la Coalición Guatemalteca para una Internet Asequible[30], con la finalidad de construir diálogo entre el sector público, privado y sociedad civil para el desarrollo e implementación de políticas públicas y regulatorias para que el acceso a Internet sea asequible en el país.

Por otro lado, el 27 de julio 2017 se desarrolló del primer Foro de Gobernanza de Internet de Guatemala[31], en el cual se discutieron temas relacionados con la privacidad digital, aunque de una

28. Ministerio de Gobernación. **Presentan conclusiones para mejorar Borrador de la Estrategia Nacional de Ciberseguridad**. Disponible en: http://mingob.gob.gt/presentan-conclusiones-para-mejorar-el-borrador-de-la-estrategia-nacional-de-ciberseguridad/

29. World Wide Web Foundation. **Carta de Derechos de Internet en Guatemala.** Disponible en: http://1e8q3q16vyc81g8l3h3md6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2017/06/Carta-de-Derechos-de-Internet-para-Guatemala.pdf

30. Alliance for Affordable Internet. **Coalición Guatemalteca para una Internet Asequible.** Disponible en: http://a4ai.org/guatemala/

manera muy general, sin incluir la protección de las personas defensoras de derechos humanos.

Estos espacios reflejan que cada vez se hace más necesario promover diálogos alrededor de la protección de los derechos humanos en línea y que la población exija reconocimiento y respeto de estos, así como la inclusión en estas conversaciones en la protección de las defensoras y los defensores. Esto les coloca en una situación de especial vulnerabilidad pues ante esos vacíos normativos es más probable que este tipo de ataques y sus perpetradores, ya sean empresas o agentes del propio estado, queden en la impunidad.

B.2. Ataques a defensoras y defensores de derechos humanos

La UDEFEGUA en su reciente informe[32] semestral (enero-junio 2017), indica que sólo en 6 meses se registraron un total de 236 agresiones contra personas defensoras en Guatemala. Estas agresiones en su mayoría corresponden a: asesinatos, intimidación, difamación, denuncia judicial, detenciones arbitrarias e ilegales y amenazas. Así mismo, 72 de estas agresiones se dieron contra personas que defienden el derecho humano a un ambiente sano (tierra, territorio y recursos naturales), y un 45% de las agresiones fueron contra mujeres defensoras.

Esta situación también es evidenciada en el informe anual de Amnistía Internacional[33], que establece que las personas defensoras aún son objeto de amenazas, estigmatización, intimidación, agresión y, en algunos casos, hasta víctimas de homicidio. Los grupos más vulnerables ante estos ataques son organizaciones de defensa de la tierra, territorio y medio ambiente.

Michel Frost, Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas en sus informes ha mostrado preocupación "por la falta de investigaciones independientes y diligentes sobre las agresiones cometidas contra los defensores de los derechos humanos ambientales, hecho que suele estar vinculado a la falta de recursos, la corrupción y la colusión entre los autores. Los Estados casi nunca han conseguido hacer comparecer ante la justicia a los autores y que estos fueran sancionados."[34]

Es importante destacar el rol de las plataformas de redes sociales para las personas defensoras en Guatemala y medios de comunicación e investigación independientes, en el sentido que son un espacio para difundir sus opiniones y actividades, principalmente en la creciente lucha contra la corrupción en el país; la defensa del territorio, el derecho a la consulta previa, el medio ambiente,

31. Foro de Gobernanza de Internet de Guatemala. http://igf.gt/

32. Udefegua (2017). Situación de Defensoras y Defensores de derechos humanos en Guatemala Un Reflejo del Deterioro de los derechos humanos en el País. Disponible en: http://udefegua.org/wp-content/uploads/2017/10/201709-Sit-Defensores-DH-SEMESTRAL.FIN_.pdf

33. Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de derechos humanos en el Mundo**. Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Pág. 217.

34. Relatoría Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas. **Informe sobre la Situación de los defensores de los derechos humanos 2016.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement

y durante los procesos de acceso a la justicia por la violación histórica a los derechos humanos.

En el último año, para la población y sociedad civil Twitter ha sido fundamental para la movilización ciudadana para exigir, entre otras cosas, la renuncia de funcionarios públicos de altos cargos, incluido el actual Presidente de la República. Como consecuencia, el aumento de perfiles considerados como bots o net centers[35] han propiciado la desinformación (desde propagación de noticias falsas hasta difamación en contra de activistas y medios independientes), principalmente para debilitar el trabajo de investigación realizado por la Comisión Internacional contra la Impunidad en Guatemala (CICIG)[36], el Ministerio Público (MP)[37], y múltiples organizaciones nacionales de derechos humanos (y particularmente a las mujeres defensoras).

Recientemente, un grupo integrado por 12 medios de comunicación solicitó al Ministerio Público que investigue el acoso que han sufrido en redes sociales, principalmente por cuentas de net centers, afirman que han sufrido "hackeos, ataques de net centers y amenazas directas, en especial contra mujeres".[38] Claramente el tema de la utilización de bots en contra de activistas y medios independientes con la finalidad de difamar o desestabilizar, la están utilizando directa o indirectamente varios gobiernos, uno de los problemas principales es lograr identificar si existe financiamiento público para estas actividades. Por otro lado, lamentablemente el Ministerio Público no posee la capacidad técnica para establecer cuáles son los perfiles “falsos o bots”, lo cual podría traer un peligro aún mayor como vigilancia y posible criminalización de activistas y personas defensoras de derechos humanos.

Finalizando la edición de este informe del Observatorio, salió a la luz pública un interesante artículo titulado Los Netcenters: negocio de manipulación de Luis Assardo, el cual detalla cómo han funcionado en Guatemala y cuales son sus efectos[39].

Por otro lado, en el marco de las investigaciones alrededor de diferentes delitos cibernéticos, desde el Ministerio de la Defensa, han manifestado públicamente la intención que sea el Ejército de Guatemala el encargado de realizar las investigaciones sobre las amenazas cibernéticas para resguardar la economía e instituciones del país[40]. El peligro que el Ejército realice investigaciones sobre ciberamenazas es terrible para la ciudadanía, porque existe una gran posibilidad que se dedique a vigilar y colectar información de ciudadanos, activistas y personas defensoras de derechos humanos.

35. Soy502. **Los netcenteros de la impunidad.** Disponible en: http://www.soy502.com/articulo/netcenteros-impunidad-20878

36. Comisión Internacional contra la Impunidad en Guatemala. http://cicig.org/

37. Nómada. **#JimmySeQueda: el netcenter de @rodrigopolo, @rmendezruiz y @pirulismo.** Disponible en: https://nomada.gt/asi-se-fabrico-el-jimmysequeda-el-netcenter-de-rodrigopolo-rmendezruiz-y-pirulismo/

38. Soy502. **Periodistas exigen que el MP investigue a los “net centers”.** Disponible en: http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-ciberneticos-149

39. Medium.com. **Los Netcenters: Negocio de Manipulación.** https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc

40. Soy502. **El Ejército quiere encargarse de las amenazas cibernéticas.** Disponible en: http://www.soy502.com/articulo/ejercito-quiere-encargarse-amenazas-ciberneticas-63338?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#link_time=1511180394

B.3. Principales hallazgos en Guatemala

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Guatemala. Los mismos han sido registrados entre los meses de junio y noviembre de 2017. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de incidentes digitales.

B.4. Casos registrados

Durante el transcurso del período antes mencionado, fueron registrados un total de cuatro casos e incidentes de seguridad digital con diferentes componentes y móviles, todos en la Ciudad de Guatemala.

B.5. Perfil de las personas/ organizaciones que reportaron incidentes

El primer caso, fue una fundación que se dedica a exigir el respeto de derechos humanos y que también coadyuva en la lucha por la transparencia y contra la impunidad en el país. En dos casos, se trató de un medio de comunicación independiente que se dedica a realizar periodismo de investigación, y el último caso, se trata de una organización que se dedica al acompañamiento internacional en el caso de violaciones a derechos humanos en el país.

B.6. Tipos de ataques

A continuación una breve descripción (no técnica) de los ataques registrados.

En el primer caso, el incidente se desarrolló en el contexto de las redes sociales, en la cual la persona defensora fue objeto de suplantación de identidad en una de estas plataformas.

En el caso del medio de comunicación, por un lado fue la filtración de capturas de pantalla de mensajes privados del director en un perfil anónimo y posteriormente en un sitio web externo, más allá del compromiso de la cuenta, se considera que pudo ser un ataque de phishing porque las capturas de pantalla no coinciden con las de su dispositivo móvil. Por otra parte, el sitio web oficial de este medio ha sido objeto de múltiples ataques de denegación de servicios a lo largo del año.

En el cuarto caso, el incidente consistió en la pérdida (en dos ocasiones) de toda la información de un servidor de la organización, afortunadamente poseían discos duros de respaldo con la información.

B.7. Posibles perpetradores

La identificación de los posibles perpetradores de los ataques es una tarea que interesa al Observatorio de Seguridad Digital, pero se debe informar que no siempre se logra porque un atacante regularmente tratará de anonimizarse y para ello utilizará los recursos técnicos y metodológicos que convengan para el tipo de ataque.

En tal sentido, esta tarea requiere, para los casos más complejos, recursos técnicos y acceso a servicios que están fuera del alcance de la organización. No obstante lo anterior, sobre la base de los hallazgos de los ataques se puede delinear un posible perfil técnico del atacante y sus objetivos.

En el primer y segundo caso, se realizó en el marco de campañas de difamación y acoso en contra de activistas, defensores y líderes de opinión publica que exigen lucha contra la impunidad, transparencia, entre otros. Como consecuencia, el objetivo era desprestigiar la labor que realizan estas personas y sus respectivas organización y medio de comunicación, suplantando su identidad en redes sociales para el primer caso y en el segundo filtrando comunicaciones privadas. Además, estas acciones intentan generar un estado de miedo e incluso pretenden que las personas y organizaciones acudan a la autocensura.

En el tercer caso, el medio digital a lo largo del año publicó investigaciones relacionadas a diferentes casos de corrupción del gobierno de turno, lo cual claramente ha incomodado a muchos sectores que están a favor de la impunidad en el país. En consecuencia, ejerciendo actividades de censura, como los ataques de denegación de servicios al sitio web impiden que la población tenga acceso a información de interés público.

En el cuarto caso, el hecho de eliminar toda la información de servidores de esta organización posiblemente se realizó con la finalidad de impedir que continúen realizando su labor, ya que los archivos con información sensible e importante fueron eliminados.

B.8. Mecanismos de Protección

En este apartado se presentan los marcos jurídicos que pudieron haber sido vulnerados en los casos que se han registrado en el capítulo de Guatemala del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos.

B.9 Posibles derechos humanos vulnerados

Dentro de la Constitución de la República se regula el derecho a la privacidad, en el que se establece la inviolabilidad de correspondencia, documentos y libros, en cualquier formato, salvo orden previa de juez competente.

B.10. Posibles tipificaciones penales

A partir de la investigación de marcos legales realizada en 2015 por Fundación Acceso[41] se puede establecer que el marco jurídico penal continúa siendo insuficiente para establecer mecanismos integrales de protección del derecho a la privacidad digital de las y los defensores de derechos humanos en el país.

En el caso de la pérdida de información en el servidor, dentro del Código Penal se regula en el artículo 274 "A" el delito de destrucción de registros informáticos, el cual posee una pena de prisión y de multa, para quien borre o destruya, de cualquier manera registros informáticos.

En el caso de la filtración de las capturas de pantalla y su divulgación se puede encuadrar la conducta bajo el delito de Intercepción o reproducción de comunicaciones regulado en el artículo 219 del Código Penal.

Sin embargo, en relación a los otros casos, la legislación en materia penal actual no regula los delitos de suplantación de identidad o ataques de denegación de servicios a sitios web.

B.11. Estrategias legales de respuesta

Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

Denuncias

En los casos registrados en Guatemala, corresponde denunciar ante el Ministerio Público, a quien le corresponde el ejercicio de la acción penal pública, es decir, es la entidad del sector justicia encargada de realizar la investigación de los delitos cometidos en contra de las personas defensoras.

Otras acciones

Guatemala regula a nivel constitucional y ordinario la figura del ombdusman, determinada como el Procurador de derechos humanos, ante el cual se puede interponer una denuncia en materia de violación de libertades y derechos fundamentales, en su rol de velar por el efectivo cumplimiento de estos. Sin embargo, el carácter de la sanción es de índole moral, porque está diseñado para desempeñar un rol de tribunal de conciencia; aunque tiene la capacidad legal de presentar denuncias ante los órganos jurisdiccionales competentes.

41. Fundación Acceso (2015). ¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensores y defensoras. http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf

Sistema Interamericano de derechos humanos

En relación al Sistema Interamericano de derechos humanos, posee ciertos requisitos previos a que los casos sean llevados a estas instancias regionales. Sin embargo, en situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la Comisión Interamericana de derechos humanos para que el Estado adopte medidas para prevenir daños irreparables a las personas o al objeto del proceso en conexión con una petición o caso pendiente.

Además, es un buen espacio que permite documentar estos y otros casos para identificar patrones de actuación por parte de organizaciones y oficinas gubernamenales que puedan estar vigilando a defensores y defensoras de derechos humanos. Esta información ponerla de conocimiento de las respectivas Relatorías para que pueda ser incluida en sus informes periódicos, con la finalidad de visibilizar la situación de la seguridad digital a nivel regional.

B.12. Conclusiones y Recomendaciones

Conclusiones

1.Persiste el contexto adverso para la defensa de las y los defensores de derechos humanos y los vacíos legales en el marco de protección de la seguridad digital en la labor que estos realizan, los cuales fueron identificados en la investigación de Fundación Acceso de 2015. En el Congreso de la República se han presentado y se están discutiendo iniciativas de ley que carecen de una perspectiva de derechos humanos, y en caso sean aprobadas como se encuentran actualmente pueden perjudicar la labor de organizaciones que se dedican a la defensa, denuncia y promoción de derechos humanos.

2.Existen incidentes de seguridad digital y estos afectan directamente la labor que las y los defensores de derechos humanos realizan, poniendo en peligro su información, su trabajo e incluso sus vidas.

3.El tema de la seguridad digital continúa estando ausente de los informes que tratan sobre la seguridad de las y los defensores de derechos humanos, provocando áreas de vulnerabilidad a través de las cuales estos pueden ser atacados.

Recomendaciones

1.La reforma al marco jurídico es necesaria para mejorar los mecanismos y niveles de protección a defensoras y defensores, enfatizando la necesidad de incluir herramientas de seguridad digital, incluyendo estándares internacionales en materia de Internet y derechos humanos.

2.Los colectivos y organizaciones que se dedican a la defensa de derechos humanos deben

generar mecanismos y protocolos internos enfocados a la seguridad digital, lo cual se puede lograr a través de la generación de capacidades en este tema dentro de sus propias colectividades.

3.Dentro de los informes sobre la situación de las y los defensores de derechos humanos es importante incluir secciones dedicadas a la seguridad digital, para visibilizar la importancia de esta en materia de protección y seguridad integral.

4.Una mesa nacional de análisis sobre Internet y derechos humanos convocada desde las organizaciones de derechos humanos con la participación de comunidades académicas y técnicas, sería una estrategia importante de impulsar. Las tendencias globales en materia de regulación de la Internet, sacrificando el derecho a la privacidad, rápidamente están teniendo eco en los congresos de nuestros países centroamericanos.


vzaa9VxK/EbHondurasgghOAGr2Ov9V
HlqVR
j86Z/sI
XlyjpbQioxwxvU1je
RXlyjpbQioxwxvU1jeZpj86Z/sI
HlqVRomqgghOAGr2Ov9V
j86Z/sIDhll vy5Wvrrs

C. CAPÍTULO HONDURAS

C.1. Contexto Legal: Internet y Derechos Humanos en Honduras

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[42], en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[43], sin embargo, la legislación penal existente en relación a la protección del derecho a la privacidad digital aún no se encuentra regulada.

Por otra parte, en febrero del 2017 el Congreso de Honduras aprobó la Ley para el Fortalecimiento y Efectividad de la Política de Seguridad, Decreto Número 6-2017, la que contenía un conjunto de reformas a diferentes legislaciones, como el Código Penal y Procesal Penal, Ley contra el Financiamiento del Terrorismo, Ley de Inteligencia Nacional, Ley de Limitación de Servicios de Telecomunicaciones en Centros Penitenciarios, Granjas Penales y Centros de Internamiento de Niños y Niñas a Nivel Nacional, Ley Especial sobre Intervenciones de las Comunicaciones Privadas, Ley de Recompensas y Ley del Sistema Penitenciario Nacional. Esta Ley fue aprobada en el contexto de la lucha contra el crimen, provee una serie de disposiciones y modificaciones en materia penal con la finalidad de reducir los delitos. Sin embargo, varias organizaciones, locales e internacionales[44], se pronunciaron en contra de esta Ley, ya que carecen de enfoque de derechos humanos.

Se realizaron reformas al Código Penal, en las que se modificaron los delitos de Extorsión y Terrorismo, y a la Ley de Centros Penitenciarios. Fue una de las reformas más criticadas, específicamente en contra de una de las reformas más preocupantes fue al delito de terrorismo, ya que su regulación es muy amplía y existe un profundo temor que pueda ser utilizada como una "ley mordaza" vulnerando la libertad de expresión, ya que equipara las protestas ciudadanas como terrorismo[45]. Las reformas al Código Penal amplía las conductas "terroristas", incluyendo quien cause estragos o daño a la propiedad, o quien no participe directamente en esos daños, pero que si

42. Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

43. Ibíd. Pág 192.

44. Amnistía Internacional. **Declaración Pública AMR 37/5587/2017 del 27 de enero de 2017.**

45. El Heraldo. **Honduras: Congreso Nacional aprobó los dos artículos más polémicos de las reformas penales**. Disponible en: http://www.elheraldo.hn/pais/1046584-466/honduras-congreso-nacional-aprob%C3%B3-los-dos-art%C3%ADculos-m%C3%A1s-pol%C3%A9micos-de-las-reformas

participe en un acto que sea para intimidar o causar terror al gobierno o población también es responsable del delito.

Además, el texto aprobado tipifica la apología e incitación a actos terroristas a quien públicamente o a través de medios de comunicación incite a otros a cometer el delito de terrorismo. Ambas reformas se pueden analizar desde la perspectiva de las movilizaciones sociales en contra de actos de corrupción, ya que en el contexto de quien convoque a manifestaciones ciudadanas o participe de estas, también puede ser objeto de proceso penal por ese delito. Lo cual vulnera los derechos de libertad de expresión, asociación y manifestación consagrados en la Constitución de Honduras, incluidas las personas defensoras de derechos humanos, quienes están desarrollando un papel muy importante para la defensa del territorio y de la democracia. Es alarmante que la criminalización de protestas ciudadanas y de la labor de defensoría sea validada a través de legislaciones que limitan libertades y derechos fundamentales.

En las reformas a la Ley Especial sobre Intervenciones de las Comunicaciones Privadas se determina la creación de la Unidad de Intervención de las Comunicaciones (UIC), a cargo, entre otras cosas, de realizar el procedimiento de obtención de detalle de llamadas entrantes y salientes de las personas en proceso de investigación, con orden de juez competente. Además, determina la obligación a los operadores de telefonía a garantizar sin limitaciones el acceso inmediato a la UIC toda la información relacionada a la intervención y extracción del contenido de las telecomunicaciones.

Honduras aún no ha iniciado el proceso de la elaboración de la Estrategia de Ciberseguridad[46]. Sin embargo, el Gobierno ha firmado un Acuerdo de Cooperación con el Gobierno de Israel para el fortalecimiento de la Dirección Nacional de Investigación e Inteligencia para la implementación de un CERT[47] en el país.

C.2. Ataque a defensoras y defensores de derechos humanos

Honduras presenta desde el 2009 un contexto de violencia sistemática en contra de defensoras y defensores de derechos humanos, como asegura en su informe el Grupo Asesor Internacional de Personas Expertas[48]. Incluso ha sido considerado por Global Witness[49] como el país más peligroso

46. El Heraldo. **Unas 16 instituciones serán protegidas de los cibercriminales en Honduras.** Disponible en: http://www.elheraldo.hn/pais/1115813-466/unas-16-instituciones-ser%C3%A1n-protegidas-de-los-cibercriminales-en-honduras

47. El Heraldo. **Israel dotará de unidades en contra del cibercrimen en Honduras.** Disponibe en: http://www.elheraldo.hn/pais/1115476-466/israel-dotar%C3%A1-de-unidades-en-contra-del-cibercrimen-en-honduras

48. Grupo Asesor Internacional de Personas Expertas (2017). **Represa de violencia: El plan que asesinó a Berta Cáceres.** Disponible en: https://www.cejil.org/sites/default/files/represa_de_violencia_es_final_.pdf Pág. 11.

49. Global Witness (2017). **Honduras: el lugar más peligroso para defender el planeta**. 48Disponible en: https://www.globalwitness.org/documents/18802/Spanish_single_v6.pdf

del mundo para defender el planeta, por el alto índice de persecución, detención y asesinatos de personas defensoras de los derechos al agua y medio ambiente.

Desde organizaciones que se dedican a la defensa de derechos humanos hasta medios de comunicación independientes, han sido objeto de vigilancia, acoso, amenazas, robo de dispositivos e información, persecución e incluso atentados en contra de su integridad física y vida.

Además, Michel Frost, Relator Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas en sus informes ha mostrado preocupación "por la falta de investigaciones independientes y diligentes sobre las agresiones cometidas contra los defensores de los derechos humanos ambientales, hecho que suele estar vinculado a la falta de recursos, la corrupción y la colusión entre los autores. Los Estados casi nunca han conseguido hacer comparecer ante la justicia a los autores y que estos fueran sancionados."[50] Especialmente en Guatemala y Honduras donde persiste la impunidad y las y los defensores de derechos humanos no confían en órganos jurisdiccionales al momento de solicitar reparaciones judiciales.

Según Global Witness tras el Golpe de Estado del 2009, más de 120 personas defensoras de la tierra y el medio ambiente han sido asesinados en Honduras[51], la mayoría de casos siguen en la impunidad por diferentes razones desde falta de voluntad política hasta corrupción del Gobierno, Ejército y empresas extractivistas. El Gobierno hondureño, a través de sus fuerzas de seguridad, ha institucionalizado prácticas de control y represión a todos niveles.

De la misma manera, Freedom House en su informe del 2017 sobre Libertad de Prensa cataloga a Honduras como un país no libre[52], la metodología del informe incluye parámetros como entornos legales, políticos y económicos en los que medios de comunicación, impresos, radiales y digitales ejercen su labor informativa y sin miedo a represalias frente actores privados, políticos e incluso del crimen organizado. Indicando además, que continúa siendo uno de los países más peligrosos en el mundo para que periodistas ejerciten su labor[53].

Amnistía Internacional en su informe anual[54] destacó que se ha acusado al Ejército de infiltrarse en movimientos sociales, además de atacar a defensores y defensoras de derechos humanos. En este sentido, la Ley de Protección para las y los Defensores de derechos humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia[55] sigue sin ser aplicada adecuadamente.

50. Relatoría Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas. **Informe sobre la situación de los defensores de los derechos humanos 2016.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement

51. *Ibíd.* Pág. 5.

52. Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon**. Disponible en: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf Pág. 24.

53. *Ibíd*. Pág. 21.

54. Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Págs. 225-226.

55. Congreso Nacional de Honduras. **Ley de Protección para las y los Defensores de derechos humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia.** Disponible en: http://www.tsc.gob.hn/leyes/Ley_Proteccion_defensores_der_humanos_periodistas_op_just.pdf

El Estado ha invertido casi 2 mil millones de lempiras (casi 85 millones de dólares americanos) en actividades de inteligencia y espionaje[56] a opositores del gobierno, bajo el escudo de combatir la delincuencia. Estas actividades de inteligencia se incluyen interceptaciones telefónicas, infecciones con *malware* y seguimiento de activistas y periodistas; es necesario destacar que la Dirección de Inteligencia utiliza estos mecanismos sin orden judicial previa.

Además, en el marco del proceso de la elección presidencial del 26 de noviembre 2017, estas prácticas de violencia política y represión de la protesta social se han extendido a toda la ciudadanía. En el que además se declaró Estado de Excepción[57], restringiendo garantías constitucionales, luego de la inconformidad de la población frente a los resultados de las votaciones y por un posible fraude electoral, lo que ha provocado hasta el momento protestas ciudadanas y excesivo uso de la fuerza por parte de las fuerzas de seguridad públicas; que incluso han dejado detenidos, heridos y muertos en todo el país[58].

C.3. PRINCIPALES HALLAZGOS EN HONDURAS

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Honduras. Los mismos han sido registrados entre los meses de junio y noviembre de 2017. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de incidentes digitales.

C.4. Casos registrados

Durante el transcurso del periodo antes mencionado, fueron registrados un total de ocho casos de incidentes de seguridad digital, todos en Tegucigalpa, Francisco Morazán.

C.5. Perfil de las personas/ organizaciones que reportaron incidentes

En los ocho casos, fueron integrantes y dirigentes estudiantiles universitarios del país quienes fueron objeto del delito de robo y, como consecuencia, su información personal y cuentas digitales fueron comprometidas.

58. ConfidencialHN. J**OH gastó casi dos mil millones para espiar a opositores.** Disponible en: http://confidencialhn.com/2017/08/28/joh-gasto-casi-dos-mil-millones-para-espiar-a-opositores/

57. Reuters. **Honduras suspende garantías constitucionales en medio de fuertas protestas tras elecciones.** Disponible en: https://lta.reuters.com/article/domesticNews/idLTAKBN1DV4UW-OUSLD

58. Amnistía Internacional. **Honduras: represión violenta después de elecciones.** Disponible en: https://www.amnesty.org/es/documents/amr37/7550/2017/es/

C.6. Tipos de ataques

A continuación una breve descripción (no técnica) de los ataques registrados.

Los ocho casos constituyeron la sustracción, robo o hurto de ocho teléfonos móviles a diferentes líderes del movimiento estudiantil hondureño, en diferentes momentos del año y contextos distintos, como una consecuencia inmediata de este acto, la información personal, cuentas y contraseñas de estas ocho personas fueron comprometidas.

Sin embargo, es importante destacar que en la actualidad y con el despliegue de los teléfonos inteligentes, las personas almacenan una gran cantidad de información, en algunos casos hasta datos sensibles, que van desde contactos hasta fotografías, pasando por toda clase de documentos y conversaciones personales. En este sentido, el compromiso de contraseñas y cuentas de correo electrónico, redes sociales y mensajerías instantáneas es una de las mayores preocupaciones.

C.7. Posibles perpetradores

En algunos de los robos de teléfonos móviles los perpetradores de estos incidentes de seguridad digital fueron integrantes de la Policía Nacional de Honduras, en los otros casos fueron por asalto, por lo que no se pudo identificar al perpetrador.

C.8. Mecanismos de Protección

En este apartado se presentan los marcos jurídicos que pudieron haber sido vulnerados en los casos que se han registrado en el capítulo de Honduras del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos.

C.9. Posibles derechos humanos vulnerados

Constitucionalmente el derecho a la propiedad privada se encuentra reconocido, en los ocho casos el objeto del delito fueron teléfonos celulares que comprenden bienes tangibles de las personas. Como una consecuencia directa de este hecho, la intimidad y privacidad de las comunicaciones también fueron vulneradas.

C.10. Posibles tipificaciones penales

En los casos registrados, la acción de sustracción de la propiedad privada, en este caso de los teléfonos celulares, puede tipificarse, según el caso y las circunstancias especiales, dentro de los delitos de robo o hurto regulados en el Código Penal, en los artículos 217 y 223, respectivamente.

C.11. Estrategias legales de respuesta

Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

Denuncias

En los casos registrados en Honduras, corresponde como primer paso interponer una denuncia ante el Ministerio Público, para que realice una investigación sobre los delitos cometidos a las y los estudiantes defensores y defensoras de derechos.

Por otro parte, Honduras también posee un Mecanismo Nacional de Protección a Defensores/as de derechos humanos, que tiene la obligación de investigar los hechos y de proteger la integridad de las personas defensoras, así como de evitar que, de alguna manera, se les obstaculice realizar de manera segura su labor como defensoras. Sin embargo, este mecanismo únicamente contempla medidas de protección física, parcialmente psicológica y legal, pero no contempla protección relacionada a la seguridad digital de sus beneficiarios.

C.12. Conclusiones y Recomendaciones

Conclusiones

1. Si bien Honduras cuenta con un Sistema Nacional de Protección para personas Defensoras de Derechos Humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia, ésta no ha madurado aún, habiendo muchas deficiencias en respuesta eficaz y eficiente. Honduras ha sido catalogado como uno de los países más peligrosos para ejercer esta labor. De la misma manera, persiste la ausencia de marcos jurídicos adecuados para la protección de la privacidad digital, los cuales fueron identificados en su momento en la investigación realizada por Fundación Acceso en el 2015.

2. El Gobierno hondureño ha invertido millones de lempiras para la implementación de su sistema de inteligencia, sin incluir en los mecanismos de control y vigilancia estándares internacionales en materia de derechos humanos

3. La amenaza que sufren directamente las personas defensoras de derechos humanos y periodistas independientes en el país va desde la física hasta la digital, en este sentido el peligro al que son sujetos en su labor diaria incluye, entre otras cosas, el peligro en su integridad física e incluso la vida, como la información que generan alrededor de su trabajo y lucha cotidiana.

4.El tema de seguridad digital continúa estando ausente de los informes que tratan sobre la seguridad de las y los defensores de derechos humanos, provocando áreas de vulnerabilidad a través de las cuales estos/as pueden ser atacadas/os.

Recomendaciones

1. La reforma al marco jurídico es necesaria para mejorar los mecanismos y niveles de protección a defensoras y defensores de derechos humanos, enfatizando en la necesidad de incluir herramientas de seguridad digital, e incluyendo estándares internacionales en materia de Internet y Derechos Humanos.

2. La ciudadanía debe exigir transparencia y rendición de cuentas sobre las diferentes herramientas de inteligencia y vigilancia, así como la regulación para que éstas sean utilizadas en el contexto de la necesidad, legalidad y proporcionalidad.

3. Los colectivos y organizaciones de derechos humanos deben generar mecanismos y protocolos internos enfocados a la seguridad digital, lo cual se puede lograr a través de la generación de capacidades en este tema dentro de las propias organizaciones y colectivos.

4. Dentro de los informes sobre la situación de las y los defensores de derechos humanos es importante incluir secciones dedicadas a la seguridad digital, para visibilizar la importancia de esta en materia de protección integral.

5. Una mesa nacional de análisis sobre Internet y Derechos Humanos convocada desde las organizaciones locales con la participación de comunidades académicas y técnicas, sería una estrategia importante de impulsar. Las tendencias globales en materia de regulación de la Internet, sacrificando el derecho a la privacidad, rápidamente están teniendo eco en los congresos de nuestros países centroamericanos.


El Salvador

D. CAPÍTULO EL SALVADOR

D.1. Contexto Legal: Internet y Derechos Humanos en El Salvador

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[59], en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[60], sin embargo, la legislación penal existente en relación a la protección del derecho a la privacidad digital aún no se encuentra regulada.

Sin embargo, El Salvador desde el 2016 posee una Ley Especial contra los Delitos Informáticos y Conexos[61], Decreto Número 260. La cual posee un catálogo de delitos, incluidos los de espionaje informático, hurto de identidad y utilización de datos personales, los cuales de una u otra manera protegen la privacidad digital.

Actualmente el Ministerio de Justicia y Seguridad Pública desarrolla una estrategia nacional de seguridad cibernética, sin embargo, aún no ha divulgado la propuesta preliminar completa. El país ya posee CSIRT y CERT[62], para responder a ataques cibernéticos y coordinar estrategias regionales.

En El Salvador aún no existen espacios multisectoriales para el diálogo alrededor de Internet y Derechos Humanos, como consecuencia los niveles de discusión pública alrededor de la protección del derecho a la privacidad en línea de todas las personas, especialmente de las y los defensores de derechos humanos, son muy escasos.

Esto les coloca en una situación de especial vulnerabilidad pues ante esos vacíos normativos y de políticas públicas es más probable que este tipo de ataques y sus perpetradores, ya sean empresas o agentes del propio gobierno, queden en la impunidad.

59. Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

60. *Ibíd.* Pág 75.

61. Asamblea Legislativa de El Salvador. **Ley Especial contra los Delitos Informáticos y Conexos**. Disponible en: https://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-los-delitos-informaticos-y-conexos

62. Banco Interamericano de Desarrollo y Organización de Estados Americanos (2016). **Ciberseguridad: ¿Estamos preparados en América Latina y El Caribe?** Disponible en: https://publications.iadb.org/handle/11319/7449?locale-attribute=es& Pág. 72.

D.2. Ataques a defensoras y defensores de Derechos Humanos

Freedom House en su informe del 2017 sobre Libertad de Prensa cataloga a El Salvador como un país parcialmente libre[63], la metodología del informe incluye parámetros como entornos legales, políticos y económicos en los que medios de comunicación, impresos, radiales y digitales ejercen su labor informativa y sin miedo a represalias frente actores privados, políticos e incluso del crimen organizado. A pesar que El Salvador tradicionalmente ha sido un país en el que la violencia contra periodistas posee una tasa baja, la intimidación contra medios de comunicación ha incrementado[64].

Durante el 2017, la Revista Factum fue objetivo de vigilancia e intimidación luego de publicar una investigación periodística relacionada con escuadrones de la muerte en una de las unidades élites de la policía nacional. Este tipo de ataques también fueron denunciados en el 2015 por El Faro en circunstancias similares (luego de una publicación sobre la policía nacional).[65]

> Amnistía Internacional, en su informe anual[66] apuntó el caso de una defensora a la que una empresa le presentó proceso penal por calumnia y difamación, esto derivado de las declaraciones que ella realizó sobre el impacto y deterioro en el medio ambiente del proyecto de esta empresa. Fue absuelta de todos los cargos, sin embargo, la empresa presentó un recurso procesal a la sentencia.

Por otra parte las personas defensoras de derechos humanos, activistas y medios de comunicación independiente han sido objeto de amenazas, estigmatización, intimidación, agresión, en algunos casos los involucrados han sido funcionarios del gobierno.

Front Line Defenders también menciona en su reciente informe de 2017, que se han registrado múltiples ataques a personas defensoras en El Salvador, particularmente hacia mujeres defensoras y personas defensoras de la población LGTTBI.

D.3. Principales hallazgos en El Salvador

Durante el transcurso del 2017, desde Fundación Acceso no se registraron casos de incidentes de seguridad digital entre defensoras y defensores de derechos humanos en El Salvador. Únicamente se tuvieron 2 contactos iniciales con el técnico encargado del país, sin embargo, al momento de realizar contacto para conocer más detalles sobre el posible incidente de seguridad digital, no se logró obtener comunicación con las personas defensoras.

63. Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon**. Disponible en: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf Pág. 24.

64. *Ibíd.* Pág. 21.

65. Revista Factum (2017). **Exterminio: El Estado cómplice.** Disponible en: http://revistafactum.com/exterminio-el-estado-complice/

66. Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de Derechos Humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Pág. 173.

J4A1dbQioxwxvU

Nicaragua

aOv9VxK/Eb

gghOAGr2Ov9V

HlqVR

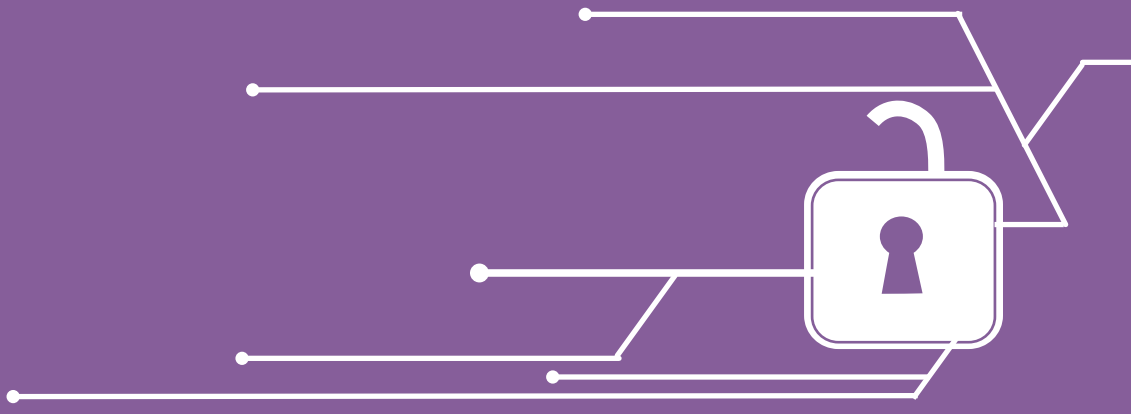
j86Z/sI

XlyjpbQioxwxvU1je

RXlyjpbQioxwxvU1jeZpj86Z/sI

HlqVRomqgghOAGr2Ov9V

j86Z/sIDhll vy5



E. NICARAGUA

E.1. Contexto Legal: Internet y Derechos Humanos en Nicaragua

En el 2015, Fundación Acceso elaboró una investigación sobre "¿Privacidad digital para defensores y defensoras de derechos humanos?"[67] , en la cual se abordaron los marcos legales aplicables para el derecho a la privacidad en la región centroamericana. En esa investigación se establecieron algunos parámetros aplicables al contexto nacional que aún continúan vigentes casi en las mismas condiciones en las que se planteó en el estudio.

En términos generales se estableció que existe un reconocimiento constitucional a nivel general sobre el derecho a la privacidad[68], sin embargo, la legislación penal existente en relación a la protección del derecho a la privacidad digital aún no se encuentra regulada.

Es importante destacar lo regulado en la Ley de Seguridad Soberana de la República de Nicaragua, Ley No. 919 del 2 de diciembre de 2015. En el artículo 8, se determina que los ataques a la seguridad cibernética, principalmente aquellos que afecten los sistemas de comunicación nacional, son considerados como amenazas a la seguridad soberana. Sin embargo, la Ley no hace una determinación clara de lo que considera como "ataque cibernético", lo cual puede llegar a ser claramente perjudicial porque el marco normativo es muy amplio y ambiguo.

En el artículo 13 prohíbe a las entidades públicas que forman parte del Sistema Nacional de Seguridad lo siguiente: realizar espionaje político, obtener o almacenar información o datos sensibles de organizaciones sociales, asimismo la interceptación e intervención de comunicaciones si orden de juez competente. Esto último, refleja, al menos en el texto legal, que los mecanismos de vigilancia masiva deben cumplir con algunos de los principios y estándares internacionales, como la legalidad, autoridad judicial competente y debido proceso.

El 14 de noviembre de 2017 se llevó a cabo en Nicaragua el I Foro sobre Gobernanza de Internet y Seguridad Informática[69], en el cual desde una óptica multisectorial se discutieron temas relacionados con la privacidad digital, aunque de una manera muy general, sin incluir consideraciones respecto a la protección de las y los defensores de derechos humanos.

Sin embargo, la falta de otros espacios reflejan que cada vez se hace más necesario promover diálogos alrededor de la protección de los derechos humanos en línea y que la población exija

67. Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

68. *Ibíd.* Pág 260.

69. Internet Society capítulo Nicaragua. http://isoc.org.ni/

reconocimiento y respeto de estos, así como la inclusión en estas conversaciones de la protección de las y los defensores de derechos humanos.

Esto les coloca en una situación de especial vulnerabilidad pues ante esos vacíos normativos es más probable que este tipo de ataques y sus perpetradores, ya sean empresas o agentes del propio gobierno, queden en la impunidad.

E.2. Ataques a defensoras y defensores de Derechos Humanos

El 10 de enero del 2017, Daniel Ortega tomó posesión del cargo de Presidente por tercera vez, su esposa Rosario Murillo fue electa como Vicepresidenta. La concentración del poder ha impactado en diferentes ámbitos de la institucionalidad en Nicaragua, desde la destitución arbitraria de diferentes funcionarios/as públicos/as opositores[70] hasta la limitación de diferentes derechos fundamentales.

En Nicaragua las defensoras y defensores de derechos humanos continúan siendo objeto de intimidación y amenazas por sus actividades en Nicaragua. Según el informe anual de Amnistía Internacional[71] principalmente las comunidades indígenas y afrodescendientes han denunciado diferentes violaciones a sus derechos fundamentales, específicamente en el contexto de la construcción del proyecto multimillonario del Canal Interoceánico; el cual fue aprobado bajo una serie de irregularidades. Varias comunidades y organizaciones de derechos humanos expresaron preocupación ante el posible impacto negativo del canal sobre sus vidas. Las implicaciones negativas del Canal Interoceánico sobre los derechos humanos, han sido recogidas en el informe de la FIDH y CENIDH[72], en el que claramente relatan la criminalización de la protesta social, hostigamiento a la población y militarización de las comunidades sobre la ruta del Canal.

En el informe anual 2016 del CENIDH[73] sobre la situación de los DDHH en Nicaragua, incluye un apartado sobre la situación particular de las personas defensoras. En este tema indican que: *"La mayoría de los casos de agresiones, amenazas, estigmatización y judicialización hacia defensores y defensoras han partido de divulgación de información que denigra y difama en sitios virtuales y diversas redes sociales donde se publican no sólo fotografías y datos personales, sino también datos familiares, dirección de las casas de habitación, exponiéndoles frente a los sujetos y/o presuntos agresores, lo que pone en alto riesgo su seguridad, además, de las constantes amenazas tanto a ellas como a sus hijos e hijas."*

70. CEJIL (2017). Nicaragua: ¿cómo se reformó la institucionalidad para concentrar el poder? Disponible en: https://www.cejil.org/sites/default/files/informe_cejil_sobre_nicaragua_-_derechos_politicos.pdf Pág. 22.

71. Amnistía Internacional (2017). **Informe annual 2016/2017: La situación de Derechos Humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ Pág. 328.

72. FIDH (2016) – **Concesión del Canal Interoceánico en Nicaragua: Grave Impacto en los derechos humanos**. Disponible en: https://www.cenidh.org/media/documents/docfile/informe_nicaragua_canal_esp1.pdf

73. CENIDH (2016). **Derechos Humanos en Nicaragua 2016.** Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_Cenidh_2016_Final2017.pdf

Front Line Defenders también menciona en su reciente informe de 2017, que se han registrado múltiples ataques a personas defensoras en Nicaragua, particularmente hacia mujeres defensoras. La Iniciativa Nicaragüense de Defensoras de Derechos Humanos ha registrado en dos años 389 agresiones ocurridas (entre 2015 y 2017) en contra de 202 defensoras. Un 45 por ciento de los agresores señalados son autoridades estatales destacándose la Policía[74].

E.3. Principales hallazgos en Nicaragua

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de Nicaragua. Los mismos han sido registrados entre los meses de junio y noviembre de 2017. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de incidentes digitales.

E.4. Casos registrados

Durante el transcurso del período antes mencionado, fueron registrados un total de **once** casos e incidentes de seguridad con diferentes componentes y móviles, en León, Managua, Matagalpa y Bilwi. Entre ellos, se detectaron 5 como incidentes positivos y 6 incidentes como falsos positivos. En este apartado sólo abordaremos los incidentes positivos.

E.5. Perfil de las personas/ organizaciones que reportaron incidentes

En el primer caso, fue una organización que se dedica a la investigación del contexto político y económico en el país. El segundo caso, fue una organización dedicada a la promoción de derechos sociales y culturales, enfocados principalmente en el derecho a la salud y su relación con otros ejes. En el tercer caso, fue a un colectivo que se dedica a exigir el respeto de los derechos de las mujeres en Nicaragua. En el cuarto caso, fue dirigido contra una integrante de un colectivo de defensa de los derechos de la comunidad LGTBI, y en el quinto caso, se solicitó que fuera anónimo, como consecuencia no se puede realizar un perfil general de la persona u organización.

E.6. Tipos de ataques

A continuación una breve descripción (no técnica) de los ataques registrados. En un principio, se describirán los incidentes positivos y posteriormente los falsos positivos registrados.

En el primer incidente, contra la organización que se dedica a la investigación del contexto político y económico, se denunció ante Fundación Acceso la filtración de correos electrónicos en un sitio web. Desde inicios del 2017, este sitio web se ha dedicado a realizar publicaciones de carácter

74. IM-Defensoras (2017). Audiencia 164 de la CIDH. Disponible en: https://www.youtube.com/watch?v=c4Pr6A3Yiq8

difamatorio contra algunas organizaciones del país, principalmente se dedica filtrar extractos de correos electrónicos de diferentes organizaciones. Por una parte se cree que esa información fue sustraída de un disco duro robado a este organización años atrás, aunque por la publicación de correos de años más recientes también se maneja la teoría que dentro de la misma organización se están filtrando los mismos.

El segundo incidente, a la organización dedicada a la promoción del derecho a la salud, también se relaciona con el caso anterior, ya que se han publicado correos electrónicos de integrantes de la misma en el referido sitio web.

En el mismo contexto, el incidente registrado contra el colectivo de los derechos de las mujeres, también ha sido víctima de la difamación y filtración de correos electrónicos.

El cuarto incidente, dirigido contra una integrante de un colectivo de defensa de los derechos de la comunidad LGTTBI, consiste en un acoso sistemático de la expareja, en el cual esta persona tuvo acceso de manera remota a su teléfono móvil con la finalidad de acosarla y vigilarla. En este caso, además del acceso remoto se registró el envío de mensajes con amenazas y obscenidades. Como consecuencia inmediata al acceso remoto del dispositivo, la información personal, cuentas y contraseñas han sido comprometidas.

El quinto incidente, se refiere al robo de un dispositivo y como consecuencia inmediata el compromiso de la información, cuentas y contraseñas de esta persona u organización.

E.7. Posibles perpetradores

La identificación de los posibles perpetradores de los ataques es una tarea que interesa al Observatorio de Seguridad Digital, pero se debe informar que no siempre se logra, principalmente en el contexto de la delincuencia común que se ha normalizado en los países de la región centroamericana. En tal sentido, esta tarea requiere, para los casos más complejos, recursos técnicos y acceso a servicios que están fuera del alcance de la organización.

Únicamente en el caso del cuarto incidente se logró determinar que el posible perpetrador fue la expareja de la persona defensora de los derechos de la comunidad LGTBI, con la finalidad de ejercer control y violencia de género sobre esta persona.

E.8. Mecanismos de protección

En este apartado se presentan los marcos jurídicos que pudieron haber sido vulnerados en los casos que se han registrado en el capítulo de Nicaragua del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos

permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos.

E.9. Posibles Derechos Humanos vulnerados

Dentro de la Constitución de la República de Nicaragua se contempla y regula el derecho a la privacidad, en el que se establece la inviolabilidad de correspondencia, documentos y libros, en cualquier formato, salvo orden previa de juez competente. El denominador común en los incidentes positivos registrados fue la vulneración del derecho constitucional a la privacidad digital, comprendiendo la información personal, cuentas, contenido de correos electrónicos y contraseñas comprometidas.

Además se violentó el derecho a la propiedad privada ya que en uno de los casos el objeto del delito fueron dispositivos digitales, que comprenden bienes tangibles de las personas.

E.10. Posibles tipificaciones penales

A partir de la investigación realizada en 2015 por Fundación Acceso se puede establecer que el marco jurídico penal continúa siendo insuficiente para establecer mecanismos integrales de protección del derecho a la privacidad digital de las y los defensores de derechos humanos en el país.

Más allá de los casos en los que existió sustracción, robo o hurto de dispositivos que contenían la información de las personas u organizaciones. El robo y hurto, regulados en los artículos 219, 220, 223, 224 y 225 del Código Penal de Nicaragua.

Por otra parte, en el caso de acoso y amenazas por parte de la expareja, los delitos cometidos fueron violencia psicológica e intimidación o amenaza contra la mujer, regulados en los artículos 11 y 13 de la Ley Integral contra la Violencia hacia las Mujeres.

E.11. Estrategias legales de respuesta

Estos son algunos de los mecanismos legales que se podrían implementar con motivo de los incidentes registrados por el Observatorio:

Denuncias

En los casos registrados en Nicaragua, corresponde denunciar ante el Ministerio Público para que realice la investigación de los delitos cometidos en contra de las personas defensoras de derechos humanos.

Acciones constitucionales

La acción constitucional de Amparo también es utilizado como un mecanismo legal para exigir la protección de derechos garantizados en la Constitución y, siendo la privacidad de las comunicaciones un derecho constitucional, se podría intentar un amparo para salvaguardar este y otros derechos.

La acción de Amparo en Nicaragua se presenta ante la Sala de lo Constitucional de la Corte Suprema de Justicia, es un proceso que exige el patrocinio de un abogado, de preferencia experto en la materia, lo cual en algunas ocasiones impide que las y los defensores de derechos humanos, y la población en general, tengan acceso a la justicia constitucional.

Otras acciones

Nicaragua regula la figura del ombdusman, determinada como el Procurador para la Defensa de Derechos Humanos, ante el cual se puede interponer una denuncia en materia de violación de libertades y derechos fundamentales, en su rol de velar por el efectivo cumplimiento de estos. Sin embargo, el carácter de la sanción es de índole moral, porque está diseñado para desempeñar un rol de tribunal de conciencia; aunque tiene la capacidad legal de presentar denuncias ante los órganos jurisdiccionales competentes.

Sistema Interamericano de Derechos Humanos

En relación al Sistema Interamericano de Derechos Humanos, posee ciertos requisitos previos a que los casos sean llevados a estas instancias regionales. Sin embargo, en situaciones de gravedad y urgencia pueden solicitarse medidas cautelares ante la Comisión Interamericana de Derechos Humanos para que el Estado adopte medidas para prevenir daños irreparables a las personas o al objeto del proceso en conexión con una petición o caso pendiente.

Además, es un buen espacio que permite documentar estos y otros casos para identificar patrones de actuación de parte de organizaciones y oficinas gubernamentales que puedan estar vigilando a defensores y defensoras de derechos humanos. Esta información ponerla de conocimiento de las respectivas Relatorías para que pueda ser incluida en sus informes periódicos, con la finalidad de visibilizar la situación de la seguridad digital a nivel regional.

E.12. Conclusiones y Recomendaciones

Conclusiones

1. Nicaragua carece de mecanismos de protección física y digital, para las y los defensores de derechos humanos. De la misma manera, persiste la ausencia de marcos jurídicos adecuados para la protección de la privacidad digital, los cuales fueron identificados en su momento en la investigación realizada por Fundación Acceso en el 2015.

2. La amenaza que sufren directamente las personas defensoras de derechos humanos y periodistas independientes en el país va desde la física hasta la digital, en este sentido el peligro al que son sujetos en su labor diaria incluye, entre otras cosas, el peligro en su integridad física e incluso la vida, como la información que generan alrededor de sus temáticas de trabajo.

3. El tema de seguridad digital continúa estando ausente de los informes que tratan sobre la seguridad de las y los defensores de derechos humanos, provocando áreas de vulnerabilidad a través de las cuales estos/as pueden ser atacadas/os.

Recomendaciones

1. La reforma al marco jurídico es necesaria para mejorar los mecanismos y niveles de protección a defensoras y defensores de Derechos Humanos, enfatizando la necesidad incluir herramientas de seguridad digital, incluyendo estándares internacionales en materia de Internet y Derechos Humanos.

2. Los colectivos y organizaciones que se dedican a la defensa de derechos humanos deben generar mecanismos y protocolos internos enfocados a la seguridad digital, lo cual se puede lograr a través de la generación de capacidades en este tema dentro sus propias organizaciones.

3. Dentro de los informes sobre el panorama de las actividades de las y los defensores de derechos humanos deben incluir secciones dedicadas a la seguridad digital, para visibilizar la importancia de esta en la seguridad integral.

F. Bibliografía

•Alliance for Affordable Internet. **Coalición Guatemalteca para una Internet Asequible.** Disponible en: http://a4ai.org/guatemala/

•Amnistía Internacional (2017). I**nforme annual 2016/2017: La situación de derechos humanos en el Mundo.** Disponible en: https://www.amnesty.org/es/documents/pol10/4800/2017/es/

•Asociación de Derechos Civiles (2015). **Educar para vigilar: Una investigación acerca de la formación institucional estatal en vigilancia e investigación en el entorno digital**. Disponible en: https://adcdigital.org.ar/wp-content/uploads/2016/01/Educar-para-vigilar.pdf

•Banco Interamericano de Desarrollo y Organización de Estados Americanos (2016). **Ciberseguridad: ¿Estamos preparados en América Latina y El Caribe?** Disponible en: https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

•CELE-UP (2012). **Hacia una Internet libre de censura: propuestas para América Latina**. Disponible en: http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

•CELE-UP (2014). **Internet y derechos humanos: aportes para la discusión en América Latina.** Disponible en: http://www.palermo.edu/cele/pdf/InternetyDDHH.pdf

•CENIDH (2016). **Derechos Humanos en Nicaragua 2016.** Disponible en: https://www.cenidh.org/media/documents/docfile/Informe_Cenidh_2016_Final2017.pdf

Congreso de la Repúbica de Guatemala. **Iniciativa 4090, Ley de Protección de Datos Personales**. Disponible en: http://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf

•Congreso de la República de Guatemala. **Iniciativa 5230.** Disponible en: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=2636

•Congreso de la República de Guatemala. **Iniciativa 5239, Ley contra Actos Terroristas**. Disponible en: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=3607

•Congreso de la República de Guatemala. **Iniciativa 5254, Ley contra la Ciberdelincuencia**. Disponible en: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf

•Consejo de derechos humanos - ONU (2014). **El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los derechos humanos.** Disponible en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjYmJj-8M3MAhXEHR4KHVVcCQYQFggdMAA&url=http%3A%2F%2Fwww.ohchr.org%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession27%2FDocuments%2FA-HRC-27-37_sp.doc&usg=AFQjCNGT_BPxxWGqFMXjIlOkF80ao6-TkA

•Comisión Interamericana de derechos humanos (2006). **Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas.** Disponible en: https://www.cidh.oas.org/countryrep/Defensores/defensoresindice.htm

•Comisión Interamericana de derechos humanos (2013). **Informe Libertad de Expresión e Internet.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

•Comisión Interamericana de derechos humanos (2015). **Informe Situación de los derechos humanos en Guatemala: Diversidad, desigualdad y exclusión.** Disponible en: https://www.oas.org/es/cidh/informes/pdfs/Guatemala2016.pdf

•Comisión Interamericana de derechos humanos (2016). **Informe Criminalización de defensoras y defensores de derechos humanos.** Disponible en: https://www.oas.org/es/cidh/informes/pdfs/criminalizacion2016.pdf

•Comisión Interamericana de derechos humanos (2017). **Informe Estándares para una Internet Libre, Abierta e Incluyente.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

•Comision Interamericana de derechos humanos (2017). **Informe de la Relatoría para la Libertad de Expresión.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/informes/anuales/InformeAnual2016RELE.pdf

•Comisión Interamericana de derechos humanos (2017). **Informe Zonas Silenciadas: regiones de alta peligrosidad para ejercer la libertad de expresión.** Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ZONAS_SILENCIADAS_ESP.pdf

•Derechos Digitales (2016). **Hacking Team Malware para la vigilancia en América Latina**. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

•Electronic Frontier Foundation (2014). **Necesarios y Proporcionados: Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.** Disponible en: https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

•Electronic Frontier Foundation y Derechos Digitales (2016). **Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones y el Sistema Interamericano de Protección de derechos humanos.** Disponible en: https://necessaryandproportionate.org/files/2016/08/23/iachr-sp-agosto2016.pdf

•Electronic Frontier Foundation (2016). **Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica**. Disponible en: https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016_es_0.pdf

•Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon.** Disponible en: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf Pág. 24.

•Front Line Defenders (2015). I**nforme Anual 2015: Defensores (as) de derechos humanos en la cuerda floja.** Disponible en: http://www.coljuristas.org/documentos/adicionales/defensores_de_ddhh_en_la_cuerda_floja.pdf

•Front Line Defenders. **Annual Report Human Rights Defenders at risk in 2017.** Disponible en: https://www.frontlinedefenders.org/en/resource-publication/annual-report-human-rights-defenders-risk-2017

•Foro de Gobernanza de Internet de Guatemala. http://igf.gt/

•Fundación Acceso (2015). **¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos.** Disponible en: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

•Medium.com. **Los Netcenters: Negocio de Manipulación.** https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc

•Ministerio de Gobernación. **Presentan conclusiones para mejorar Borrador de la Estrategia Nacional de Ciberseguridad.** Disponible en: http://mingob.gob.gt/presentan-conclusiones-para-mejorar-el-borrador-de-la-estrategia-nacional-de-ciberseguridad/

•Motherboard. **El imperio 'ilegal' de Hacking Team en América Latina.** Disponible en: https://motherboard.vice.com/es/article/wngqmx/el-imperio-ilegal-de-hacking-team-en-america-latina-5886b78158d4ae45b7112d84

•Nación Digital. https://www.naciondigital.gob.gt/

•Nómada. **#JimmySeQueda: el netcenter de @rodrigopolo, @rmendezruiz y @pirulismo**. Disponible en: https://nomada.gt/asi-se-fabrico-el-jimmysequeda-el-netcenter-de-rodrigopolo-rmendezruiz-y-pirulismo/

•Organización de Estados Americanos. **Convención Americana de derechos humanos**. Disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

•Organización de Naciones Unidas. **Declaración Universal de derechos humanos.** Disponible en: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

•Organización de Naciones Unidas. **Pacto Internacional de Derechos Civiles y Políticos**. Disponible en: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

•Organización de Naciones Unidas (1999). **Resolución 53/144 del 8 de marzo de 1999**. Disponible en: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

•Prensa Libre. **Una peligrosa propuesta de ley.** Disponible en: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley

•Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas (2016). **Informe anual.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/51/PDF/G1707751.pdf?OpenElement

•Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas (2017). **Informe anual.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/51/PDF/G1707751.pdf?OpenElement

•Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas (2017). **Informe.** Disponible en: http://www.un.org/ga/search/view_doc.asp?symbol=A/72/350

•Relatoría Especial sobre la situación de los defensores de los derechos humanos de las Naciones Unidas. **Informe sobre la Situación de los defensores de los derechos humanos 2016.** Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement

•Revista Factum. Exterminio: **El Estado cómplice.** Disponible en: http://revistafactum.com/exterminio-el-estado-complice/

•Soy502. **El Ejército quiere encargarse de las amenazas cibernéticas.** Disponible en: http://www.soy502.com/articulo/ejercito-quiere-encargarse-amenazas-ciberneticas-63338?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#link_time=1511180394

•Soy502. **Los netcenteros de la impunidad.** Disponible en: http://www.soy502.com/articulo/netcenteros-impunidad-20878

•Soy502. **Periodistas exigen que el MP investigue a los "net centers".** Disponible en: http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-ciberneticos-149

•Udefegua. **Situación de Defensoras y Defensores de derechos humanos en Guatemala Un Reflejo del Deterioro de los derechos humanos en el País.** Disponible en: http://udefegua.org/wp-content/uploads/2017/10/201709-Sit-Defensores-DH-SEMESTRAL.FIN_.pdf

•Web We Want. **Carta de Derechos de Internet en Guatemala.** Disponible en: https://webwewant.org/es/guatemala/

HlqVRomqggh
j86Z/sIDhll vy5

j86Z/sIDhll vy5WvrrskJ

FUNDACIÓN Acceso