

# ESTUDIO DE IMPACTOS Y AFRONTAMIENTOS PSICOSOCIALES ANTE ATAQUES DIGITALES (ESPECÍFICAMENTE TECNOLOGÍAS ESPÍA O DE VIGILANCIA O SPYWARE EN INGLÉS)



Autora

Olga Paz, con contribuciones significativas de Gabriela Vargas, Dennise Albornoz y Jacobo Mogollón Villar

Coordinación de la investigación

Fundación Acceso

Idea original y diseño metodológico

Fundación Acceso

Supervisión técnica y revisión del informe

Fundación Acceso, The Engine Room

Organización responsable de la publicación

Fundación Acceso

Agradecemos especialmente a todas las personas entrevistadas por compartir sus experiencias, reflexiones y tiempo, lo cual hizo posible la construcción colectiva de este estudio

Fecha de publicación

Abril, 2025

Licencia

CC BY-NC 4.0. Atribución/Reconocimiento-NoComercial  
4.0 Internacional

Versión accesible de este documento en:  
[pasalavoz.acceso.or.cr/Estudio\\_de\\_impactos/](https://pasalavoz.acceso.or.cr/Estudio_de_impactos/)



Landing Page



# Contenido

<b>Introducción</b> .....	<b>03</b>
<b>Efectos psicosociales del software espía</b> .....	<b>11</b>
<b>Metodología</b> .....	<b>13</b>
<b>Resultados de la investigación</b> .....	<b>14</b>
<b>Características de los ataques de software espía</b> .....	<b>14</b>
a) El uso de software espía busca el control social y la censura .....	14
b) El software espía como herramienta de vigilancia estatal .....	16
c) La interrelación entre el software espía con violencia física o digital .....	18
<b>a. Impactos psicológicos</b> .....	<b>20</b>
1. Pánico .....	20
2. Normalización de la violencia .....	21
3. Hipervigilancia .....	22
5. Ansiedad .....	24
7. Depresión .....	25
8. Miedo .....	26
<b>b. Impactos psicosociales</b> .....	<b>28</b>
1. Aislamiento social .....	28
2. Proyecto de vida .....	29
3. En el ámbito familiar .....	31
4. Impacto con base en el género .....	33
5. En cuanto al equipo de trabajo y el entorno laboral .....	34
<b>Afrontamientos</b> .....	<b>38</b>
1. Cambios de hábitos y rutina .....	39
2. Reubicación .....	40
3. Autocuidado .....	41
5. Asesoría técnica .....	42
6. Red de apoyo .....	43
7. Apoyo interinstitucional .....	45
<b>Conclusiones</b> .....	<b>46</b>
<b>Recomendaciones</b> .....	<b>49</b>

# Introducción

En el contexto latinoamericano, la vigilancia dirigida a personas defensoras de derechos humanos, operadoras de justicia y periodistas, ha sido una práctica histórica y sistémica. El informe “Vigilancia en Centroamérica: Internet, privacidad y derechos humanos” de la Fundación Acceso,<sup>1</sup> define la vigilancia en internet como el monitoreo, la recopilación y el análisis de datos en línea, realizados tanto por actores estatales como privados. Este paradigma de vigilancia abarca el seguimiento de actividades en redes sociales, el rastreo de comunicaciones electrónicas y el acceso a información personal, frecuentemente, sin el consentimiento explícito o, incluso, sin el conocimiento de las personas afectadas.

En la actualidad, las operaciones de espionaje han sido reconfiguradas y orientadas hacia la identificación y neutralización de actores sociales etiquetados como “enemigos internos”, perpetuando así una lógica contrainsurgente de persecución que, en la segunda mitad del siglo XX, se dirigía contra sectores considerados como amenaza para el statu quo. Durante ese período, regímenes autoritarios en América Latina catalogaban como opositores a una amplia gama de actores: desde organizaciones insurgentes nacidas al calor de las dictaduras hasta movimientos sociales, religiosos, prodemocráticos o antimilitaristas, incluyendo a personas defensoras de derechos humanos.

En el siglo XXI, las estructuras estatales que históricamente aplicaron mecanismos de vigilancia y represión han demostrado una alta capacidad de adaptación al entorno digital. Hoy emplean tecnologías avanzadas para infiltrar dispositivos electrónicos, acceder a información confidencial y ejercer presión o intimidación sobre personas y colectivos considerados como amenazas al poder establecido, ya sea institucional o vinculado al crimen organizado. La persistencia de estas prácticas revela que, más allá de la transformación de las herramientas, se mantiene una visión estructural que interpreta la defensa de los derechos humanos como una forma de oposición política. Esta perspectiva es sostenida por

---

<sup>1</sup> Fundación Acceso. (2020). Vigilancia en Centroamérica. [www.acceso.or.cr/wp-content/uploads/2021/08/2020-VigilanciaCA-28S.pdf](http://www.acceso.or.cr/wp-content/uploads/2021/08/2020-VigilanciaCA-28S.pdf)

discursos oficiales que presentan estas acciones como necesarias para “combatir la criminalidad” y preservar la “seguridad nacional.”.

No obstante, la realidad evidencia que las tecnologías de espionaje, en particular el Spyware, han sido utilizadas, principalmente, para perseguir a personas defensoras de derechos, vigilar a opositoras políticas y hostigar a periodistas y activistas.<sup>2</sup> En contextos donde no existen salvaguardas legales adecuadas, el software espía se convierte en un mecanismo de represión que permite a los gobiernos mantener el control sobre organizaciones o personas específicas. Esta práctica coloca a quienes son objeto de espionaje en una situación de vulnerabilidad extrema, expone sus redes de contacto, sus fuentes de información y sus estrategias de trabajo a sectores interesados en desarticular sus esfuerzos y silenciar sus voces.

La facilidad para acceder a datos sensibles, la amplitud y profundidad de la intrusión y la dificultad para detectar estas operaciones, configuran un escenario en el que el espionaje se vuelve menos detectable. Este escalamiento no solo multiplica las posibilidades de vulneración de la privacidad y la seguridad, al exceder cualquier proporción razonable, sino que también genera nuevas formas de afectación, incluidas las que se manifiestan en el ámbito psicosocial. Por lo tanto, resulta fundamental analizar a fondo las implicaciones de estas tecnologías, tanto en su dimensión técnica como en su impacto emocional y social.

El objetivo de esta investigación es analizar el impacto del software espía (spyware) como herramienta de vigilancia estatal en la región latinoamericana contra personas defensoras y periodistas, que han sido objeto de esta intrusión. Se busca examinar cómo estas tecnologías tienen efectos que, mas allá de los datos y la esfera digital, afectan la seguridad física, la salud, el bienestar económico-social y los derechos de las personas afectadas.

A través de un análisis de casos documentados, se pretende comprender los impactos específicos psicosociales y las formas de afrontamiento personal y colectivo.

---

2 Access Now. (2023, mayo 3). Estados: Frenen el spyware que amenaza la libertad de prensa. <https://www.accessnow.org/press-release/declaracion-conjunta-spyware-libertad-de-prensa/>

# Tecnologías Espía o de Vigilancia (Spyware)

## Uso de software espía como herramienta de inteligencia y represión estatal.

La creciente disponibilidad de tecnologías avanzadas de espionaje ha potenciado la capacidad de algunos gobiernos para ejercer un control sistemático sobre las personas que consideran una amenaza para su dominio. En este contexto, el uso de spyware se ha consolidado como una estrategia clave, dirigida a objetivos específicos dentro de un ciclo de inteligencia que no solo recopila información, sino que facilita la represión, la intimidación y, en muchos casos, el hostigamiento digital y físico. Este ciclo opera con base en la selección previa de objetivos determinados por su perfil político, su trabajo en la defensa de derechos humanos o su pertenencia a organizaciones que son percibidas como un riesgo para las autoridades de turno. La implementación de estas herramientas requiere la participación de estructuras estatales con acceso a recursos, tecnología y, en muchos casos, apoyo directo o indirecto de actores con poder político y económico<sup>3</sup>

Es fundamental diferenciar tres prácticas: la vigilancia digital, el espionaje con spyware y los ataques o el acoso en línea. Cada una de ellas tiene características específicas que se relacionan con un uso estratégico y específico de las tecnologías para lograr distintos fines, así como en alcance, niveles de



<sup>3</sup> Amnistía Internacional (2023, octubre 9). Global: El escándalo de los 'Archivos Predator' revela ataques descarados con software espía contra la sociedad civil, figuras políticas y altos cargos. [Comunicado de prensa]. <https://www.amnesty.org/es/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/>.

intrusión y efectos. De la misma manera, estas prácticas pueden ser aplicadas en combinación como parte de las tácticas de represión e intimidación, no solo digital sino incluso física.<sup>4</sup>

La vigilancia digital es el monitoreo sistemático de actividades en línea, realizado por gobiernos, empresas o actores privados, con fines de control político e investigaciones sobre estructuras y redes de personas, tanto para la explotación comercial y extractiva de datos como para la identificación, seguimiento y neutralización de “sujetos de interés.”

El hostigamiento en línea, en cambio, es un patrón de comportamiento abusivo y agresivo dirigido a una persona o grupo en el entorno digital. Incluye ataques verbales, difamación, amenazas, acoso sexual y la difusión de información personal, real o ficticia, con el fin de intimidar o dañar. A diferencia de la vigilancia digital, su propósito principal es causar daño emocional, psicológico o, a la imagen pública de la persona. Sin embargo, estos ataques no se limitan al ámbito individual, también se utilizan como mecanismo para afectar a colectivos específicos (como mujeres defensoras, comunidades indígenas, población LGBTIQ+ u organizaciones sociales) con el propósito de estigmatizarlas, debilitar su legitimidad y reforzar su marginación en el espacio público y político.

El espionaje con spyware, por su parte, constituye una clase de software malicioso, diseñado, específicamente, para infiltrarse de forma encubierta en dispositivos electrónicos con la intención de recolectar datos sin el conocimiento ni el consentimiento de las personas afectadas.

Este tipo de herramienta permite el monitoreo integral de actividades digitales, incluyendo acceso a comunicaciones cifradas, geolocalización en tiempo real, activación remota de micrófonos y cámaras; además de extracción de archivos o credenciales sensibles. Su implementación se inscribe dentro de operaciones de inteligencia, dirigidas a personas y entidades consideradas estratégicamente

---

4 Kizza, J.M. (2023). Cyberbullying, Cyberstalking and Cyber Harassment. In: Ethical and Secure Computing. Undergraduate Topics in Computer Science. Springer, Cham. [https://doi.org/10.1007/978-3-031-31906-8\\_9](https://doi.org/10.1007/978-3-031-31906-8_9)

como fuentes de datos relevantes para el análisis de dinámicas organizativas, capacidades operativas y patrones de comportamiento o, elaboración de mapas de redes, con el propósito de alimentar procesos de toma de decisiones, evaluación de amenazas y diseño de acciones orientadas al control, neutralización o desarticulación de dichos actores. La información obtenida a través de estas intrusiones puede, posteriormente, ser empleada para diseñar y ejecutar campañas de hostigamiento, criminalización, extorsión o desprestigio, así como facilitar otras formas de agresión, tanto en el ámbito digital como en el terreno físico, político o legal.<sup>5 6</sup>

### **Características del espionaje facilitado por spyware**

El spyware representa una evolución estratégica preocupante frente a métodos tradicionales de obtención de inteligencia, por su capacidad de operar con alto sigilo, persistencia y precisión. A diferencia de prácticas visibles o invasivas, como interrogatorios, infiltraciones, seguimientos presenciales o requisas, permite acceder a información crítica sin alertar al objetivo, minimizando riesgos operativos de la estructura que lo opera.

Esta capacidad de operar con extrema discreción, maximiza el control dentro del ciclo de inteligencia, al sostener una vigilancia prolongada y encubierta sobre personas u organizaciones. Esto permite una acumulación constante y detallada de información sobre sus dinámicas internas, vulnerando principios fundamentales de privacidad y abriendo la puerta a abusos de poder difíciles de detectar o fiscalizar.<sup>7</sup>

Una vez que el spyware se instala, su objetivo principal es mantener la persistencia sin ser detectado. Para ello, emplea vulnerabilidades de día cero (zero-day exploits), que son fallas desconocidas por los fabricantes de software y, aún, sin solución. En muchos casos, la infección ocurre sin que el usuario realice ninguna acción (zero-click attacks), lo que lo hace particularmente peligroso. Asimismo, estos

---

5 Oliveira, P. (n.d.). Cybercrime Module 12 Key Issues: Cyberstalking and Cyberharassment. United Nations Office on Drugs and Crime. <https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html>

6 Hiperderecho. (n.d.). Tecnoresistencias. <https://hiperderecho.org/tecnoresistencias/identifica/>

7 Ahmad, Atif, et al. (2021). (2021, March 27). Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack. <https://doi.org/10.48550/ARXIV.2103.15005>

programas implementan sofisticados métodos de evasión, ocultándose en procesos legítimos del sistema, borrando registros de actividad y evitando ser detectados por antivirus o herramientas de monitoreo de seguridad.<sup>8</sup>

Por otra parte, el uso de spyware constituye una grave vulneración de derechos fundamentales y del bienestar integral de las personas objeto de vigilancia. Sus efectos no son neutros, reproducen y amplifican desigualdades estructurales preexistentes.

Cuando se dirige contra mujeres, personas LGBTIQ+ o colectivos históricamente marginados, adquiere características específicas que exceden la afectación a la privacidad. La información extraída puede ser instrumentalizada para chantajes, represalias o campañas de estigmatización que refuerzan discursos de odio y prácticas de violencia basadas en prejuicios de género, orientación sexual, identidad o expresión.<sup>9</sup>

## **Uso de spyware por gobiernos en América Latina**

A escala global, cada vez más gobiernos adquieren spyware con el pretexto de combatir el crimen y el terrorismo.<sup>10</sup> Sin embargo, investigaciones han demostrado que estas tecnologías se utilizan, principalmente, para vigilar a periodistas, activistas y figuras políticas. Un informe de Amnistía Internacional en 2023 reveló que el Spyware Predator había sido utilizado para espiar a funcionarios de la ONU, senadores de Estados Unidos y presidentas de parlamentos.<sup>11</sup>

En América Latina, el interés gubernamental por estas tecnologías ha ido en aumento. Un estudio de 2016 documentó la adquisición del software espía Hacking Team (comercializado como Galileo o DaVinci) por parte de Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá. Este software, anunciado

---

8 Kareem, Karwan. (2024, April 30). A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security. arXiv, <https://doi.org/10.48550/ARXIV.2404.19677>

9 Access Now. (2023, marzo 8). Women human rights defenders targeted with Pegasus spyware in Bahrain and Jordan. <https://www.access-now.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/>

10 UN News. (2023, marzo 14). Counter-Terrorism “rhetoric” Used to Justify Rise of Surveillance Technology: Human Rights Expert. <https://news.un.org/en/story/2023/03/1134552>

11 Amnistía Internacional. (2023, marzo 29). Amnistía Internacional denuncia nueva campaña de hackeo ligada a empresa de software espía mercenario. <https://www.amnesty.org/es/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/>

originalmente “para la persecución del crimen”, ha sido principalmente utilizado para espiar a personas defensoras de derechos humanos, exponiéndolas a hostigamiento, amenazas y ataques coordinados.<sup>12</sup>

El uso de spyware no solo representa una amenaza latente, sino que también forma parte de una estrategia más amplia de intimidación y control. En El Salvador, bajo la administración de Nayib Bukele, periodistas del medio digital El Faro fueron víctimas de al menos 226 ataques con Pegasus entre 2020 y 2021. El análisis pericial realizado por The Citizen Lab en conjunto con Access Now establece que, desde el 29 de junio de 2020, miembros del periódico digital El Faro sufrieron al menos 226 ataques con Pegasus<sup>13,14</sup>. La gravedad del caso motivó a la Comisión Interamericana de Derechos Humanos a expresar su apoyo al medio y condenar “cualquier acción intrusiva de los dispositivos de comunicación” que no cuente con un “marco legal y transparente que esté acorde con las normas y estándares internacionales de derechos humanos, garantizando los principios de necesidad, proporcionalidad.”<sup>15</sup>

En México, el uso de Pegasus ha sido ampliamente documentado. Investigaciones en 2017, de Citizen Lab, R3D, SocialTIC y Article 19, revelaron ataques dirigidos contra periodistas, abogados, legisladores y activistas anticorrupción.<sup>16</sup> Entre 2019 y 2021, nuevas investigaciones forenses realizadas por R3D y Citizen Lab, confirmaron infecciones con Pegasus en dispositivos de periodistas y personas defensoras de derechos humanos mediante ataques de tipo “zero-click”, que no requieren ninguna interacción por parte de la persona intervenida. Estas evidencias confirmaron el uso sistemático de este software espía contra integrantes de la

---

12 Pérez de A., Gisela. (2016). Hacking Team: malware para la vigilancia en América Latina. Derechos Digitales. <https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf>

13 Bonilla, D. y Reyes D. (2022, January 12). In Brief: Pegasus Spying on El Faro. El Faro (<http://elfaro.net/especial/in-brief-pegasus-spying-on-el-faro/>)

14 Scott-Railton, John, et al. (2022, January 12) Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware. Citizen Lab Research Report No. 148, University of Toronto. <https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/>

15 CIDH (Comisión Interamericana de Derechos Humanos). (2022, enero 31). La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador. [Comunicado de prensa]. <https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp>

16 Scott-Railton, M., Razzak, A., Nigro, D. (2022, octubre 2). Identifican nuevos abusos del software espía Pegasus en México. The Citizen Lab. <https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/>

sociedad civil mexicana, reafirmando el patrón de vigilancia con fines de represión e intimidación en el país.<sup>17</sup>

A pesar de las evidencias, la regulación del spyware sigue siendo inexistente en la mayoría de los países de la región. Investigaciones han confirmado el uso de malware en Honduras y Guatemala, entre otros países, sin que existan mecanismos efectivos de protección legal, supervisión o rendición de cuentas.<sup>18</sup>

---

<sup>17</sup> R3D: Red en Defensa de los Derechos Digitales. (2018, septiembre 22). Pegasus continúa operando en México, revela informe del Citizen Lab. <https://r3d.mx/2018/09/21/pegasus-continua-operando-en-mexico-revela-informe-del-citizen-lab/>

<sup>18</sup> "Fundación Acceso. (2020). Herramientas de Vigilancia Digital Identificadas en Centroamérica. [https://www.acceso.or.cr/wp-content/uploads/2021/08/2020\\_Art\\_Herramientas\\_Vigilancia\\_CA-mayo2020.pdf](https://www.acceso.or.cr/wp-content/uploads/2021/08/2020_Art_Herramientas_Vigilancia_CA-mayo2020.pdf)

# Efectos Psicosociales Del Software Espía

Para comprender los efectos del software espía en la dimensión psicosocial, partiremos por comprender el enfoque psicosocial. “No es simplemente una suma entre lo psicológico y social, sino una mirada integral que permite comprender como los procesos sociales afectan a las personas y como ellas procesan, resisten o reproducen esos efectos en sus vidas” (Berinstain, 2006, p. 30).<sup>19</sup> Este enfoque nos lleva a identificar como las experiencias traumáticas afectan en lo individual y colectivo, con impactos en la identidad, el proyecto de vida, la memoria colectiva y los procesos de reconstrucción social.

Frente a los distintos impactos provocados por situaciones de violencia o vulneración de derechos, las personas –tanto en lo individual como en lo colectivo– activan diversas formas de respuesta que les permiten resistir, adaptarse y dar sentido a lo vivido. En este contexto, el afrontamiento se entiende como el conjunto de estrategias cognitivas, emocionales y conductuales con las que se intenta gestionar el estrés y las emociones asociadas a la adversidad, favoreciendo así procesos de resiliencia y reconstrucción del tejido social.

Los ataques con software espía tienen consecuencias. Según el estudio “Experiencias emocionales en las víctimas de violaciones a la ciberseguridad” las personas vigiladas describieron que la ira, la tristeza y la inseguridad, están asociadas con los ataques de seguridad cibernética. Una reacción común fue la paranoia, la sensación constante de ser vigilado. La paranoia afecta la capacidad de confiar en el entorno. El estudio documenta cómo estos ataques pueden generar depresión por la invasión a la privacidad; además, la falta de control sobre la propia información, genera desesperanza.<sup>20</sup>

---

19 Berinstain, C. (2006). Manual de atención psicosocial en procesos de reparación integral. Instituto Interamericano de Derechos Humanos.

20 Budimir, S., Fontaine, J. R. J., & Roesch, E. B. (2021). Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology, Behavior and Social Networking*, 24(9), 612-16. <https://doi.org/10.1089/cyber.2020.0525>

En otro estudio, “Ataque, infección, vigilancia y daño” realizado en 2023, define daño cibernético como la consecuencia perjudicial de un evento que afecta el bienestar del individuo. Expone que las personas sufren daños psicológicos graves, en particular miedo, ansiedad, inseguridad, sentimiento de paranoia, pérdida de confianza y aislamiento.<sup>21</sup> Los informes sobre vigilancia también documentan que las personas se censuran por miedo. “Las personas periodistas y defensoras de derechos humanos juegan un rol indispensable en nuestras sociedades y, cuando son silenciadas, los círculos sociales cercanos son impactados.”<sup>22</sup> Otro impacto puede ser el aislamiento social, debido a que las personas afectadas pueden volverse más reacias con otras personas, temen que sus comunicaciones sean interceptadas.<sup>23</sup>



21 Kekre, Cardillo, Fisher. (2023). Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People. [https://www.graduateinstitute.ch/sites/internet/files/2024-01/ARP\\_FINAL\\_REPORT\\_-\\_Aditi\\_Amol\\_Kekre.pdf](https://www.graduateinstitute.ch/sites/internet/files/2024-01/ARP_FINAL_REPORT_-_Aditi_Amol_Kekre.pdf)

22 Declaración de la Alta Comisionada de la ONU para los Derechos Humanos, Michelle Bachelet, sobre el uso de software espía para vigilar periodistas y personas defensoras de derechos humanos | ONU-DH ([hchr.org.mx](https://www.unhcr.org/mx)).

23 <https://www.sciencedirect.com/science/article/abs/pii/B9780128162033000046?via%3Dihub>

# Metodología

Este estudio buscó comprender el impacto psicosocial que incluye el ámbito familiar, laboral, económico, así como las formas de afrontamiento que pusieron en marcha para enfrentar sus efectos.

Para ello se utilizó un método cualitativo<sup>24</sup> con cinco entrevistas individuales y una entrevista grupal con dos personas expertas en ciberseguridad y protección digital, con el fin de explorar las experiencias de personas que han enfrentado situaciones de vigilancia a través de software espía.

Se diseñaron entrevistas semiestructuradas para las personas individuales y para la grupal. Las entrevistas se llevaron a cabo de manera virtual a través de la plataforma meet.greenhost.net, además, se proporcionó un entorno seguro y confidencial.

En cada entrevista, las personas participantes relataron los hechos vividos y compartieron sus reflexiones personales sobre cómo estos eventos afectaron sus vidas. Estas entrevistas se realizaron del 11 al 22 de septiembre de 2024.

Las entrevistas fueron anónimas y se expresan en este documento de manera codificada. Sus nombres, en este informe, son ficticios y se trata de periodistas o abogados/as que trabajan en el ámbito de la defensa de los derechos humanos. Todas las personas entrevistadas firmaron un consentimiento informado que garantiza el anonimato y la privacidad.

Se realizó una entrevista grupal con dos expertos en acompañamiento y protección digital. Ellos reportan sobre los casos que han asesorado de manera anónima y confidencial. Los casos que suelen atender llegan a las personas expertas por el vínculo organizativo establecido previamente o por referencias de organizaciones aliadas.

---

24 Enfoque cualitativo, un enfoque apropiado debido a su poder para ahondar “en profundidad en complejidades y procesos” y explorar fenómenos menos conocidos. Marshall & Rossman. (1999). *Designing qualitative research*, p. 57. (3rd ed.). Sage.

# Resultados de la investigación

A continuación, se presentan los principales resultados en distintos apartados, la primera sección se refiere a las características del espionaje por spyware desde el punto de vista de las personas afectadas; la segunda sección, trata sobre los principales impactos psicosociales. Y finalmente, en la tercera, se describen las principales formas de afrontamiento que se encontraron en las entrevistas.

## Características de los ataques de software espía

### a) El uso de software espía busca el control social y la censura

Según las entrevistas realizadas, el objetivo de instalar software espía trasciende la vigilancia. Opinan que el fin es el control, fomentar la sensación de vulnerabilidad, la amenaza y amedrentar a las personas por la labor que realizan. Un especialista que participó en la entrevista grupal afirma que los teléfonos son una extensión nuestra, tienen toda nuestra información,

“Los teléfonos son una extensión de nosotros muy importante. Socialmente las personas las suelen usar 24/7, ahí tienen contactos, conversaciones fotos videos, ubicaciones, si esta información cae en manos de actores o personas malintencionadas, tiene implicaciones en su seguridad física, sobre todo a periodistas que publican cosas sobre corrupción que hacen señalamientos directos, bueno obviamente, riesgos de amenazas contra la persona.”  
(participante entrevista grupal).

Una entrevistada refiere que vive la vigilancia como estar dentro del panóptico que plantea Foucault. El concepto de panóptico en la teoría de Michel Foucault se refiere a un modelo de vigilancia y control social. Se inspiró en el diseño arquitectónico del Panóptico ideado por Jeremy Bentham, que permitía a un vigilante observar a todos los prisioneros sin que estos supieran si estaban siendo

observados. Para él es una metáfora del poder moderno y de cómo las sociedades disciplinarias ejercen control sobre los individuos. La idea central es que la posibilidad de ser observado induce a la persona a autorregular su comportamiento, promoviendo la conformidad y la obediencia (Foucault 2002, p. 202),

“La constante sensación de estar siendo visto siempre como Foucault y el panóptico. Todos mis [años] 20 los viví así, como que en el momento pensaba, no está siendo así, pero el pensamiento siempre estaba.” (E5).

Ella agrega que,

“Cuando cumplí 21 años, un agente asesor del presidente publicó mi locación en vivo, aquí están todos (nombre de la institución) por si quieren venir a darle presentes. Yo estaba con mis amigos de 21 años. También estaba con compañeros del periódico, entonces yo pensaba, estoy poniendo en riesgo a mis amigos.” (E5).

El panóptico cumpliría su función cuando las personas empiezan a autorregularse y autocensurarse,

“Sí, he tenido mucho miedo, autocensura, porque pienso muchas veces que lo que diga, lo que escribí o lo que pienso me va a causar problemas, me va a generar seguimientos y ese tipo de cosas. Yo voy en la calle, salgo a caminar, salgo en mi vehículo y siempre estoy pensando que alguien puede estar detrás de mí. Estoy pensando que alguien está vigilándome, muy seguido. Si la computadora se pone lenta o si se calienta el teléfono muy seguido, pienso que hay alguien que está tratando de ingresar a mis dispositivos para saber que estoy haciendo.” (E4).

Otro entrevistado habla sobre el control,

“El nombre del software tiene la palabra vigilancia, pero el fin no es la vigilancia sino el control.” (E2).

## **b) El software espía como herramienta de vigilancia estatal**

Las personas fueron infectadas aparentemente porque trabajaban en proyectos que incomodaban al gobierno; entonces, les instalan un software espía para controlar relaciones, movimientos, contactos y comunicaciones,

“Porque los casos que vi de los periodistas y de derechos humanos, si ve el tipo de infección todos los casos coinciden en tiempos donde ellos, ellas, ellos estaban trabajando con socios del gobierno o casos del gobierno que iba a tener un impacto negativo y el gobierno ha hecho espionajes.” (E2).

Para otras personas entrevistadas, el gobierno quería saber quiénes son las fuentes<sup>25</sup> de la información que publican,

“Lo que buscaban [era] tener una idea de nuestras vidas, estaban todo el día en nuestros teléfonos, les facilitaba conocer movimientos y creo que lo que más les interesaba era saber qué nos compartían nuestras fuentes y, qué información teníamos o las llamadas que hacíamos (E3).

Lo cierto es que el trabajo que realizan estos periodistas ha sido muy importante para ciertos sectores que, llegan a pagar altas sumas de dinero para conocer de cerca el trabajo periodístico. Como explica el entrevistado,

“Es muy caro este espionaje, entendimos que cada licencia está alrededor de 50 000 dólares, entendemos que el software que nos instalaron tiene costos muy altos por la capacidad que tiene de intervenir.” (E4).

---

25 <https://www.amnesty.org/en/latest/news/2024/05/thailand-state-backed-digital-violence-silence-women-lgbti-activists/>

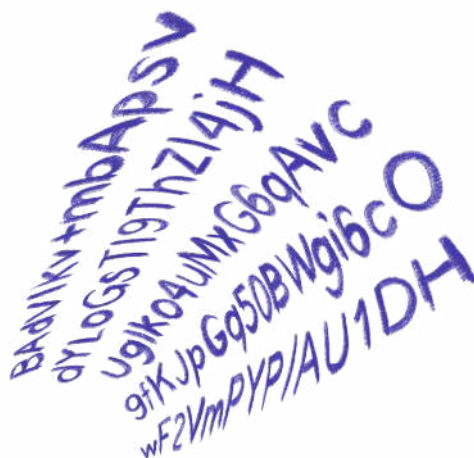
También se genera una desacreditación de estas personas con acusaciones que pueden afectar su integridad; además de tratarlas como enemigos del gobierno,

“El gobierno produce discursos en contra de los y las comunicadoras concurrentemente, sacaban narrativas, cortinas de humo para controlar el discurso, para retomar el control del discurso. Cuando sale una noticia escandalosa, por ejemplo, la negociación con las pandillas, el gobierno entonces lo que hace es sacar alguna noticia, por ejemplo, acusar falsamente... de violación o acusar a una periodista de obtener beneficios por dar favores sexuales, distrae a la opinión pública.” (E2).

Es importante considerar que los ataques vienen de personas muy poderosas,

“Hay que considerar que el espionaje viene de grupos altamente violentos, como militares, grupos organizados del crimen que también amenazan de muerte.” (Entrevista con expertos).

Para concluir, instalar un software espía es un tipo de agresión que busca el control de diferentes ámbitos de las personas y grupos sociales a los que pertenecen. Las personas se sienten vigiladas y desarrollan afectaciones psicosociales como estrés, cansancio, hipervigilancia, falta de comprensión de lo que les sucede y quiebre del proyecto de vida.



### **c) La interrelación entre el software espía con violencia física o digital**

La vigilancia en los casos estudiados ha sido una estrategia dentro de otro tipo de agresiones que se han utilizado en contra de las personas entrevistadas, sus organizaciones o grupos de pertenencia. Este tipo de vigilancia va acompañada de otras agresiones como vigilancia física, amenazas, encarcelamientos, criminalización, desprestigio y violencia en redes sociales,

“Uno de mis compañeros fue detenido, entonces fuimos muy afectados por su detención porque como nosotros estábamos emitiendo opiniones, lo detuvieron de manera sospechosa sin el debido proceso. Ha impactado porque nos dimos cuenta de que si podía ser real.” (E1).

Es importante destacar cómo los ataques espía se suman a otras experiencias difíciles que han vivido por el carácter de su trabajo, como enfrentarse cotidianamente a la violencia, la muerte y la desaparición,

“Eso como que rompió la piñata del trauma, porque en el último viaje que iba [a mi país] decía: aquí vi un muerto, aquí vine cuando mataron a otro, esta es la casa que quemaron cuando mataron a tal persona. El último reportaje que hice... fue cuando mataron a dos personas y los sacaron de la colonia en donde yo crecí. Cuando vi que una chava de mi edad desapareció en la colonia donde yo caminaba todos los días, ahí decidí migrar.” (E5).

Otra persona entrevistada habla de que la vigilancia en línea se acompaña de vigilancia física,

“En el transcurso de los meses empecé a tener vigilancia física en mi colonia, cosa que era muy inusual porque es una colonia donde solo habitan personas de la tercera edad, familias, una colonia en donde casi no vive nadie, empecé a notar personas inusuales fotografiando las casas de la zona o haciendo recorridos, carros particulares no familiares parqueados, patrullas.” (E2).

Otra añade,

“Yo sé que al final, el espionaje formó parte de otro cúmulo de situaciones que me llevó a una baja laboral, de unos dos meses, para poder recibir tratamiento.” (E3).

Una entrevistada explica la diferencia entre la vigilancia física y la vigilancia a través de software espía,

“En la vigilancia no digital es posible tener alertas o que la detectemos, la vigilancia en internet es imperceptible e invasiva, ya que manejamos cosas de nuestra vida privada en los móviles y tiene más canales para que nos vigilen, se puede realizar de manera anónima, se puede tener acceso a otros tipos de información sobre nuestra vida, favorece la impunidad.” (E1).

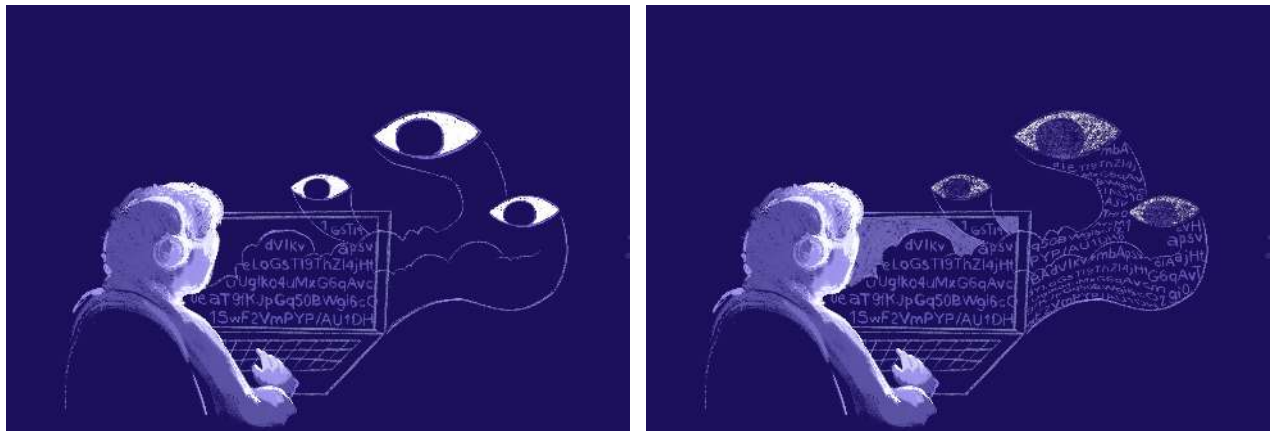
Debido a que la vigilancia con software espía es imperceptible e invasiva, las personas se sienten vigiladas, pero sobre todo controladas todo el tiempo, sucede entonces que cuestionen su profesión y los valores que han depositado en su carrera, que se autocensuren y silencien.

## Impactos Psicológicos y Psicosociales

Los efectos de las agresiones con software espía, en combinación con otras agresiones, son amplios y se expresan tanto en la dimensión psicológica como la psicosocial.

Entender la profundidad del daño causado a las personas y comunidades requiere distinguir entre las dimensiones psicológicas y psicosociales del impacto. Esta diferenciación, planteada por Elizabeth Lira (2017), es fundamental para abordar de forma integral las secuelas de la represión y las violaciones a los derechos humanos. Mientras los impactos psicológicos se expresan en síntomas individuales como el miedo, la ansiedad o el trauma, los impactos psicosociales aluden a una afectación más amplia que atraviesa la confianza colectiva, la vida comunitaria, los vínculos y la memoria social.

## a. Impactos psicológicos



### 1. Pánico

En un primer momento el impacto lleva a la persona a un estado de incredulidad o de conmoción, no sabe cómo responder y se siente abrumada o llega a sentir pánico. Esto hace que se aíse o se paralice. A diferencia del miedo que puede producir una reacción más intensa y desorganizada.<sup>26</sup>

Según la entrevista realizada a uno de los expertos las personas entran en pánico,

“Pues pánico total, si una persona tiene idea de que esto le sucede, pues pánico total, la mayoría de las veces las personas ni siquiera saben que hacer, es una situación en la que, por general, las personas no se encuentran preparadas.” (entrevista grupal).

“Es tan importante centrarnos en las primeras horas cuando recibimos el espionaje porque esas primeras horas fueron las que más generaron una sobrecarga emocional, hay que aprender a manejarla.” (E3).

Una entrevistada lo explica,

“Estar así con tantas cosas encima, con el estrés, a uno se le dificulta tomar otro tipo de decisiones que estando en un estado normal, no sería tan difícil, pero yo que conozco de medidas de seguridad, me bloqueé, en esos momentos ni quería lidiar con eso, me estresaba el hecho de pensar en eso.” (E1).

26 Morales, M. (2023, septiembre 16). Miedo, pánico y angustia: similitudes y/o diferencias. Revista Central. Recuperado de <https://www.revista-central.com.mx/bienestar/diferencias-miedo-panico-angustia>

Agrega que,

“Lo que hace generalmente es aislarse, aislarse y/o congelarse, paralizarse, no saber que hacer.” (E1).

## 2. Normalización de la violencia

Otras personas como mecanismo de defensa tienden a normalizar la situación, ven el ataque como algo que podría pasar y pasó,

“La violencia tiende a convertirse en algo natural en contextos donde se ha hecho cotidiana, donde ha perdido su carácter de excepcionalidad. Esta naturalización conlleva una aceptación pasiva o resignada y produce un efecto de anestesia emocional que bloquea la empatía, la indignación y la posibilidad de actuar.” (Beristain, 2010, p. 58).<sup>27</sup>

Al trabajar en los medios de comunicación saben que corren riesgos y que los pueden perseguir y encarcelar. Para poder sobrevivir en estas condiciones hay una especie de normalización de la violencia digital,

“La normalización te dice, bueno yo sé que me pueden matar. En los periodistas el perfil de riesgo está más elevado, estoy a la merced de ser la víctima de esta situación como (resignarse).” (entrevista grupal).

Si bien se normaliza, se sabe que las personas no deben de vivir con ese miedo constante,

“Se normaliza. Pero afuera hay millones de gente que viven sin miedo y eso es normal.” (E5).

Lo que podría funcionar como un mecanismo de defensa es la “negación”, que consiste en rehusar a aceptar la realidad por temor a que sea dolorosa. Puede ser útil en un principio, pero puede interferir con una vida emocional saludable.<sup>28</sup>

---

27 Beristain, C. M. (2010). Manual sobre perspectiva psicosocial en la investigación de derechos humanos. Hegoa. Instituto de Estudios sobre Desarrollo y Cooperación Internacional. <https://publicaciones.hegoa.ehu.es/publications/233>

28 <https://www.amnesty.org/es/what-we-do/technology/online-violence/> - <https://www.amnesty.org/en/latest/news/2024/05/thailand-state-backed-digital-violence-silence-women-lgbti-activists/>

### 3. Hipervigilancia

Las personas entrevistadas hablaron de que inician una etapa de hipervigilancia que les agota por estar todo el tiempo alerta. La hipervigilancia es un estado de alerta extrema. Las personas en este estado están constantemente atentas a posibles amenazas y peligros. También es un síntoma de trastorno de estrés postraumático (TEPT). Va acompañada de ansiedad, afecta la capacidad de concentración, lo que tiene consecuencias en el rendimiento laboral y en las relaciones sociales. Estar en un estado de alerta causa agotamiento físico y mental. Asimismo, las personas hipervigilantes pueden evitar la visita a lugares o personas, lo que los lleva a aislarse.<sup>29</sup>

“Sensación de hipervigilancia, pero ya sabías que iba a pasar, hay una cadena de emociones, la primera frustración y decepción. Una cosa, es decir, sabía que podía pasar y, otra es, ya está.” (entrevista grupal).

“Hipervigilancia, cambio de calles, las más rebuscadas, evitar las rutas principales, manejar por barrios. Casi no salía de la casa, la mayoría de las veces utilizando precauciones que la mayoría de gente no las usaría, ni siquiera se le ocurriría.” (E2).

### 4. Pensamientos recurrentes

Los pensamientos recurrentes son ideas o imágenes que se repiten en la mente una y otra vez, pueden ser involuntarios y, a menudo, están asociados a la ansiedad, al estrés o, también estar relacionadas con el trastorno de estrés postraumático (TEPT). Pueden también, interferir en la capacidad de concentración o en su vida cotidiana<sup>30</sup>

Las personas inician un proceso de autocuestionamiento, preguntándose: ¿qué hice?, empiezan a tener pensamientos repetitivos sobre los datos que, posiblemente, obtuvieron de sus dispositivos y cómo los podrían utilizar en su contra,

---

29 <https://www.amnesty.org/es/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/>

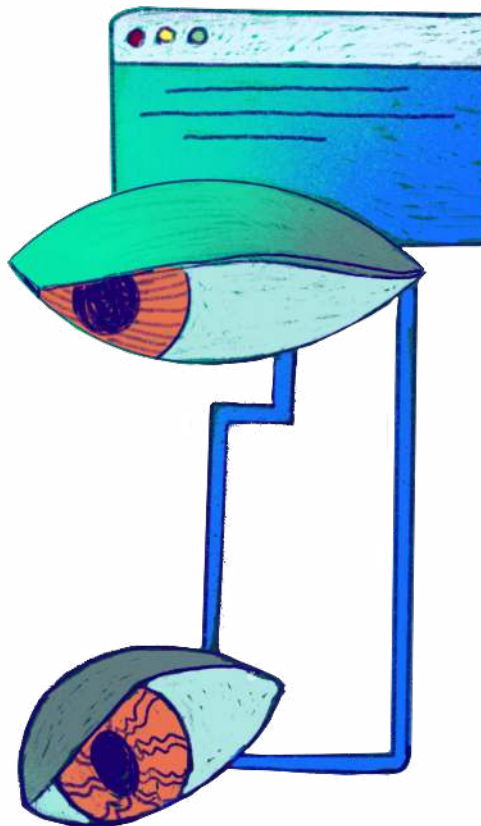
30 Budimir, S., Fontaine, J. R. J., & Roesch, E. B. (2021). Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology, Behavior and Social Networking*, 24(9), 612-616. <https://doi.org/10.1089/cyber.2020.0525>

“Entonces empiezan las interrogantes de que supieron de mi pareja, de mis hijos, hijas e hijes, también hay una sensación bien profunda de enojo. De frustración ante la impunidad, porque no es un tema nuevo que los gobiernos espían, entonces están saliendo casos y las cosas no cambian, es una sensación de impotencia ante la impunidad.” (entrevista grupal).

Los pensamientos recurrentes también crean constantemente escenarios sobre lo que puede suceder ahora que tienen la información,

“Creas escenarios en la cabeza porque tenés certeza de qué información tienen.” (E5).

Todas las personas entrevistadas dijeron que sufren de pensamientos recurrentes desde que se enteraron de que les instalaron el software espía. Las personas entrevistadas con pensamientos recurrentes también sufren de ansiedad y alteración en el sueño.



## 5. Ansiedad

Las personas entrevistadas presentan diferentes respuestas de ansiedad que interfieren significativamente con las actividades cotidianas. Es una reacción ante eventos amenazantes, se caracteriza por una preocupación excesiva y persistente acompañada de síntomas como tensión muscular, palpitaciones, dificultad para respirar y trastornos de sueño. Las personas entrevistadas indicaron como la vigilancia puede cronificar o intensificar la ansiedad,

“Tuve un par de ataques de ansiedad, esa sensación de estar hiperventilado con un dolor en el pecho.” (E2).

“Ansiedad sí, estuve en constante alerta, en esos períodos en que yo me di cuenta que se estaba realizando vigilancia hacia mí, lo que produjo en mí es insomnio, estrés, me ha provocado o intensificado la ansiedad que yo venía sintiendo después de la cuarentena. La pandemia me dejó un trastorno de ansiedad, pero luego me di cuenta de la vigilancia en contra mía y eso vino a intensificar o a hacerme retroceder en el trabajo que estaba realizando para combatir la ansiedad y el insomnio, también por el estado de alerta.” (E1).

Esta entrevistada cuando entendió qué implicaba la instalación de un software espía se le incrementó la ansiedad,

“Eso nos desbordó porque llegamos a tener niveles de ansiedad muy altos cuando nos explicaron que es Pegasus y entender el alcance que tenía.” (E3).

“Se me diagnosticaba mucha ansiedad, pero todavía no me habían dado el aval para hablar del tema, entonces justo, voy acumulando y acumulando hasta que la olla explotó y fue al siguiente año que yo decidiera darme un tiempo de baja.” (E3).

Las personas entrevistadas, al saber que son vigiladas, refieren que se les ha incrementado la ansiedad que habían experimentado por otros eventos anteriores en su vida, llegando hasta sentir ataques de pánico.

## 6. Alteraciones en el sueño

Las alteraciones en el sueño puede ser una forma de respuesta a estas experiencias, derivada de altos niveles de ansiedad o angustia. Entre ellos puede

darse insomnio, dificultad persistente para conciliar el sueño o, por otro lado, tener sueño permanente. Despertar a horas inusuales o, simplemente, alteraciones en el propio ritmo de sueño,

“Insomnio, siempre he tenido problemas de insomnio. En esos años si tenía un insomnio y se intensificó mucho esos días, al punto de dormir solamente por fatiga, ni siquiera por necesidad, el cuerpo lo hace.” (E2).

Otra entrevistada también hablo sobre pesadillas,

“La ansiedad se volvió en sueños intensos, soñaba que me perseguían o que me detenían, soñaba que mis amigos estaban en peligro.” (E3).

Esta persona que vive en el exilio sufre de pesadillas y la ansiedad se incrementa cuando regresa a su país. Por ejemplo, piensa que la pueden apresar por no pagar impuestos,

“Llevo años con pesadillas (de mi país) y cuando he ido con bajo perfil, lo paso mal, genuinamente mal, estoy viendo si no debo impuestos, si no van a meterme presa por 5 dólares. A mis amigas nunca les digo la fecha en la que llego, a mi mamá le aviso por llamada, nunca le digo cuando llego.” (E5).

## 7. Depresión

Dos de los entrevistados hablaron de sufrir depresión. En contextos de violencia socio-política, la respuesta de depresión se presenta de diferentes formas: sentimientos de tristeza, ganas de llorar, malestar e irritabilidad, aislamiento, desgana, problemas para dormir, autoreproches, pesimismo.<sup>31</sup>

En algunos casos esta depresión se desencadena desde situaciones anteriores, sin embargo, se reactivan con la vigilancia,

“Yo estuve en una depresión en los últimos meses a raíz de cosas que sufrí en mi infancia, creo que la desencadenaron también todas estas situaciones.” (E4).

“Problemas de depresión..., luego de ese diagnóstico me medicaron por depresión.” (E 2).

---

31 Kekre, A., Cardillo, M., Fisher, S. (2023). Targeting, Infecting, Surveilling, Harming. A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People. Geneva Graduate Institute, Cyberpeace Institute.

“Yo por la ansiedad o por el insomnio, por la depresión, había días que no quería hacer nada.” (E1).

Las personas entrevistadas experimentan varias de estas respuestas, la vida les cambió y el impacto ha afectado el ámbito familiar, social y laboral.

## **8. Miedo**

Tres de las personas entrevistadas hablaron de sentir miedo. Según Elizabeth Lira, el miedo puede provocar conductas específicas que pueden ser descritas como procesos adaptativos frente a situaciones amenazantes. La experiencia de permanente dificultad y riesgo para enfrentar la vida cotidiana incide subjetivamente en la persona y la manera de percibirse a sí mismo y a su entorno. El miedo puede transformarse en permanente sobre todo si se cronifican las circunstancias percibidas como amenaza vital.

El miedo ha hecho que las personas se censuren,

“Si he tenido mucho miedo, autocensura, porque pienso muchas veces que lo que diga, lo que escribí o lo que pienso, me va a causar problemas, me va a generar seguimientos y ese tipo de cosas.” (E4).

O que no realicen actividades que antes normalmente realizaban,

“Yo ya no quería hablar por teléfono, porque tenía miedo.” (E5).

El miedo también es por la posibilidad de que sus familiares sufran agresiones,

“Tenía unos proyectos de hacer podcast, al regresar mi esposa con mi niño (al país de origen) renuncié por miedo, si bien yo estoy acá (en el exilio), ellos están allá y son un blanco fácil, ir tras de mi padre de mis hermanas y de mi hijo o de mi esposa.” (E2).

Aunque esta persona ya tiene más de dos años de estar afuera, las preocupaciones no han bajado, siente miedo, angustia, se siente amenazada y piensa que el gobierno todavía la puede afectar. Ella sufre de una sensación generalizada de

inseguridad que le provoca miedo constante. Por ejemplo,

“Ahora tuve que ir al consulado (de su país) a renovar mi pasaporte, acá en donde yo vivo, yo estaba llorando en el consulado, porque tenía que poner mi dirección y mi teléfono actual, es un procedimiento normal, que yo sé que nadie del consulado quiere hacerme algo, las caras visibles del periódico son otras, pero eso no implicó que sintiera miedo, al estar ahí.” (E5).

“No me parece normal o sano que uno se ponga a llorar al renovar el pasaporte” (E5).

Si bien el miedo es una emoción provocada por una percepción de peligro, una reacción que advierte de una amenaza, activa reacciones como lucha, paralización o huida. El problema para las personas entrevistadas con el software espía es que no tienen claro quién o quiénes están detrás de la amenaza.

## **9. Efectos en el cuerpo y la salud**

Las personas entrevistadas también hablan sobre problemas con su salud, dolores corporales y padecimientos que podrían volverse crónicos como: colitis, dolores de cabeza, cervicalgia. Para Van Der Kolk, que desarrolla una larga investigación sobre las huellas del trauma en las emociones y el cuerpo, explica que existe una relación entre el impacto psicológico del estrés y el trauma y, la afectación en el cuerpo, aduciendo que funcionamos de manera integral, mente y cuerpo.<sup>32</sup>

Estos efectos en el cuerpo ya existían antes, pero la vigilancia y otras formas de violencia asociadas las han desarrollado. Como explica esta persona,

“Antes por mucho tiempo padecí de colon irritable, sin embargo, con todo este relajó, me regresó la colitis. Luego he estado con problemas de alimentación que tienen su origen en la salud mental.” (E2).

“Dolor de cuerpo, dolor de cabeza, adormecimiento en la cara, he estado con medicamentos.” (E4).

---

32 Van der Kolk, Bessel A. (2020). El cuerpo lleva la cuenta: cerebro, mente y cuerpo en la superación del trauma. Translated by Montse Foz Casals, 3a. edición., Editorial Eleftheria.

“Me generaba un problema mayor en mi espalda y en mi cuello, se me diagnosticó cervicalgia y desarticulación de cuello. Me hicieron varios estudios porque querían descartar problema artrítico. El psiquiatra me ha dicho que yo tengo trastorno somatomorfo porque somatizo parte de los problemas que hay a mi alrededor.” (E3).

## **b. Impactos psicosociales**

### **1. Aislamiento social**

Este tipo de impacto es una de las expresiones más significativas del daño psicosocial, impide la elaboración colectiva del sufrimiento, profundiza el miedo y obstaculiza los procesos de recuperación y reconstrucción del tejido social.<sup>33</sup>

Todas las personas entrevistadas hablaron de una sensación generalizada de inseguridad que provoca una evitación de lugares y personas. Esto repercute en el apoyo social, tienden a aislarse de las personas que podrían brindarles contención y solidaridad,

“No puedo visitar lugares que antes frecuentaba o sentirme completamente libre y en paz. Ahora hay cierta paranoia de estar monitoreando quien está alrededor, quién nos está escuchando, el sentir que puedo hablar plenamente a través de mi teléfono.” (E1).

Por lo delicado que resulta haber sufrido un ataque con software espía y, para no poner en peligro a las personas con las que se tiene relación, como contactos, familia o las fuentes, se les ha aconsejado no hablar sobre el incidente, pero esto deja sin iniciar un proceso de desahogo emocional y construcción de vínculos saludables,

“Fue duro porque ya nos habían dado recomendaciones que no podíamos hablarlo con nadie, entonces en un inicio éramos solo las personas que estábamos. Un grupo muy pequeño que estábamos enteradas, pero luego nos dimos cuenta, con mi compañera, que era algo que nos sobrepasaba. Yo sé que al final el espionaje formó parte de otro cúmulo de situaciones que

---

<sup>33</sup> Equipo de Acción Psicosocial y Acción Comunitaria. (2013). Reparar lo invisible: Desafíos para una atención psicosocial transformadora. Ediciones Antropos.

generaron mucha ansiedad, pero eso fue la cereza del pastel que me llevó a una baja laboral, de unos dos meses, para poder recibir tratamiento.” (E1).

De igual manera, los espacios de ocio también se ven afectados. Por ejemplo, un grupo de periodistas han decidido tomar precauciones en su comportamiento al salir al ámbito público,

“Siempre hay que comportarnos como periodistas, es una situación muy terrible y no podemos comportarnos como una persona normal. El hecho de que algo tan básico como si te tomas una copa o agarras un vehículo, aunque esté permitido, nosotros tenemos advertencia de no conducir con una gota de alcohol en el cuerpo, ningún comportamiento que vaya a ver comprometida nuestra integridad o que venga una ola de propaganda en contra de nosotros.” (E4).

## 2. Proyecto de vida

El denominado 'proyecto de vida' atiende a la realización integral de la persona, considerando su vocación, aptitudes, circunstancias, potencialidades y aspiraciones, que le permiten fijarse razonablemente determinadas expectativas y acceder a ellas.<sup>34</sup> Por esto, el impacto psicosocial incluye la desestructuración del horizonte vital, es decir, la imposibilidad de continuar con los planes, sueños y vínculos que daban sentido a la existencia.<sup>35</sup>

En las entrevistas realizadas se pueden ver diferentes niveles de afectación en el proyecto de vida. En el ámbito laboral, tres personas dejaron sus trabajos; dos sufrieron separaciones al salir al exilio, lo que implicó dejar a sus familias y amigos. Dejaron su tierra, sus costumbres, sus hogares.

Las personas a lo largo de la vida vamos tendiendo metas a largo plazo y expectativas según nuestras posibilidades para el desarrollo integral. Un ejemplo de afectación al proyecto de vida lo muestra esta entrevistada. Ella explica que durante los años que le dedicó al trabajo no pudo realizar las cosas que personas a

---

34 Esteban, Ana. (2002). El desarraigo como vivencia del exilio y de la globalización. Open Edición Journal.

35 Beristain, C. M. (2010). Manual sobre perspectiva psicosocial en la investigación de derechos humanos. Hegoa. Instituto de Estudios sobre Desarrollo y Cooperación Internacional. <https://publicaciones.hegoa.ehu.es/publications/233>

su edad realizan, hacía un trabajo, pero todos los ámbitos personales estaban atravesados por las amenazas del Estado,

“Yo ya no quería estar relacionada con el (trabajo), le dediqué 20 años al periodismo, y yo pensaba, púchica hay un montón de cosas que no he vivido en esa etapa y hay un montón de cosas que he vivido que no debía de haber vivido en esa etapa.” (E5).

El proyecto de vida se convierte en su mayor vulnerabilidad, su profesión hace que pueda llegar a sufrir agresiones, vigilancia y control,

“Muchos sentimientos de soledad y también el hecho de que el trabajo que hacemos está ya desvalorizado y que ha perdido todos los sentidos. Estoy haciendo un trabajo que prácticamente no sirve para nada porque lo desacreditan, de tal forma, que es muy grave, ese creo que es un tipo de soledad, el hecho de pensarse en un trabajo que no vale tanto, entonces uno se siente abandonado.” (E4).

Una de las personas entrevistadas empezó a trabajar a los 19 años en un periódico temas de derechos humanos. Posteriormente, se dedicó a temas de memoria histórica, violencia de género y derechos humanos. Con el gobierno de Nayib Bukele empezaron las sospechas, seguimientos y las amenazas en redes sociales. En septiembre de 2021 recibió en su celular un mensaje que le decía que tenía un software espía, luego constataron que había sido infectada con Pegasus.

El impacto fue fuerte y en distintas dimensiones de la vida,

“Ya no publico tanto en redes sociales, dejé mi trabajo, hubo muchos factores por los que me fui y pasé a hacer trabajo más detrás de cámara. Los factores internos también influyen, pero el espionaje estatal fue la gota que derramó el vaso, dije ya no tengo nada que hacer acá. Saber que no solo tengan mi información, sino la información de mi familia, de mi mamá, de mis sobrinos. Mi mamá ya no quería hablar por teléfono porque tenía miedo.” (E5).

“Una falta absoluta de libertad y del sentido de seguridad. Tener la confirmación fue lo más feo a pesar de que ya tenía dudas.” (E5).

El exilio es uno de los factores que más afectan el proyecto de vida: el cambio de país, de cultura, de idioma, la pérdida de cotidianidad, de cercanía con la familia, todos estos aspectos hacen que las personas tengan que reinventarse y, en uno de los casos, cambiar totalmente de trabajo.

Dos de las personas entrevistadas viven en el exilio, lo que ha representado un costo muy alto para su economía y, en lo emocional, nuevos retos por el desarraigo y separación de la familia. Si bien en el exilio se logra tener más certeza sobre la seguridad personal, se pierden otras cosas que dan sentido a la vida, como la relación con la familia, las amistades y los espacios generales de relacionamiento.

El exilio y desplazamiento de sus lugares de origen puede provocar el mayor impacto al proyecto de vida a las personas que son forzadas a abandonar su hogar y su entorno familiar. Pueden experimentar una serie de emociones como la pérdida de conexión con otras personas, incertidumbre y falta de control sobre el futuro, separación de seres queridos y la adaptación a un nuevo entorno. Las personas en el exilio a menudo experimentan una fuerte nostalgia por su hogar y su vida anterior.<sup>36</sup>

### **3. En el ámbito familiar**

En general, las familias viven en los mismos contextos que las personas afectadas, por lo que saben los riesgos que corren sus familiares al hacer la labor de defensoría o de periodismo.

La familia sufre por los ataques que las y los defensores y periodistas están viviendo. En su afán de protegerles les piden que abandonen su proyecto de vida. Esto hace que prefieran silenciarse en el espacio familiar y, así, se incrementa el aislamiento y los sentimientos de soledad,

---

<sup>36</sup> Son las consecuencias que tienen las experiencias y las vivencias de las agresiones sobre las emociones y estado mental de las entrevistadas.

“A nivel familiar, si me sentí un poco sola porque lo que hubiera querido era un poco más de apoyo y lo que recibí de ellos fue un regaño. Fue una invitación a censurarme, por lo que de parte de ellos, sí me sentí sola, en la obligación de no comentar cualquier cosa con cualquier persona por temor a que se revirtiera contra mí, el estar opinando y, la misma situación la viví con amigos.” (E1).

Para las personas que viven un ataque espía, el sufrimiento de la familia o de personas cercanas son fuente de ansiedad y un estresor adicional por lo que deciden el distanciamiento,

“Me alejé de mis amigos, me alejé de mi familia, cambié de casa, fue un momento bien estresante porque tuve que realizar varios cambios a nivel personal, a nivel familiar, profesional no tanto, aunque sí adoptar medidas de seguridad.” (E1).

Las amistades o familiares también se alejan por miedo a sufrir el espionaje y sus consecuencias,

“Ha habido un aislamiento social por el miedo generalizado que existe, uno nota que hay cierto rechazo y, uno lo nota, mucha gente que quiere mantener la distancia.” (E4).

Como resultado de este distanciamiento, el círculo social se reduce a las personas con las que se comparte una relación laboral o de activismo,

“Se nota la lejanía, entonces lo único que hacemos es tener más relación social con nuestros propios compañeros.” (E4).

Sin embargo, hay otras familias que pueden brindar cobijo y apoyo a las personas vigiladas, precisamente, por estar desconectadas de ámbitos de sociedad civil.

Las familias también pueden estar afectadas por las separaciones, sobre todo por el exilio.

#### 4. Impacto con base en el género

Las entrevistas realizadas nos dieron referencia sobre los ataques con un claro contenido de violencia de género dirigido a mujeres defensoras. Como indica la investigación de Amnistía Internacional, los ataques spyware dirigidos a personas de la comunidad LGBTIQ+ también suponen un riesgo diferenciado.<sup>37</sup> Al hablar de contenidos violentos con discriminación basada en género, dominan estereotipos asignados a las mujeres con contenido machistas, discursos que en la historia se han utilizado contra las mujeres como: descalificarlas al llamarlas “putas” o ejercer violencia sexual.

Las mujeres entrevistadas dicen que los ataques contra ellas tienen contenido de violencia sexual. Este acoso tiene que ver con las agresiones en redes sociales y un discurso que, generalmente, va encaminado a la creación de consenso sobre estereotipos de género,

“Los ataques hacia mujeres son de tipo sexual y, en general, las activistas mujeres han sufrido más ataques sexuales.” (E1).

Otra entrevistada opina,

“Hasta para atacarnos nos discriminan, ellos pueden aguantar que son tontos o que son estúpidos, pero a ellos nadie les dice te voy a violar, son cosas que les pasan a las mujeres.” (E5).

La violencia contra las mujeres ejercida en redes tiene como objetivo paralizarlas y atacarlas en aspectos de su sexualidad, en su aspecto físico. También su propósito es ir contra su reputación y amenazarlas de violación y muerte,

“Los ataques son agresivos, pero muchas veces la reacción que se tiene de ese ataque puede llegar a ser muy cruel cuando se es mujer, porque lo que quieren es destruir a la persona a modo de que se sienta en riesgo y agredida.” (E3).

---

<sup>37</sup> Beristain, C. M. (n.d.). Sobre perspectiva psicosocial en la investigación de derechos humanos. Corteidh.or.cr. <https://www.corteidh.or.cr/tablas/27117.pdf>

Las agresiones buscan paralizar a las mujeres por atreverse a entrar en un ámbito público históricamente reservado para los hombres; además, los ataques van destinados a desprestigiarlas por ser mujeres y no por su trabajo.

## **5. En cuanto al equipo de trabajo y el entorno laboral**

En los equipos de trabajo el spyware tiene diferentes efectos como el miedo, la sobrecarga y el cansancio. Cuando las personas rompen el silencio y se atreven a contarlo, pueden generar una cadena de pánico que podría perdurar en el tiempo alterando el funcionamiento de las organizaciones,

“En una organización lo primero que se hace es contarlo y va a generar una cadena de pánico, de cómo comprometieron a esta persona y, yo colaboré con esta persona hace dos días, entonces, esto lleva a que las personas se sientan inseguras.” (entrevista grupal).

Produce desconfianza en los equipos de trabajo. El hecho del espionaje altera la confianza básica de las personas dentro de las organizaciones,

“Esto tiene secuelas a largo plazo, perduran en el tiempo. Hay un trabajo que hay que hacer posterior para concientizar de cómo funciona la tecnología, porque los cimientos en los que las organizaciones se basaban para trabajar, se derrumban.” (entrevista grupal).

Otro factor que afecta al equipo de trabajo es el cansancio, hay que realizar el trabajo diario, pero con nuevas actuaciones de seguridad y cuidado. Lo que produce un resultado de cansancio en los equipos,

“Todos lo estamos manejando como una inercia, estamos cansados, se nota el cansancio del equipo, estamos lidiando con el trabajo, pero, además, con esta situación, pensando que hoy atacan a uno, hoy pueden estar vigilando de esta manera, entonces. (En estas circunstancias) ¿cómo se discute sobre normas de seguridad?”

Se prioriza seguridad en una sociedad en la que tendrías que estar pensando en cómo hacer mejor tu trabajo.” (E4).

De la misma manera, hay un impacto económico en los equipos de trabajo, hay preocupación, por parte de un entrevistado, de los gastos extra que tienen que realizar la organización que lo contrató,

“Del lado de (mi trabajo) ha afectado de maneras diferentes, ellos (su organización) tienen una carga económica asociada al contratarme. Al contratar una persona (local), no tendrían que pagar abogado de migración” (E2).

También hay miedo a que la organización sufra nuevas agresiones, como un impacto mediático.

Al contratar a alguien que ha sido víctima, primero, se exponen a que, si mi dispositivo fuera jaqueado, la conversación de trabajo [se conozca]. Al fin y al cabo, es inevitable tener conversaciones de trabajo. Por otro lado, el gobierno con los datos que colectaron, o la vigilancia física tendrían un impacto mediático.” (E2).

Otro entrevistado habla de una parálisis temporal en los equipos de trabajo,

“Hay una parálisis temporal, sobre todo en el momento que se termina de hacer el análisis inicial, porque, generalmente, cuando hay una persona vigilada, primero se tiene que hacer el análisis de hasta donde fue el alcance del impacto. Hay que identificar que otros actores se comprometieron dentro de la organización (entrevista grupal).

Sobre el desempeño laboral las personas expresan que no pueden concentrarse de la manera como lo hacían antes y que deben dedicar horas laborales a su bienestar psicológico,

“Adicionalmente, impacta un poco el desempeño de mi trabajo, no solo que me quita años de vida y de vida útil, sino que he tenido situaciones en las que

mi desempeño no es el mejor, ni el adecuado, porque estoy cargando con todo esto, que no hay manera que ni mi organización ni yo mismo me lo puedo quitar. No puedo evitar que el Estado me persiga, no puedo resolver yo solo todos los problemas de salud mental que han aflorado o empeorado por esta situación, entonces también eso me presiona a mí para tratar de mantenerme cuerdo.” (E2).

“Siento que a diferencia de hace 5 años he bajado el rendimiento, la producción, uno invierte tiempo en curarse, en recuperarse y se deja de lado todo lo demás que uno hace en el trabajo. Después de esto me he dedicado a saldar mis problemas personales, no es por comodidad, han surgido cosas que uno no sabe controlar.” (E4).

Otro impacto es en los equipos que atienden a las personas y organizaciones que fueron infectadas, ellos también pueden afectarse al dar la asesoría técnica para enfrentar su situación.

Un especialista entrevistado dice que ellos reciben apoyo psicoemocional,

“Hay cosas que nos sobrepasan, a veces ha habido casos de vigilancia hacia nosotros y esos escenarios son más estresantes y debemos tener mecanismos por si hay alguien que lo necesite. Por parte de los donantes tenemos un fondo de respuesta rápida para apoyar estas situaciones.” (entrevista grupal).

Agrega que,

“Desgaste por empatía. Se deben visibilizar los riesgos con las personas que recién se están incorporando a este trabajo, pueden sufrir burnout, desgaste por empatía, es importante subrayarlo.” (entrevista grupal).

Los equipos de trabajo sufren efectos que tienen que ver con la desconfianza, el cansancio, la inseguridad, también tiene un impacto económico y logístico, deben

hacer un reacomodo en las finanzas, en los procesos organizativos, además de buscar apoyo psicológico y técnico en aspectos de seguridad.

## **6. Impacto económico**

La economía de las personas afectadas también ha sido impactada por todos los gastos extras que deben hacer para su salud, traslados de su vivienda actual o de su país; además de la compra de nuevos dispositivos electrónicos.

“Exámenes y tratamientos que son caros, mi doctor me dijo cuando vi al psiquiatra, que estaba dejando todo mi salario en tratamiento, dijo, revalúe si quiere seguir (trabajando).” (E1).

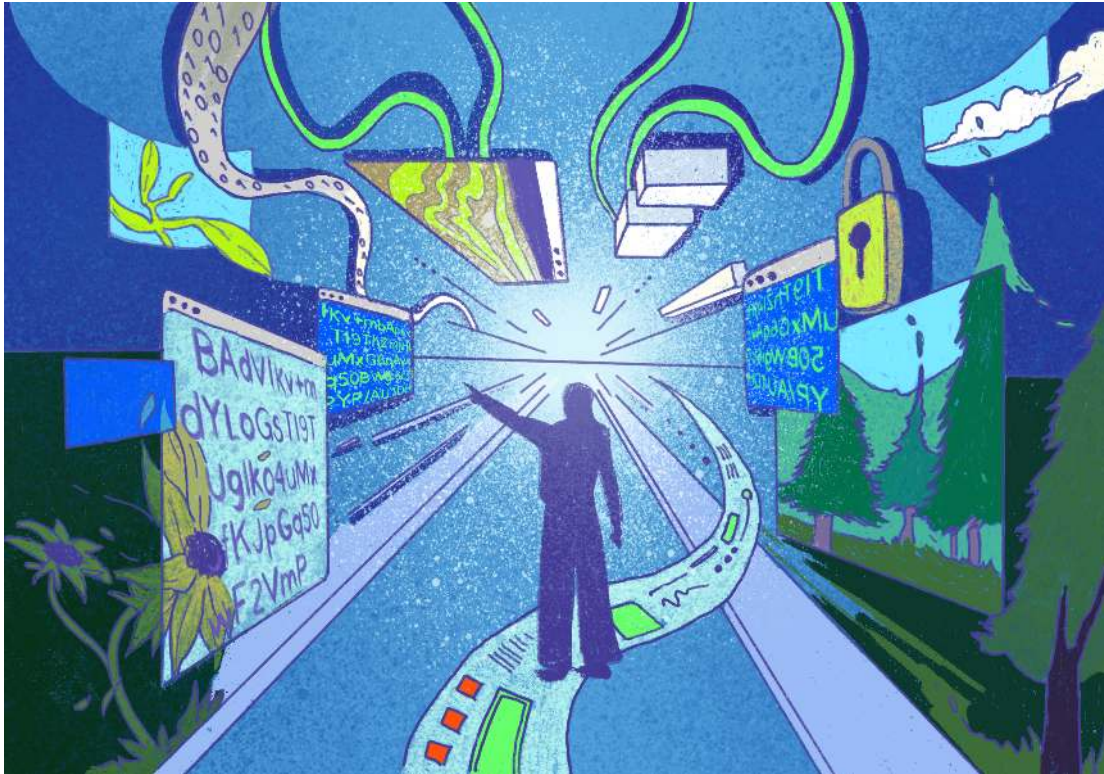
También hablan de la compra de nuevos equipos por la desconfianza de utilizar equipos que ya fueron infectados,

“Entonces hay un impacto inmediato de adquirir un nuevo dispositivo, pero esto solo para los que tienen recursos. Al final lo que cuenta es la paz mental y la paz la puede dar, obtener otro dispositivo, pero hay otros que no podrán.” (entrevista grupal).

“Hay casos en los que una persona decide desplazarse y, esto tiene un costo económico, lo que hemos visto es que no existen formas para manejarlo, aun en casos de cambio de dispositivo, así que siempre suele venir de los fondos propios de la persona.” (entrevista grupal).

# Afrontamientos

El afrontamiento se concibe como un proceso integral que trasciende la respuesta individual ante la adversidad.



Desde la perspectiva de Aluna, el afrontamiento se aborda desde una mirada transdisciplinaria que integra dimensiones psicoemocionales de seguridad, organizativas y políticas. Este enfoque busca fortalecer las estrategias de resistencia y autonomía frente a las violencias estructurales, promoviendo la justicia social.<sup>38</sup>

Berinstain destaca que el afrontamiento en contextos de violaciones de derechos humanos implica procesos de adaptación activa y pasiva; en este sentido, las personas afectadas podrían desarrollar mecanismos de defensa que les permita sobreponerse a las experiencias vividas. Los mecanismos pueden incluir el silencio o la resistencia colectiva.<sup>39</sup>

38 Aluna Acompañamiento Psicosocial. (2021). (2019, diciembre 3) Impactos psicosociales de la defensa de los derechos humanos sobre las mujeres defensoras. PBI México. <https://pbi-mexico.org/es/noticias/impactos-psicosociales-de-la-defensa-de-los-derechos-humanos-sobre-las-mujeres-defensoras>

39 Martín Berinstain, C. (2017). Metodologías de investigación, búsqueda y atención a las víctimas: Del caso Ayotzinapa a nuevos mecanismos en la lucha contra la impunidad. FLACSO. <https://www.flacso.edu.mx/libro/metodologias-de-investigacion-busqueda-y-atencion-a-las-victimas-del-caso-ayotzinapa-a-nuevos-mecanismos-en-la-lucha-contra-la-impunidad/>

De esta manera, entendemos el afrontamiento como un proceso colectivo y transformador que involucra una reconstrucción de redes de apoyo y resiliencia comunitaria, posicionando la dignidad humana frente a los mecanismos de opresión.

Esta sección describe estrategias de afrontamiento utilizadas por las personas entrevistadas.

## **1. Cambios de hábitos y rutina**

En lo individual, las personas describen un cambio en sus hábitos orientados a la seguridad. Al preguntar cómo lo afrontan, todas las personas entrevistadas señalaron el cambio de rutinas como algo generalizado.

“Cambié mis rutinas totalmente, los bares a los que recurría antes del espionaje, también después de la pandemia, no volví a mi vida anterior, si voy a algún lugar, pueden estar monitoreando, porque usualmente... a veces nos movemos en manadas en esos lugares.” (E3).

Los cambios de rutina involucran cambios en usos de la tecnología. Las personas han encontrado formas de afrontar el impacto del software espía realizando cambios en las rutinas, dejando de usar redes sociales o cambiándose a medios de comunicación más seguros.

“las medidas que he tomado ha sido dejar de usar las redes sociales o desactivar mis cuentas en redes sociales, bajar el perfil.” (E1).

“Sí, adoptar medidas de seguridad, las que me daba la cabeza en ese momento. Usar una VPN, en mi celular, en mi dispositivo, hacer cambios al router de la casa” (E1).

“Con mis amistades, dejamos los mensajes. Tuvimos que migrar de aplicación, preferimos una aplicación segura. Hablo con todo el mundo por Signal.” (E3).

Otro mecanismo de afrontamiento es el uso de nuevos dispositivos de comunicación, así se garantiza que están “limpios”, aunque tiene un costo alto para su economía que ya ha sido impactada,

“Adquirir un nuevo dispositivo, pero esto solo para los que tienen recursos, al final lo que cuentan es la paz mental y, la paz, la puede dar obtener otro dispositivo.” (entrevista grupal).

## **2. Reubicación**

Las personas afectadas hablaron de cambiar de residencia, lo que les proporciona seguridad, buscan lugares donde no les reconocen con facilidad o no se les asocia al rol que tenían. Les da tranquilidad y la posibilidad de descansar y sentirse un poco más seguros.

“Vivir en esta casa, luego mudarme para otra, separarme de mi pareja, sobre todo cuando estaba haciendo esas investigaciones.” (E1).

Dos personas han afrontado la situación saliendo del país para sentirse más seguras,

“Salir del país lo supimos al final de año.” (E5).

Por octubre empecé a tramitar mi salida del país, la mía, de mi esposa e hijo.  
(E2)

Si no salen del país, sí deciden aislarse un tiempo,

“Ha habido personas que han decidido aislarse por un tiempo, deciden parar un par de días, un par de semanas para elaborar una estrategia nueva con base en lo que se identificó porque al final sus espacios privados fueron vulnerados, por eso necesitan este espacio para armar una estrategia nueva.” (entrevista grupal).

Las personas que han estado sometidas a tensión y sufren efectos psicológicos debido al estrés elevado, experimentan, además, miedo. Cambiar de ambiente es una forma de dar un respiro a la tensión y, por un tiempo, brinda una sensación de tranquilidad.

### 3. Autocuidado

El autocuidado entendido como la capacidad de reconocer las propias necesidades físicas, emocionales, relacionales y espirituales, constituye un componente clave dentro de los mecanismos de afrontamiento psicosocial.<sup>40</sup> En las personas entrevistadas se identificó el ejercicio como un mecanismo para bajar la ansiedad y poder dormir mejor.

Una persona dijo,

“Trate de equilibrarlo con ejercicio. En esa etapa yo intensifiqué mis ejercicios y vi que podía conciliar el sueño, sobre todo los desvelos y todo lo que implicaba. Además del impacto que también lo emocional tiene a nivel físico, lo intensifique con el ejercicio.” (E1).

El ejercicio reduce el estrés,<sup>41</sup> lleva a la persona a moverse en otro ámbito con la posibilidad de cambiar de pensamientos, mejorar el estado de ánimo y la salud en general.

### 4. Búsqueda de apoyo psicológico

Todas las personas entrevistadas dicen haber recibido apoyo psicológico, si bien algunas de ellas ya lo venían recibiendo, lo buscaron con algunas organizaciones. Esto les ayudó a trabajar la ansiedad, la depresión y los trastornos del sueño,

“Yo ya tenía mi terapeuta anterior, dos años antes, no quise meterme en otro proceso, lo afronté bien por eso, la terapeuta me ayudo un montón.” (E5).

“Yo ya tenía un psicólogo con quien estaba trabajando duelos.” (E3).

El acompañamiento psicológico ha sido un apoyo fundamental para las personas que tuvieron acceso a recibirlo, así, han podido contar con alguien en quien pueden confiar con atención especializada.

---

40 Equipo de Acción Psicosocial y Acción Comunitaria. (2013). Reparar lo invisible: Desafíos para una atención psicosocial transformadora. Bogotá: Ediciones Antropos.

41 Lazarus, R. S., Valdés, M., Folkman, S. (1986). Estrés y procesos cognitivos. Martínez Roca.

## 5. Asesoría técnica

Otra forma de afrontamiento ha sido la búsqueda de ayuda de un experto en seguridad digital, lo que lo que les ha permitido mitigar un poco el estrés al conocer qué fue lo que sucedió y, qué se puede hacer para enfrentar las situaciones de riesgo,

“Recibí asesoramiento de personas expertas, pero de manera remota y, por eso mismo que no tenía cabeza, sí recibí acompañamiento, pero en esa situación eran recomendaciones que yo tenía que implementar.” (E1).

Otro entrevistado afirma que recibir formación de expertos puede ayudar a comprender mejor el fenómeno,

“Reforzar el conocimiento sobre cómo tener herramientas, hay que saber cómo piensa el enemigo, cómo ejecutan estas cosas, para saber qué medidas tomar. cómo poner llaves a todos los dispositivos, cómo tenemos el conocimiento para cuidarnos de manera más natural, sin recurrir a cosas emergentes.” (E4).

El apoyo técnico funciona tanto para evitar la soledad en estos momentos de estrés y preocupación, como para obtener un poco más de información, lo que proporciona control sobre una situación nueva que los hace sentir intimidados.



## 6. Red de apoyo

Las redes de apoyo son espacios donde se reconoce el sufrimiento, se valida la experiencia vivida y se genera confianza para iniciar procesos de sanación, justicia y transformación social. No son solo herramientas funcionales, sino también espacios de cuidado ético, político y emocional.<sup>42</sup>

La búsqueda de apoyo social, crear vínculos con personas que pueden entender este tipo de agresión ha sido muy importante para las personas entrevistadas.

“Yo fui construyendo mi red de apoyo con personas que yo conversaba sobre ciertos temas o que yo vi que eran afectadas. Lo que hay que hacer es conectares en lugar de aislarse.” (E1).

Esto se ve reforzado por su grupo de pertenencia que les apoya,

“El tema de apoyo entre las organizaciones hemos visto que desde hace tres años ha habido un esfuerzo grande de organización de hacer redes.”

“En la comunidad de periodistas se ve mucho estos apoyos en redes, sobre todo en comunicados.” (entrevista grupal).

El apoyo social juega un papel fundamental en el afrontamiento,

“Tuve bastantes personas de apoyo desde amistades especialistas y fundaciones para periodistas. En un evento expliqué que no podía estar por problemas de salud mental, hablaron con una organización hermana y me apoyaron con el pago a los psiquiatras. Otra organización de mujeres periodistas me apoyaron con el impacto económico que estaba generando todo esto y de ahí tuve otras. Y otros apoyos, más emocional, de personas que siempre estuvieron.” (E1).

Como forma de afrontamiento, las personas, sobre todo públicas, denuncian y se protegen como colectivo. Algunas entrevistas enfatizaron que entre las formas de

---

42 Equipo de Acción Psicosocial y Acción Comunitaria. (2013). Reparar lo invisible: Desafíos para una atención psicosocial transformadora. Ediciones Antropos.

cuidarse ha sido agruparse como gremio, por ejemplo, el periodismo para denunciar públicamente. Algunas de las acciones para solidarizarse con la persona afectada es hacer comunicados y conferencias de prensa para mostrar que el periodista o la periodista no están solos.

El humor y la risa han sido usadas en los ámbitos laborales para bajar la ansiedad, como explica una entrevistada sobre cómo se banalizaba la violencia.

“Mi escritorio estaba de espaldas, les decía, a mí es la primera que van a matar, los otros decían, si nos agarran de parte de la calle al que van a matar es a mí. Esos eran los chistes.” (E5).

En resumen, los grupos han desarrollado estrategias de afrontamiento como la denuncia, la risa, el humor, el apoyo, la solidaridad y la defensa mutua.

En muchos casos las familias han constituido esta red de apoyo, pues representan un espacio seguro para las personas vigiladas. Acuden a su familia, como el lugar en el que pueden cambiar rutinas y desconectarse del ámbito de la sociedad civil, sentirse apoyada y arropada,

“Las personas deciden refugiarse con sus familias, las que están desconectados de los ámbitos de sociedad civil, entonces los costos no son tan altos y tienen un espacio seguro de confianza, porque tienen el alojamiento con las familias.” (entrevista grupal).

Un experto en protección explica,

“Se requiere trabajo amplio que siempre se logra en red, en nuestro caso formamos parte de una red. Pero si trabajas sola, no sería un trabajo que se podría llevar adelante. La revisión técnica es solo el primer paso, pero el análisis no resuelve el problema, se necesita trabajar con abogados, abogadas, tomadoras de decisiones, hacer evaluaciones desde otros ámbitos, para accionar mucho más amplio.” (entrevista grupal).

## 7. Apoyo interinstitucional

El apoyo institucional es importante para el cuidado de personas que han sido vigiladas con software espía,

“Estuve en un programa de cuidado con reporteros sin fronteras y eso también me ayudo a trabajar mi ansiedad, aprendí a que el espionaje no se puede evitar, que es muy difícil. Pero hay manera de limitar los riesgos.” (E3).

Las organizaciones buscan cómo mejorar el cuidado colectivo en los equipos. Brindando atención psicológica o vinculando a sus equipos con personas expertas que pueden apoyar en la seguridad,

“(la organización) sacó que si necesitábamos terapia teníamos 10 sesiones.” (E5).

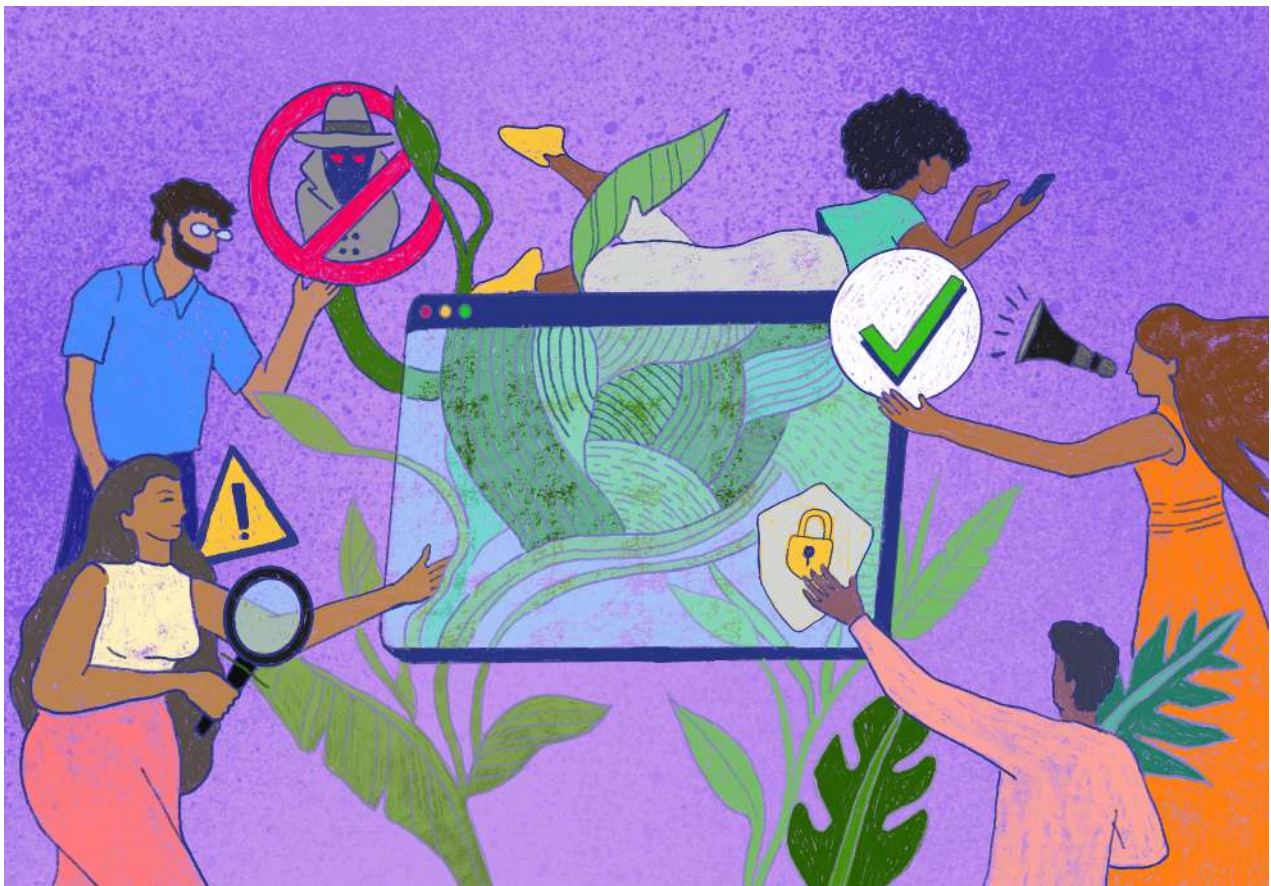
Ellos que trabajan apoyando personas que han sido infectadas con software espía cuando se le pregunta cómo se protegen de los efectos dice,

“Hay un trabajo personal, de mi lado, de distanciamiento, para mí es importante el trabajo, pero he logrado distanciarme y dissociarme para verlo como trabajo y que no me invada a nivel personal.” (entrevista grupal).

Las personas y los equipos han logrado encontrar formas de enfrentar la vulnerabilidad generada por la instalación de un software espía, brindando apoyo psicológico, reforzando la seguridad de los equipos de cómputo o celulares, dando capacitación a las personas para mejorar su sensación de seguridad. También expresan la necesidad de trabajar en red para tener asesoría. Ellos y ellas han trabajado para lograr conformar una red para abordar temas legales, tecnológicos, psicosociales y logísticos.

# Conclusiones

1. Según las entrevistas realizadas, el fin de instalar software espía va más allá de la vigilancia, el fin es el control, fomentar el sentimiento de vulnerabilidad, crear una sensación de amenaza y reprimir a las personas en la labor que realizan.
2. En los casos de las personas entrevistadas la instalación de un software espía vino acompañada de otras agresiones como: seguimientos físicos, encarcelamientos de colegas cercanos, ataques en redes sociales, desplazamiento y exilio, eventos que impactan la salud mental y constituyen trauma secuencial o acumulativo. Los efectos psicosociales se reflejan en lo individual, colectivo, emocional, cognitivo y físico.



3. Las personas han vivido cambios en la vida familiar, laboral y económica profundizando los impactos psicosociales.
4. Los impactos psicosociales a raíz del spyware profundizaron los niveles de ansiedad o depresión que se registraban antes de este tipo de agresiones.
5. La primera reacción que tuvieron frente a la noticia fue de dos tipos, algunas personas reaccionaron con una conmoción inicial, miedo intenso, ansiedad y hasta pánico. Otras, según las entrevistas realizadas, tuvieron reacciones más tranquilas debido a que tenían la sensación de que les iba a suceder.
6. Entre los efectos encontrados está la hipervigilancia que es un estado de alerta extrema. Esta va acompañada de ansiedad, afecta la capacidad de concentración, lo que tiene consecuencias en el rendimiento laboral y en las relaciones sociales.
7. Expresaron un miedo intenso que puede permanecer en el tiempo cuando hay un estímulo que lo reactiva, llegando a convertirse en una amenaza vital.
8. El proyecto de vida se vio afectado, por ejemplo, dos personas salieron al exilio y renunciaron a su trabajo. Esto implica adaptarse a una nueva cultura, a un nuevo idioma, en un caso y, a nuevas rutinas. También implica la separación de familias y amigos.
9. En el ámbito familiar puede haber reacciones de censura, así como familias que pueden brindar cobijo y apoyo. Las familias también han sido impactadas por las separaciones.
10. El contexto social donde se producen los ataques es de miedo generalizado, la población teme emitir opiniones en contra del gobierno. Esto hace que amistades y personas cercanas tienden a alejarse de la persona para no sufrir lo mismo.

11. En los equipos de trabajo se evidencian diferentes impactos, desde pánico hasta el cansancio, en muchos casos es necesario implementar nuevas medidas de protección en un contexto de inseguridad.

12. La economía de las personas afectadas también ha sido impactada por todos los gastos extraordinarios que deben hacer para atender su salud, implementar mecanismos de reubicación y adquirir nuevos dispositivos electrónicos.

Entre los afrontamientos encontrados están:

- Bajar el perfil en redes sociales, cambiar de rutinas, moverse en espacios distintos que tengan la sensación de control sobre lo sucedido y sus consecuencias.
- Refugiarse con sus familias representó conectarse con emociones de bienestar, un refuerzo de vínculos de apego y una sensación de estar fuera de peligro por un tiempo.
- El fortalecimiento de la red de apoyo con sus amistades o personas cercanas también fue un mecanismo de afrontamiento. La creación de redes para que se sintieran seguras.
- En lo grupal, también se crearon acciones conjuntas de denuncia, comunicados y conferencias de prensa. Lo que da seguridad a las personas y sentimiento de unidad y colectividad.
- En las organizaciones se han fortalecido o creado apoyos interinstitucionales proporcionando espacios de soporte, tanto tecnológico como psicológico para afrontar las consecuencias del software espía. Las personas se sienten más respaldadas y constituye, para ellas, un factor de afrontamiento muy importante.

# Recomendaciones

1. Trabajar con organizaciones de derechos humanos, periodistas y operadores de justicia para que puedan prevenir futuras intervenciones, para saber qué hacer y cómo enfrentar un ataque de software espía a través de la tecnología y la logística, con el propósito de que se sientan con un poco de control sobre las amenazas que viven, tomando también en cuenta la diferencia de género en las agresiones.
2. Proveer acompañamiento psicosocial y apoyo psicológico a las personas que sufren un ataque con software espía para abordar los niveles de ansiedad, miedo e hipervigilancia que llegan a sentir.
3. Se recomienda crear redes de apoyo con personas que han vivido situaciones similares y puedan asesorar desde la práctica cómo vivieron y sobrevivieron esta agresión. Las redes fortalecen vínculos sociales, sentimientos de pertenencia y mitigan la necesidad de generar aislamiento.
4. Facilitar apoyo psicosocial y formación en manejo de emociones para los equipos que trabajan con personas y organizaciones que han sufrido ataques con software espía.
5. Socializar y fortalecer la creación de fondos económicos para ofrecer a las personas dispositivos de comunicación seguros, logística si necesitan movilizarse o instalar sistemas de seguridad.
6. En casos extremo y, si las personas necesitan abandonar el país, que cuenten con recursos para garantizar la salida sus países y el establecimiento en otro lugar. También respaldo para procesos legales de migración.

7. Crear una red con otros profesionales que brinden asesoría jurídica en casos de criminalización.
  
8. Elaborar protocolos de actuación en casos de ataques con software espía para que sirvan de guía a las organizaciones que pueden sufrir este tipo de agresiones, que se tome en cuenta otras violencias que se infligen con la vigilancia.

# Bibliografía

Access Now. (2023, May 3). Estados: Frenen El Spyware Que Amenaza La Libertad de Prensa. Access Now.

<https://www.accessnow.org/press-release/declaracion-conjunta-spyware-libertad-de-prensa/>

Ahmad, Atif, et al. (2021, March 27). Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack.

<https://doi.org/10.48550/ARXIV.2103.15005>

Aluna Acompañamiento Psicosocial. (2022). Serie Claves hacia el acompañamiento psicosocial cuadernillo principal.

Aluna Acompañamiento Psicosocial. (2021). (2019 diciembre 3) Impactos psicosociales de la defensa de los derechos humanos sobre las mujeres defensoras. PBI México.

<https://pbi-mexico.org/es/noticias/impactos-psicosociales-de-la-defensa-de-los-derechos-humanos-sobre-las-mujeres-defensoras>

536db9\_ee2088f8bd1e4ff9a2a7f6d5eec4b372.pdf (usrfiles.com)

Amnistía Internacional. (2024, May 16). Thailand: State-backed digital violence used to silence women and LGBTI activists.

<https://www.amnesty.org/es/what-we-do/technology/online-violence/> -

<https://www.amnesty.org/en/latest/news/2024/05/thailand-state-backed-digital-violence-silence-women-lgbti-activists/>

Amnistía Internacional. (2023, diciembre 14). ¿Qué es software espía y qué podemos hacer para preservar la protección?

<https://www.amnesty.org/es/latest/campaigns/2023/12/what-is-spyware-and-what-you-can-do-to-stay-protected/>

Amnistía Internacional. (2023, octubre 9) Global: El escándalo de los 'Archivos Predator' revela ataques descarados con software espía contra la sociedad civil,

figuras políticas y altos cargos.

<https://www.amnesty.org/es/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/>

Bada, M. & Nurse, J. (2020). "The social and psychological impact of cyberattacks". En (Eds.) Vladlena Benson, John Mcalaney, *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 73-92). Academic Press.

<https://doi.org/10.1016/B978-0-12-816203-3.00004-6>Get rights and content

Barlow, D. H. y Durand, V. M. (2003): *Psicopatología*. Thomson.

Barrientos M., Najarro F. (2024, 26 de agosto). Prensa Libre. Brigada de Comunicaciones del Ejército cuidará el ciberespacio y espacio electromagnético. [https://www.prensalibre.com/guatemala/politica/brigada-de-comunicaciones-en-el-ejercito-cuidara-ciberespacio-y-espacio-electromagnetico/#google\\_vignette](https://www.prensalibre.com/guatemala/politica/brigada-de-comunicaciones-en-el-ejercito-cuidara-ciberespacio-y-espacio-electromagnetico/#google_vignette)

Beristain, C. M. (n.d.). Sobre perspectiva psicosocial en la investigación de derechos humanos. Corteidh.or.cr. Retrieved March 11, 2025, from <https://www.corteidh.or.cr/tablas/27117.pdf>

Beristain, C. (1999). *Reconstruir el tejido social. Un enfoque de ayuda humanitaria*. Icaria Antrazyt.

Bonifaz, Rafael. (2020). "Herramientas de Vigilancia Digital Identificadas en Centroamérica". Fundación Acceso. [https://www.acceso.or.cr/wp-content/uploads/2021/08/2020\\_Art\\_Herramientas\\_Vigilancia\\_CA-mayo2020.pdf](https://www.acceso.or.cr/wp-content/uploads/2021/08/2020_Art_Herramientas_Vigilancia_CA-mayo2020.pdf)

Budimir, S., Fontaine, J. R. J., & Roesch, E. B. (2021). "Emotional Experiences of Cybersecurity Breach Victims". *Cyberpsychology, Behavior and Social Networking*, 24(9), 612-616. <https://doi.org/10.1089/cyber.2020.0525>

CIDH (Comisión Interamericana de Derechos Humanos). (31 de enero de 2022). La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador. [Comunicado de prensa].

<https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp>

Comité de Derechos Humanos, Observación General No. 31, la índole de la obligación jurídica general impuesta a los Estados Parte en el Pacto, 80º período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 at 225 (2004). párr. 15. Declaración de la Alta Comisionada de la ONU para los Derechos Humanos, Michelle Bachelet, sobre el uso de software espía para vigilar periodistas y personas defensoras de derechos humanos | ONU-DH (hchr.org.mx)

Corte Interamericana de de Derechos Humanos. (1977). Caso Loayza Tamayo vs. Perú.

[https://corteidh.or.cr/docs/casos/articulos/seriec\\_33\\_esp.pdf](https://corteidh.or.cr/docs/casos/articulos/seriec_33_esp.pdf)

Duque, V. (2020). Hacia una cultura del buen trato y bienestar Promoviendo el autocuidado y cuidado de los equipos de trabajo. Jotay/ECAP.

ECAP (Equipo de Estudios Comunitarios y Atención Psicosocial). (2025). Módulo 5. Impactos individuales, familiares y colectivos de la violencia sociopolítica. Diplomado en Salud Mental Comunitaria. (n.d.). Org.gt.

Bonilla, D. y Reyes D. (12 de enero de 2022). In Brief: Pegasus Spying on El Faro. El Faro

(<http://elfaro.net/especial/in-brief-pegasus-spying-on-el-faro/>)

<https://ecapguatemala.org.gt/modulo-5-diplomado-en-salud-mental-comunitaria/>

Equipo de Acción Psicosocial y Acción Comunitaria. (2013). Reparar lo invisible:

Desafíos para una atención psicosocial transformadora. Ediciones Antropos.

Esteban, Ana. (2002). El desarraigo como vivencia del exilio y de la globalización. Open

Edition Journal.

FLACSO. (2017). Metodologías de investigación, búsqueda y atención a las víctimas. Del caso Ayotzinapa a nuevos mecanismos en la lucha contra la impunidad. Carlos M. Beristain, Alejandro Valencia V., Ángela Buitrago R., Francisco Cox V. (coords.). <https://www.flacso.edu.mx/libro/metodologias-de-investigacion-busqueda-y-atencion-a-las-victimas-del-caso-ayotzinapa-a-nuevos-mecanismos-en-la-lucha-contra-la-impunidad/>

Foucault, Michel. (2002). Vigilar y castigar, nacimiento de la prisión. Siglo XXI editores.

Freud, A. (1963). El yo y los mecanismos de defensa. Amorrortu.

Fundación Vía Libre. Módulo 4: Vigilancia estatal. "Curso online: Privacidad y vigilancia en entornos digitales"

<http://www.articaonline.com/wp-content/uploads/2016/01/Modulo-4-Privacidad.pdf>

Hiperderecho. (n.d.). Tecnoresistencias.

<https://hiperderecho.org/tecnoresistencias/identifica/>

Gómez, N. (2009). Peritaje Psicosocial por Violaciones a Derechos Humanos. ECAP.

ILAS (Instituto Latinoamericano de Salud Mental y Derechos Humanos). (1994).

Trauma Psicosocial y Adolescentes Latinoamericanos: Formas de Accionar Grupal.

LOM.

ILAS (Instituto Latinoamericano de Salud Mental y Derechos Humanos). (1989). Lira, Elizabeth; Becker, David; Castillo, Ma. Isabel et al. Derechos humanos: todo es según el dolor con que se mira. En

[https://ilas.cl/nuevo/wp-content/uploads/2021/11/Derechos-Humanos-Todo-Es-Segun-El-Dolor-Con-Que-Se-Mira-by-Lira-Elizabeth-z-lib.org\\_.pdf](https://ilas.cl/nuevo/wp-content/uploads/2021/11/Derechos-Humanos-Todo-Es-Segun-El-Dolor-Con-Que-Se-Mira-by-Lira-Elizabeth-z-lib.org_.pdf)

Kareem, Karwan. (30 de abril de 2024). A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security. arXiv, <https://doi.org/10.48550/ARXIV.2404.19677>

Kekre, Cardillo, Fisher. (2023). Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People. <https://www.graduateinstitute.ch/sites/internet/files/2024-01/ARP%20FINAL%20REPORT%20-%20Aditi%20Amol%20Kekre.pdf>

Kizza, J. M. (2023). Cyberbullying, Cyberstalking and Cyber Harassment. In: Ethical and Secure Computing. Undergraduate Topics in Computer Science. Springer, Cham. [https://doi.org/10.1007/978-3-031-31906-8\\_9](https://doi.org/10.1007/978-3-031-31906-8_9)

Kordon, D., y Edelman, L. (2005). Efectos psicológicos y psicosociales de la represión política y la impunidad: de la dictadura a la actualidad. Editorial Madres de Plaza de Mayo.

Lazarus, R.S., Valdés M., Manuel y Folkman, S. (1986). Estrés y procesos cognitivos. Martínez Roca.

Muñoz, B. (2023). (2022, January 27). Journalism in Latin America is Under Attack by Spyware. Wilson Center. <https://www.wilsoncenter.org/blog-post/journalism-latin-america-under-attack-spyware>

Nash Rojas, C. E. (2009). Alcance del concepto de tortura y otros tratos crueles, inhumanos y degradantes. Anuario de Derecho constitucional Latinoamericano pp. 585-601. <https://www.corteidh.or.cr/tablas/r23545.pdf>

Oliveira, P. (n.d.). Cybercrime Module 12 Key Issues: Cyberstalking and Cyberharassment. United Nations Office on Drugs and Crime.

<https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html>

Pen América. (2021 junio 15). Manual contra el acoso en línea. “Definir la violencia en línea: un glosario de términos”.

<https://onlineharassmentfieldmanual.pen.org/es/violencia-en-linea-glosario/>

Pérez, G. (2016). “Hacking Team Malware para la vigilancia en América Latina”.

Derechos digitales.

<https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf>

R3D: Red en Defensa de los Derechos Digitales. (2018, septiembre 22). Pegasus continúa operando en México, revela informe del Citizen Lab.

<https://r3d.mx/2018/09/21/pegasus-continua-operando-en-mexico-revela-informe-del-citizen-lab/>

Scott W., Joan. (1996). “El género: una categoría útil para el análisis histórico”, en Martha Lamas (Comp.) El género: La construcción cultural de la diferencia sexual. PUEG-UNAM. pp. 265-302.

Scott-Railton, John, et al. (2022 January 12) Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware. Citizen Lab Research Report No. 148, University of Toronto.

<https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/>

Scott-Railton, M., Razzak, A., Nigro, D. (2022, octubre 2). Identifican nuevos abusos del software espía Pegasus en México. The Citizen Lab.

<https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/>

Southwick, Natalie. (2023, June 5). Surveillance Technology Is on the Rise in Latin America. Americas Quarterly.  
<https://www.americasquarterly.org/article/surveillance-technology-is-on-the-rise-in-latin-america/>

UN News. (2023, March 14). Counter-Terrorism “rhetoric” Used to Justify Rise of Surveillance Technology: Human Rights Expert.  
<https://news.un.org/en/story/2023/03/1134552>

Van Der Kolk. (2020). El Cuerpo Lleva la cuenta, cerebro, mente y cuerpo en la superación del trauma. 3ra edición. Editorial Eleftheria.

Vázquez, C., Crespo M., J.M. (1998). “Estrategias de afrontamiento”. En Medición clínica y psiquiatría (pp. 425-435). Masson.  
<https://centrodocumentacion.psicosocial.net/wp-content/uploads/2004/01/c-vazquez-estrategias-de-afrontamiento.pdf>

