FUNDACIÓN Acceso

STUDY ON THE PSYCHOSOCIAL IMPACT OF AND COPING WITH DIGITAL ATTACKS

(SPECIFICALLY SPYWARE)

Author
Olga Paz, with significant contributions from Gabriela Vargas, Dennise Albornoz and Jacobo Mogollón Villar.

Coordination of research
Fundación Acceso

Original concept and methodological design
Fundación Acceso

Technical supervision and report review
Fundación Acceso, The Engine Room

Organization responsible for publication
Fundación Acceso

Special thanks to all interviewees for sharing their experiences, reflections and time, making it possible to prepare this study collectively.

Publication date
April 2025

Table of contents

Introduction

In the Latin American context, spying that targets human rights defenders, justice operators and journalists has been a systemic and historical practice. Fundación Acceso's report "Vigilancia en Centroamérica: Internet, privacidad y derechos humanos"[1] [Surveillance in Central America: Internet, Privacy and Human Rights] defines internet surveillance as the monitoring, collection and analysis of on-line data, conducted by both state and private actors. This surveillance paradigm includes the monitoring of activity on social media, tracking electronic communications and accessing personal information, often without the explicit consent of the people affected, or even without their knowledge.

These days, spy operations have been reconfigured and geared towards the identification and neutralization of social actors labelled as "internal enemies," thus furthering a counterinsurgency mentality of persecution that, in the second half of the 20th century, targeted sectors considered a threat to the status quo. During that period, authoritarian regimes in Latin America classified a wide range of actors as opposition figures, from insurgent organizations born in the heat of dictatorships, to social, religious, pro-democracy and anti-military movements, including human rights defenders.

In the 21st century, state structures with a history of applying surveillance and repression mechanisms have demonstrated great skill in adapting to the digital environment. Today they use advanced technology to infiltrate electronic devices, access confidential information and apply pressure on or intimidate individuals and collectives considered threats to those in power, be they institutional or linked to organized crime. The persistence of these practices reveals that, beyond the transformation in tools, there is a structural vision that interprets the defense of human

1 Fundación Acceso. (2020). Vigilancia en Centroamérica. https://www.acceso.or.cr/wp-content/uploads/2021/08/2020-Vigilancia-CA-28S.pdf

rights as a kind of political opposition. This perspective is supported by official statements that present these actions as necessary to "combat crime" and protect "national security."

However, reality demonstrates that surveillance technologies, and especially spyware, have been used mainly to persecute human rights defenders, spy on political opponents and harass journalists and activists.[2] In contexts where there are no adequate legal safeguards, spyware becomes a mechanism for repression that enables governments to maintain control over specific organizations or individuals. This practice puts these targets of spying in an extremely vulnerable situation, leaving their networks of contacts, their information sources and their working strategies exposed to sectors interested in disrupting their efforts and silencing their voices.

The ease of accessing sensitive data, the breadth and depth of the intrusion and the difficulty of detecting these operations sets the stage for spying that is increasingly becoming virtually undetectable. This escalation not only increases the likelihood of privacy and security violations, by exceeding any reasonable proportion, but it also creates new types of impact, including those that appear in the psychosocial arena. It is therefore essential to fully analyze the implications of these technologies, in both their technical aspects and their social and emotional impact.

The goal of this study is to analyze the impact of spyware as a tool for government surveillance in Latin America used against human rights defenders and journalists, who have been targeted by this intrusion. It seeks to examine how these technologies have effects that, beyond data and the digital realm, compromise the physical safety, health, economic and social well-being, and rights of the people affected.

Using an analysis of documented cases, we attempt to understand the specific psychosocial impacts, as well as kinds of individual and collective coping strategies.

---

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

Surveillance technologies (spyware)

Use of spyware as a tool for intelligence and state repression

The growing availability of advanced spy technologies has boosted the capacity of some governments to exercise systematic control over people they consider a threat to their power. In this context, the use of spyware has been consolidated as a key strategy, targeting specific objectives in an intelligence cycle that not only gathers information but also enables repression, intimidation and, in many cases, digital and physical harassment. This cycle operates on the prior selection of certain targets due to their political profile, their work defending human rights or their participation in organizations perceived to be a risk to the authorities. The implementation of these tools requires the participation of government structures with access to resources, technology and, often, direct or indirect support from actors with political and economic power.[3]

It is essential to distinguish among three practices: digital surveillance, spyware, and cyberattacks or cyber harassment. Each of these has particular characteristics that are related to the specific strategic uses of technology to achieve different ends, in addition to their scope, levels of intrusion and effects. Moreover, these practices can be applied in combination as elements of digital and even physical repression and intimidation tactics.[4]

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

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

Digital surveillance is the systematic monitoring of on-line activity, conducted by governments, companies or private actors, for purposes of political control and investigating structures and networks of people, both for commercial exploitation and data extraction, as well as for the identification, persecution and neutralization of "persons of interest."

Cyber harassment, on the other hand, is a pattern of abusive and aggressive behavior targeting an individual or group in the digital environment. It includes verbal attacks, defamation, threats, sexual harassment and the publication of personal information, real or fabricated, to intimidate or cause harm. Unlike digital surveillance, its main goal is to inflict emotional or psychological harm, or to damage the person's public image. However, these attacks are not limited to the individual; they are also used as a mechanism to affect specific collectives (such as women defenders, indigenous communities, LGBTIQ+ people and social organizations) with the aim of stigmatizing them, undermining their legitimacy and reinforcing their marginalization in public and political spaces.

Spyware is a type of malware specifically designed to be secretly installed on electronic devices with the intent to gather data with neither the knowledge nor consent of the people affected.

This kind of tool makes it possible to fully monitor digital activities, including access to encrypted communications; real-time geolocation; remote activation of microphones and cameras; and the extraction of files or sensitive credentials. Its implementation falls under intelligence operations, targeting individuals and entities considered to be strategic sources of data pertinent to the analysis of organizational dynamics, operational capacities and patterns of behavior, or network mapping. The goal is to inform decision-making processes, threat assessment and the design of actions for the control, neutralization or disruption of these actors. The information obtained via these intrusions can later be used to design and implement harassment, criminalization, extortion or

slander campaigns, as well as to facilitate other types of attacks, both in the digital environment and in physical, political or legal realms.[5] [6]

Characteristics of spyware-facilitated surveillance

Spyware is a worrying strategic evolution compared to traditional methods of intelligence gathering, due to its ability to operate with high levels of secrecy, persistence and accuracy. Unlike visible or invasive practices, such as interrogations, tapping, in-person tailing or searches, it facilitates access to critical information without alerting the target, minimizing the operational risks to the structure employing it.

This ability to operate with extreme discretion maximizes control within the intelligence cycle by sustaining prolonged, clandestine surveillance of individuals and organizations. This enables a constant detailed accumulation of information on internal dynamics, violating basic principles of privacy and opening the door to abuses of power that are difficult to detect or audit.[7]

Once the spyware is installed, its main goal is to maintain an undetected presence. For this, it uses zero-day exploits, which are bugs unknown to the software manufacturers that are as yet unresolved. In many cases, the infiltration happens without the user having taken any action (zero-click attacks), which makes it especially dangerous. Likewise, these programs use sophisticated evasive measures, hiding in legitimate system processes, erasing activity logs and avoiding detection by antivirus or security-monitoring tools.[8]

In addition, spyware use represents a serious violation of fundamental rights and of the surveillance targets' overall well-being. Its effects are not neutral: they reproduce and exacerbate preexisting structural inequalities.

---

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

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

When they target women, LGBTIQ+ people or historically marginalized collectives, they take on specific characteristics that go beyond the impact on privacy. Extracted information can be exploited for blackmail, retaliation or smear campaigns that reinforce hate speech and violent practices based on stereotypes of gender, sexual orientation, identity or expression.[9]

Use of spyware by governments in Latin America

Globally, more and more governments are procuring spyware on the grounds of fighting crime and terrorism.[10] However, investigations have shown that these technologies are used, mainly, to spy on journalists, activists and political figures. An Amnesty International report from 2023 revealed that Predator spyware had been used to spy on UN officials, United States senators and women heads of parliament.[11]

In Latin America, government interest in these technologies has been on the rise. A 2016 study documented the acquisition of Hacking Team spyware (marketed as Galileo or DaVinci) by Brazil, Chile, Colombia, Ecuador, Honduras, Mexico and Panama. This software, originally promoted "for fighting crime," has been primarily used to spy on human rights defenders, exposing them to harassment, threats and coordinated attacks.[12]

Spyware use is not only a latent threat, but also part of a broader intimidation and control strategy. In El Salvador, under Nayib Bukele's administration, journalists from El Faro digital news media were victims of Pegasus attacks from 2020 to 2021. Forensic analysis by The Citizen Lab together with Access Now shows that, starting on June 26, 2020, members

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

10 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

11 Amnistía Internacional. (2023, March 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/

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

of El Faro suffered at least 226 Pegasus attacks.[13] [14] The seriousness of the case spurred the Inter-American Commission on Human Rights to express their support for the media outlet and condemn "[a]ll instances of communications device tapping" that is not "backed by a transparent legal framework and compl[ies] with international human rights standards, as well as ensuring respect for the principles of necessity, proportionality[.]"[15]

In Mexico, the use of Pegasus has been widely documented. Investigations in 2017 by The Citizen Lab, R3D, SocialTIC and Article 19 exposed attacks targeting journalists, lawye rs, legislators and anti-corruption activists.[16] From 2019 to 2021, new forensic investigations conducted by R3D and The Citizen Lab confirmed Pegasus infections on the devices of journalists and human rights defenders via "zero-click" attacks that require no interaction from the people subject to infiltration. The evidence documented the systematic use of this spyware against members of Mexican civil society, confirming the pattern of surveillance for the purposes of repression and intimidation in the country.[17]

Despite this evidence, spyware regulation is still lacking in most countries in the region. Investigations have confirmed the use of malware in Honduras and Guatemala, among other countries, with no effective legal protection, oversight or accountability mechanisms.[18]

---

13 Bonilla, D. & 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, January 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. [Press release]. https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

16 Scott-Railton, M., Razzak, A., Nigro, D. (2022, October 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/

17 R3D: Red en Defensa de los Derechos Digitales. (2018, September 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/

18 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

The psychosocial effects of spyware

To understand the psychosocial dimension of spyware's effects, we will start by understanding the psychosocial approach. This is not simply a combination of the psychological and the social, but rather a holistic perspective that makes it possible to understand how social processes affect people and how they process, resist or reproduce these effects in their lives (Beristain, 2006, p. 30).[19] This perspective leads us to identify how traumatic experiences have an individual and a collective effect, with impacts on identity, life plans, collective memory and social rebuilding processes.

When facing the different types of impact caused by situations of violence or rights violations, people—both individually and collectively—activate a range of responses that enable them to resist, adapt and assign meaning to the experience. In this context, coping is understood as the set of cognitive, emotional and behavioral strategies used in an attempt to manage the stress and emotions linked to the adversity, thus favoring processes for resilience and restoring the social fabric.

Spyware attacks have consequences. According to the study "Emotional Experiences of Cybersecurity Breach Victims," the people spied upon described how anger, sadness and insecurity are linked to cybersecurity attacks. A common reaction was paranoia, the constant feeling of being monitored. Paranoia affects one's ability to trust the environment. The study documents how these attacks can lead to depression due to the invasion of privacy; further, the lack of control over one's own information leads to hopelessness.[20]

---

19 Beristain, 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

Another study, “Targeting, Infecting, Surveilling, Harming,” conducted in 2023, defines cyberharm as the damaging consequence of an event that affects an individual’s well-being. It shows that people suffer serious psychological harm, especially fear, anxiety, insecurity, feelings of paranoia, loss of trust and isolation.[21] Reports on surveillance also document that people censor themselves out of fear. Journalists and human rights defenders play an indispensable role in our societies and when they are silenced, close social circles are affected.[22] Another impact can be social isolation, due to which those affected can become more distant from others, fearing that their communications may be infiltrated.[23]

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

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).

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

Methodology

This study attempts to understand psychosocial impacts covering family, work and economic dimensions, as well as the coping strategies that were implemented to face these effects.

To this end, a qualitative method[24] was used based on five individual interviews and one group interview with two experts in cybersecurity and digital protection, in order to explore the experiences of people who have faced spyware surveillance situations.

Semi-structured interviews were designed for the individuals and for the group. The interviews were conducted virtually using the meet.greenhost.net platform. A safe, confidential environment was provided.

In each interview, the participants recounted the events they experienced and shared their personal reflections on how these events affected their lives. These interviews were conducted from September 11 to 22, 2024.

The interviews were anonymous and are shared in the present document in a coded manner. The individuals are journalists or lawyers who work in the area of human rights defense, and their names in this report are fictitious. All the interviewees signed an informed consent agreement that ensures anonymity and privacy.

A group interview was conducted with two experts in digital accompaniment and protection. They reported on the cases they have handled anonymously and confidentially. The cases the experts usually handle come to them via previously established organizational ties or through referrals from partner organizations.

---

24 Qualitative approach, an appropriate approach due to its ability to examine complexities and processes in depth and to explore lesser known phenomena. Marshall & Rossman. (1999). Designing qualitative research, p. 57. (3rd ed.). Sage.

Investigation results

Below, the main results are presented under different headings. The first section refers to the characteristics of spyware surveillance from the perspective of the people affected. The second section addresses the primary psychosocial impacts. Finally, in the third section, the main types of coping strategies found in the interviews are described.

Characteristics of spyware attacks

a) Spyware use seeks social control and censorship

According to the interviewees, the goal of installing spyware goes beyond surveillance. They believe that the purpose is control, fostering a sense of vulnerability, and threatening and intimidating people for the work they do. A specialist who participated in the group interviews states that our telephones are an extension of ourselves, holding all our information:

> "Telephones are a very important extension of ourselves. Socially, people usually use them 24/7. They have contacts, conversations, photos, videos, and locations on them. If this information falls int o the hands of malicious people, it has implications for physical safety, especially for journalists who publish things on corruption that make direct accusations, obviously, risks of threats to the person." (Group interview participant).

One interviewee mentions that she experiences surveillance as if she were inside Foucault's panopticon. The concept of panopticon in Michel Foucault's theory refers to a model of surveillance and social control inspired by the architectural design of the Panopticon, created by Jeremy Bentham. This enabled a guard to observe all prisoners without their knowing whether they were being watched. For him, it is a metaphor for modern power and of how disciplinary societies exercise control over

individuals. The central idea is that the possibility of being watched leads a person to self-regulate their behavior, fostering conformity and obedience (Foucault 2002, p. 202).

> "The constant sense of being always watched like Foucault and the panopticon. I lived my whole 20's like this, like at the time I would think, it's not like that, but the thought was always there." (E5).

She adds:

> "When I turned 21, one of the President's advisors published my live location, here are all [institution name] in case you want to come give them a present. I was with my 21-year-old friends. I was also with colleagues from the newspaper, so I thought, they are putting my friends at risk." (E5).

The panopticon fulfills its purpose when people start to self-regulate and self-censor:

> "Yes, I've been really afraid, I have self-censored, because I often think that what I might say, what I wrote or what I think can cause problems for me, it's going to lead to being followed and that kind of thing. I'm walking down the street, I go out for a walk, I take my car out, and I'm always thinking that someone could be tailing me. I'm thinking that someone is watching me, very often. If the computer slows down or if the phone often heats up, I think that there is someone trying to access my devices to know what I'm doing." (E4).

Another interviewee refers to control:

> "The name of the software includes the word 'spy', but the goal is control, not spying." (E2).

b) Spyware as a tool for state surveillance

The people were infected apparently because they were working on projects that bothered the government; so, spyware was installed on them to monitor relationships, movements, contacts and communications:

> "Because the cases I saw of journalists and human rights, if you look at the kind of infection, all the cases coincide with times where they were working with government counterparts or government cases that were going to have a negative impact, and the government has conducted spying." (E2).

For other interviewees, the government wanted to know who their sources[25] were for the information they published:

> "What they were looking for [was] to have an idea about our lives. They were on our phones all day, this let them know our movements and I think that what they were most interested in was knowing what our sources were sharing with us and what information we had or what calls we were making." (E3).

There is no doubt that the work done by these journalists has been highly significant for certain sectors that end up paying large sums of money to become familiar with the smallest details of journalism. As the interviewee explains:

> "This surveillance is very expensive. We understand that each license costs around 50,000 dollars; we understand that the software they install on us has very high costs given the ability it has for infiltration." (E4).

It also leads to discrediting these people with accusations that can affect their integrity, in addition to treating them as enemies of the state:

---

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

> “The government produces rhetoric against communicators concurrently, they would fabricate narratives, smokescreens to steer the rhetoric, to take back control of the rhetoric. When a scandalous news item comes out—for example, the negotiation with gangs—then what the government does is to publish some news, for example, falsely accusing... of rape or accusing a female journalist of getting benefits in exchange for sexual favors. It distracts public opinion.” (E2).

It is important to keep in mind that the attacks come from very powerful people:

> “You have to take into account that the surveillance comes from extremely violent groups, like the military, organized crime gangs that also make death threats.” (Interview with experts).

In conclusion, installing spyware is a kind of attack that seeks control over different facets of people and the social groups to which they belong. People feel spied on, and they develop psychosocial effects like stress, fatigue, hypervigilance, lack of understanding of what is happening to them and a rupture in life plans.

c) The interrelationship between spyware and physical or digital violence

The surveillance in the cases studied has been a strategy within other kinds of attack used against the interviewees, their organizations or the groups to which they belong. This kind of surveillance occurs alongside other attacks such as physical surveillance, threats, imprisonment, criminalization, slander and violence on social media:

> "One of my colleagues was arrested, so we were really affected by his arrest because since we were stating opinions, they arrested him suspiciously with no due process. This has had an impact because we realized it could really happen." (E1).

It is important to highlight how the spying attacks come on top of other difficult experiences that they have had due to the nature of their work, such as facing violence, death and disappearance every day:

> "It is like the trauma piñata broke open, because on the last trip when I was going [to my country], I would say: here I saw a dead person, here is where I went when they killed someone else, this is the house they burned when they killed so-and-so. The last reporting I did... was when they killed two people and they removed them from the neighborhood where I grew up. When I saw that a girl my age disappeared in the neighborhood where I was walking every day, that's when I decided to emigrate." (E5).

Another interviewee told of how on-line surveillance is paired with physical surveillance:

> "Over the course of several months I started to see physical surveillance in my neighborhood, which was very unusual because it's a neighborhood where only elderly people, families live, a neighborhood where hardly anyone lives. I started to see unusual people taking photos of the houses in the area or making rounds, unfamiliar private cars parked, patrol cars." (E2).

Another adds:

> “I know that in the end, spying was a part of another set of situations that led me to take a leave of absence from work for about two months, so that I could receive treatment.” (E3).

One woman interviewed explained the difference between physical surveillance and spyware surveillance:

> “In non-digital surveillance, it’s possible to have warnings or for us to detect it. Internet surveillance is imperceptible and invasive, since we deal with things from our private life on our cell phones and there are more channels where they can spy on us. It can be done anonymously; they can get access to other kinds of information on our life. It breeds impunity.” (E1).

Since spyware surveillance is imperceptible and invasive, people feel watched, but above all monitored all the time. Eventually they question their profession and the values they have invested in their career; they censor and silence themselves.

Psychological and psychosocial impacts

The effects of spyware attacks, in combination with other attacks, are wide ranging and expressed in both psychological and psychosocial dimensions.

Understanding the depth of harm caused to people and communities requires distinguishing between the psychological and psychosocial dimensions of the impact. This differentiation, proposed by Elizabeth Lire (2017), is essential for comprehensively addressing the after-effects of repression and human rights violations. While psychological impacts are expressed through individual symptoms like fear, anxiety and trauma, psychosocial impacts allude to a broader effect that seeps into collective trust, community life, bonds and social memory.

a. Psychological impacts

1.- Panic

The impact first leads the person to a state of incredulity or shock; they do not know how to react and they feel overwhelmed or even panic. This causes them to isolate themselves or become paralyzed, in contrast to fear, which can produce a more intense and disorganized reaction.[26] According to the interview conducted with one of the experts, people enter into panic:

> "Total panic, if a person has the idea that this is happening, well it's total panic. Most of the time people don't even know what to do, it's a situation where, generally speaking, people are not prepared for it." (Group interview).

> "It is so important to focus during the first hours when we receive the spying because these first hours were the ones that most generated emotional overload. We must learn to manage it." (E3).

One woman interviewed explained:

> "Being there with so many things happening to us, with the stress, makes it difficult for us to make another kind of decision

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

> that in a normal state wouldn't be that difficult. But for me with my knowledge of security measures, I felt blocked. In those moments I didn't even want to deal with it, even just thinking about it stressed me out." (E1).

She adds:

> "What you usually do is isolate yourself, isolate yourself and/or freeze, get paralyzed, not knowing what to do." (E1).

2.- Normalization of violence

As a defense mechanism, others tend to normalize the situation; they see the attack as something that could happen and did happen:

> "Violence tends to become something natural in contexts where it has become an everyday event, where it has lost its exceptional nature. This naturalization involves a passive or resigned acceptance and produces an emotionally anesthetic effect that blocks empathy, indignation and the possibility of acting." (Beristain, 2010, p. 58).[27]

Because they work in media, they know that they run risks and that they can be persecuted and imprisoned. To survive in these conditions there is a kind of normalization of digital violence:

> "Normalization tells you, well, I know that they can kill me. Among journalists the risk profile is higher, I'm at the mercy of being the victim in this situation like [being resigned to it]." (Group interview).

Although it is normalized, we know that people should not live with this constant fear:

---

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.eus/publications/233

> “It gets normalized. But outside there are millions of people who live without fear and that is normal.” (E5).

What could work as a defense mechanism is “denial” which consists of refusing to accept reality for fear that it could be painful. This might be useful at first, but it can interfere with a healthy emotional life.[28]

3. Hypervigilance

The interviewees talked about entering a stage of hypervigilance that exhausts them, because they are on alert all the time. Hypervigilance is a state of extreme alertness. People in this state are constantly on the alert for potential threats and dangers. It is also a symptom of post-traumatic stress disorder (PTSD). It is paired with anxiety and it affects the ability to concentrate, which has consequences for job performance and social relationships. Being in a state of alert produces physical and mental exhaustion. Likewise, hypervigilant people may avoid visiting places or people, which leads them to become isolated.[29]

> “A feeling of hypervigilance, but you already knew that would happen, there is a cascade of emotions, first frustration and disappointment. It’s one thing to say, I knew it could happen, and it’s another to see, here it is.” (Group interview).

> “Hypervigilance, changing streets, the most complicated, avoiding main paths, driving through neighborhoods. I practically didn’t leave home, mostly taking precautions that most people wouldn’t use, that wouldn’t even occur to them.” (E2).

---

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/

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

4. Recurring thoughts

Recurring thoughts are ideas or images that repeatedly run through the mind over and over. They can be involuntary and they are often linked to anxiety and stress or related to PTSD. They may also interfere with the ability to concentrate or in daily life.[30]

People start a process of self-doubt, asking themselves: What did I do? They start to have repetitive thoughts about the data that could possibly have been obtained from their devices and how this could be used against them:

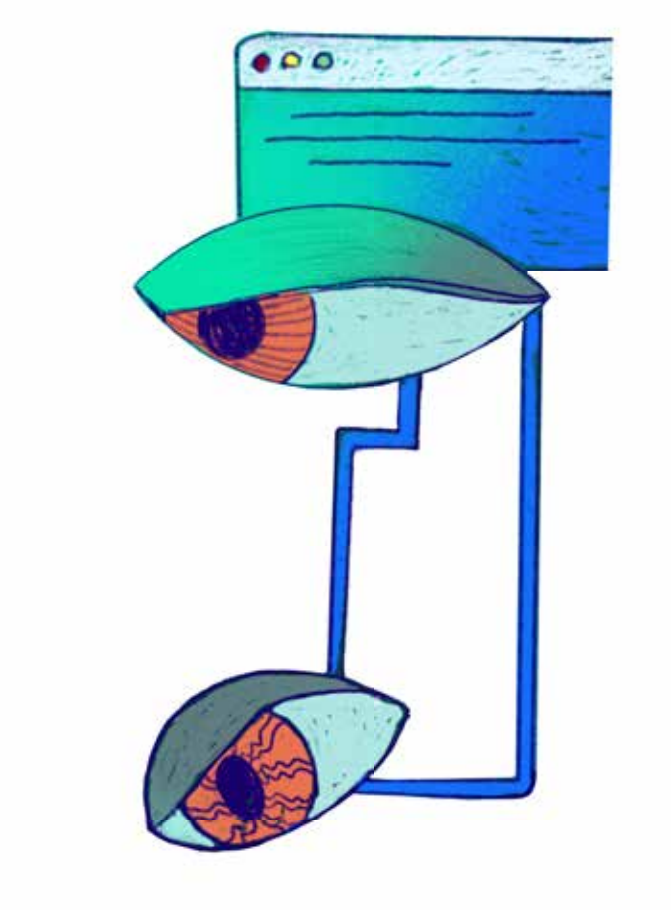
> *"Then the questions start about what they found out about my partner, my children. There is also a deep sense of anger, of frustration with impunity, because there's nothing new about governments spying, so cases are coming out and things don't change. It's a feeling of impotence in the face of impunity."* (Group interview).

Recurring thoughts also constantly create scenarios about what could happen now that they have the information:

> "You create scenarios in your head because you're sure about the information they have." (E5).

Everyone interviewed said that they have suffered from recurring thoughts since they found out about the spyware being installed. Interviewees with recurring thoughts also suffer from anxiety and sleep disturbance.

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



5. Anxiety

The interviewees showed different responses to anxiety that significantly interfere with daily activities. This is a reaction to threatening events and is characterized by excessive, persistent worry accompanied by symptoms such as clenched muscles, palpitations, breathing difficulties and sleep disorders. The interviewees mentioned how surveillance can make anxiety chronic or more intense.

> “I had a couple of anxiety attacks, this feeling of hyperventilati ng with chest pain.” (E2).

> “Anxiety, yes, I was on constant alert. In those periods when I found out that surveillance was being conducted on me, what it produced in me is insomnia, stress. It has triggered or intensified the anxiety that I had been feeling since the quarantine. The pandemic left me with an anxiety disorder, but then I found out about the surveillance against me and this ended up intensifying or making me lose ground in the work

> that I was doing to fight the anxiety and insomnia, also for the state of being on alert." (E1).

When this interviewee understood what the installation of spyware entailed, her anxiety increased:

> "This overwhelmed us because we ended up with very high levels of anxiety when they explained what Pegasus is and understood its reach." (E3).

> "I was diagnosed with a lot of anxiety, but they still hadn't given me the go ahead to talk about the issue, so I just keep accumulating and accumulating until the pressure cooker explodes, and it was the following year that I decided to take a break from work." (E3).

The interviewees, when they find out that they are being spied on, mention that the anxiety they had felt for other earlier events in their lives has increased, even leading to panic attacks.

6. Sleep disturbances

Sleep disturbances can be a type of response to these experiences, stemming from high levels of anxiety or anguish. They may include insomnia, persistent difficulty in falling asleep; or the opposite, feeling permanently sleepy; waking at unusual times; or, simply, changes in the rhythm of sleep itself:
"Insomnia, I have always had insomnia problems. In those years I had insomnia and it intensified a lot in those days, to where I could only sleep due to fatigue, the body won't do it even out of necessity." (E2).

Another woman interviewed also talked about nightmares:

> "The anxiety turned into intense dreams, I would dream that I was being chased or that they were arresting me, I would dream that my friends were in danger." (E3).

This person living in exile suffers from nightmares, and the anxiety increases when she returns to her country. For example, she thinks that they could put her in jail for failing to pay taxes:

> "I have spent years with nightmares [of my country] and when I have gone secretly, I have a terrible time, really bad. I'm checking to make sure I don't owe any taxes, if they are going to put me in jail over 5 dollars. I never tell my friends the date I'll be arriving, I let my mother know with a phone call, I never tell her when I'm arriving." (E5).

7. Depression

Two of the interviewees talked about suffering from depression. In contexts of socio-political violence, the depression response takes different forms: feelings of sadness, wanting to cry, discomfort and irritability, isolation, listlessness, sleeping problems, self-criticism, pessimism.[31]

In some cases, this depression had developed based on prior situations; however, it gets reactivated by the surveillance:

> "I was depressed in the last few months because of things I suffered in childhood, I think that all these situations also caused it." (E4).

> "Problems with depression... following that diagnosis I was prescribed depression medication." (E2).

> "In my case, due to anxiety or insomnia, due to depression, there were days when I didn't want to do anything." (E1).

The interviewees experienced several of these responses. Life changed them, and the impact has affected the areas of family, social relationships and work.

---

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. https://www.graduateinstitute.ch/sites/internet/files/2024-01/ARP%20FINAL%20REPORT%20-%20Aditi%20Amol%20Kekre.pdf

8. Fear

Three of the people interviewed talked about feeling fear. According to Elizabeth Lira, fear can trigger specific behaviors that could be described as adaptive processes in the face of threatening situations. The experience of permanent difficulty and risk in facing daily life subjectively affects the person and their way of perceiving both themselves and their environment. Fear could become permanent, especially if the circumstances perceived as life threatening become chronic.

Fear has caused people to censor themselves:

> "Yes, I've been really afraid, self-censorship, because I often think that what I might say, what I wrote or what I think, can cause problems for me, it's going to lead to being followed and that kind of thing." (E4).

Or they avoid engaging in activities that previously they would normally do:

> "I no longer wanted to talk on the phone, because I was afraid." (E5).

Fear is also caused by the possibility of their family members suffering attacks:

> "I had a few projects for doing a podcast. When my wife and son returned [to our country of origin], I gave up out of fear. Although I'm here [in exile], they are there and they are an easy target, going after my father, my sisters and my son or my wife." (E2).

Although this person has already been outside the country for over two years, the worries have not decreased. She feels fear and anguish; she feels threatened and thinks that the government can still hurt her. She

suffers from a general feeling of insecurity that causes her constant fear. For example:

> "Recently I had to go to the consulate [of her country] to renew my passport, here where I'm living. I was crying at the consulate, because I had to write down my address and my current telephone number. It's a normal procedure, and I know that nobody at the consulate wants to do anything to me. The public faces of the newspaper are others, but that doesn't mean that I didn't feel afraid by being there." (E5).
>
> "I don't think it's normal or healthy for someone to start crying while renewing a passport." (E5).

Although fear is an emotion caused by the perception of danger, a reaction that warns of a threat, it activates reactions like fight, freeze or flight. The problem for the interviewees is that with spyware, they are not clear who is behind the threat.

9. Effects on the body and health

The people interviewed also talked about health problems, body pain and health problems that could become chronic, such as colitis, headaches and neck pain. Van Der Kolk, who is conducting a long investigation into the signs of trauma in emotions and the body, explains that there is a relationship between the psychological impact of stress and trauma and the effect on the body, arguing that we operate holistically, mind and body.[32]

These effects on the body were already there, but the surveillance and other related types of violence have developed them further. As this person explains:

---

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.

> "Before, I suffered from irritable bowel syndrome for a long time; however, with this whole mess, the colitis came back. Then I have had eating problems that stem from mental health." (E2).

> "Body pain, headache, numbness in the face, I've been taking medications." (E4).

> "It was causing a bigger problem in my back and in my neck. I was diagnosed with neck pain and neck dislocation. They did several studies on me because they wanted to rule out arthritis problems. The psychiatrist told me that I have somatic symptom disorder because I somatize part of the problems that surround me." (E3).

b. Psychosocial impacts

1. Social isolation

This kind of impact is one of the most significant for psychosocial harm. It prevents the collective definition of suffering, heightens fear, and blocks recovery and social fabric reconstruction processes.[33]

All the interviewees spoke of a general feeling of insecurity that triggers avoidance of places and people. This has repercussions for social support because they tend to isolate themselves from people who could provide comfort and solidarity:

> "I cannot visit places that I used to go to or feel completely free and at peace. Now there is a kind of paranoia of monitoring who is around, who is listening to us, the feeling that I can talk fully on my phone." (E1).

Because having suffered a spyware attack is sensitive and to avoid putting the people they relate to at risk, such as contacts, family or sources, they

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

have been advised not to talk about the incident. However, this means they are unable to start a process of emotional discharge and building healthy ties:

> "It was hard because they had given us recommendations that we couldn't talk to anyone, so at first we were just those of us there, a very small group who knew. But then we found out, along with my partner, that it was something that was too big for us. I know that in the end the spying is part of another set of situations that produced a lot of anxiety, but this was the last straw that led me to take a leave of absence from work, for around two months, so I could receive treatment." (E1).

Likewise, leisure spaces are also affected. For example, a group of journalists has decided to take precautions in their behavior when they go out in public:

> "We always have to behave like journalists, it's a really terrible situation and we cannot behave like a normal person. The fact that something as basic as having a glass of wine or taking a car, although it's allowed, we have been warned not to drive with even one drop of alcohol in our body, no behavior that could compromise our integrity or that could lead to a wave of propaganda against us." (E4).

2. Life plans

A "life plan" corresponds to a person's holistic development, taking into account their vocation, skills, circumstances, potential and aspirations, and enabling them to reasonably set and achieve certain expectations.[34] Psychosocial impact includes disruption of future life goals, i.e., the impossibility of continuing the plans, dreams and ties that gave life meaning.[35]

---

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.eus/publications/233

In the interviews, different levels of impact on life plans can be seen. In terms of work, three people left their jobs and two suffered separations when they went into exile, which meant leaving their family and friends. They left behind their land, their customs and their homes.

Throughout life, people have long-term goals and expectations in accordance with their possibilities for holistic development. An example of how life plans are affected is shown by this interviewee. She explains that during the years she dedicated herself to work, she could not do the things that people of her age do; she worked, but her entire personal life subject to threats from the government:

> "I didn't want to be linked to [work]. I gave 20 years to journalism, and I thought, wow, there are a lot of things that I haven't experienced at that stage, and there are ton of things that I have experienced that I shouldn't have had to live through at that stage." (E5).

The life plan becomes their greatest vulnerability; their profession means that they can ultimately suffer attacks, surveillance and control:

> "A lot of feelings of loneliness and also the fact that the work we do is now devalued and has lost all meaning. I'm doing a job that practically does no good because they disparage it, such that, it's really serious. I think that's a kind of loneliness, imagining that you're in a job that isn't worth much, so you feel abandoned." (E4).

One of the people interviewed began to work at age 19 at a newspaper on human rights issues. Later, they dedicated themself to topics on historical memory, gender-based violence and human rights. Under Nayib Bukele's government, the suspicions, tailing and threats on social media began. In September 2021, they received a message on their phone that said it had spyware, and then they confirmed that it had been infected with Pegasus.

The impact was huge and on different dimensions of life:

> "I don't publish that much on social media. I left my job; there were a lot of factors for why I left, and I went on to do a more behind-the-scenes job. The internal factors also had influence, but the state spying was the straw that broke the camel's back. I said, nothing is left for me here. Knowing that they not only have my information, but also my family's information, my mom's, my nieces' and nephews'. My mom didn't want to talk on the phone anymore because she was afraid." (E5).

> "A complete lack of freedom and of feeling safe. Getting the confirmation was the worst, despite the fact that I already had doubts." (E5).

Exile is one of the factors that most affects the life plan: the change of country, culture and language, the loss of daily life, of being close to family, all these aspects mean that people have to reinvent themselves and, in one case, completely change professions.

Two of the people interviewed live in exile, which has entailed a very high cost to their finances and, on an emotional level, new challenges due to the uprooting and separation from family. Although in exile it is possible to have more certainty around personal safety, other things are lost that give meaning to life, such as family relationships, friendships and spaces for relating in general.

Exile and displacement from their places of origin can have the most impact on life plans for people who are forced to abandon their home and family environment. They can experience a series of emotions such as loss of connection with others, uncertainty and lack of control over the future, separation from loved ones and adaptation to a new environment. People in exile often feel deep nostalgia for their home and former life.[36]

---

36 These are the consequences on the interviewees' emotions and mental state from the experience of attacks and living through them.

3. Family

In general, families live in the same contexts as the people affected, so they know the risks their family members face in the course of their work as defenders or journalists.

Family suffers due to the attacks that the defenders and journalists are experiencing. In their desire to protect them, they ask them to abandon their life plan. This means they prefer keeping silent in the family space, thus increasing isolation and feelings of loneliness:

> "In terms of family, I felt somewhat alone because what I would have wanted was a little more support and what I received from them was scolding. It was an invitation to censor myself, so in that regard, I did feel alone, obliged not to talk about any old thing with any person for fear that it would come back to haunt me, expressing opinions, and I experienced the same situation with my friends." (E1).

For people who experience a spy attack, the suffering of family or of close contacts was a source of anxiety and an additional source of stress, leading to the decision to distance themselves:

> "I became distant from my friends, I got distant from my family, I moved house, it was a really stressful time because I had to make several changes at a personal level, with my family, not really professionally, although I did adopt security measures." (E1).

Friends and family members also keep their distance for fear of being subject to surveillance and its consequences:

> "There has been social isolation due t o the widespread fear that exists. You see that there is a kind of rejection, and you can see it, a lot of people want to keep their distance." (E4).

As a result of this distancing, the social circle shrinks down to the people with whom they share a work or activist relationship:

> "The distance is felt, so the only thing we can do is to have more social relationships with our colleagues." (E4).

However, there are other families who can offer comfort and support to the people surveilled, precisely because they are disconnected from civil society contexts.

Families can also be affected by the separations, especially by exile.

4. Gender-based impact

The interviews pointed us to attacks that clearly contained gender-based violence targeting women defenders. As noted in the Amnesty International investigation, spyware attacks targeting people from the LGBTIQ+ community also involve differentiated risk.[37] When we talk about violent content with gender-based discrimination, the most prevalent are stereotypes of women with machista content, discourses that have historically been used against women, such as disparaging them by calling them "whores" or exercising sexual violence.

The women interviewed say that the attacks against them have violent sexual content. This harassment involves attacks on social media and rhetoric that, generally, is geared towards manufacturing consensus around gender stereotypes:

> "The attacks on women are sexual in nature and, in general, women activists have suffered more sexual attacks." (E1).

Another woman interviewed commented:

> "Even when they attack us, they discriminate against us. Men can put up with being [called] fools or stupid, but no one says

37 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

> to them, I'm going to rape you—these are things that happen to women." (E5).

The objective of the violence against women exercised on social media is to paralyze them and use aspects of their sexuality or their physical appearance to attack them. The purpose is also to undermine their reputation and threaten them with rape and murder:

> "The attacks are aggressive, but often the reaction to these attacks can be very cruel when a woman is involved, because what they want is to destroy the person such that they feel at risk and attacked." (E3).

The attacks seek to paralyze the women for daring to enter a public sphere historically reserved for men; in addition, the attacks attempt to discredit them for being women and not due to their work.

5. Work teams and work environment

Spyware has different effects, like fear, overload and fatigue, on work teams. When people break the silence, daring to talk about it can trigger a chain reaction of panic that could persist over time, changing how the organizations operate:

> "In an organization, the first thing that is done is to talk about it, and that is going to trigger a chain reaction of panic, of how they compromised this person and I worked with this person two days ago, so, that leads to people feeling insecure." (Group interview).

It produces distrust on work teams. The reality of the surveillance changes the basic trust people have within the organizations:

> "This has long-term effects, long-lasting. There is work that has to be done afterwards to raise awareness about how technology works, because the foundations on which the organizations were basing their work are crumbling." (Group interview).

Another factor affecting the work team is fatigue; work has to be done every day, but with new security and care actions. This results in fatigue on the teams:

> "Everyone is handling it like an inertia, we're tired, you can see the team's fatigue. We're dealing with work but also, with this situation, thinking that today they're attacking one person, today they could be spying in this way, so... [In these circumstances,] how can you discuss security norms?
>
> Security is prioritized in a society where you should be thinking about how to do your job better." (E4).

Likewise, there is an economic impact on work teams. There is concern, for one interviewee, about the extra expenses that the organization that hired him will have to take on:

> "In terms of [my job], it has had different effects. They [his organization] have an economic burden related to hiring me. By hiring a [local] person, they wouldn't have to pay for an immigration lawyer." (E2).

There is also fear that the organization could suffer new attacks, as a media impact:

> "By hiring someone who has been a victim, first, they are exposed to, if my device were hacked, the work conversation [may become known]. In the end, having work conversations is inevitable. On the other hand, with the data or the physical surveillance the government collects, they would have a media impact." (E2).

Another interviewee talked about a temporary paralysis on the work teams:

> "There is a temporary paralysis, especially when the initial

analysis wraps up because, generally, when there is a person spied on, first you have to do the analysis of the impact's reach. You have to identify which other actors were compromised within the organization." (Group interview).

Regarding work performance, people expressed that they are unable to concentrate like they used to and that they must spend work time on their psychological well-being:

"In addition, it does have some impact on my job performance. They not only took years off my life and usefulness, but I have also had situations in which my performance is not the best, not even adequate, because I'm weighed down by all this, there is no way that either my organization or I could get rid of it. I can't avoid having the government persecute me, I cannot on my own resolve all the mental health problems that have arisen or gotten worse because of this situation, so this also puts pressure on me to try to stay sane." (E2).

"I feel that unlike five years ago, my performance, production, has dropped. You invest time in getting better, in recovery, and you put aside everything else that you do at work. After this I have focused on addressing my personal problems. It's not because it's easier, but things have come up that you don't know how to control." (E4).

Another impact is that on teams that respond to people and organizations that were infected, they can also be affected when they provide technical assistance for confronting the situation.

One specialist interviewed said that they receive psycho-emotional support:

"There are things that are beyond our control. Sometimes there have been cases where we were spied on and these scenarios are more stressful and we must have mechanisms in case there

> is someone who needs it. From our donors we have a rapid response fund to support these situations." (Group interview).

He adds:

> "Empathy burnout. The risks must be made visible to people who have recently joined this work. They can suffer burnout, empathy burnout, it's important to emphasize." (Group interview).

The work teams suffer effects that involve mistrust, fatigue and insecurity. There is also an economic and logistical impact: they must readjust their finances and organizational processes, as well as seeking psychological and technical support on security aspects.

6. Economic impact

The economy of the affected people has also felt impact because of all the extra expenses they must incur for their health, travel to their current home or to their country, and purchasing new electronic devices.

> "Exams and treatments are expensive. My doctor told me when I saw the psychiatrist that I was spending my whole salary on treatment, he told me to reassess whether I want to continue [working]." (E1).

They also spoke of purchasing new equipment due to the lack of trust in using equipment that was already infected:

> "So, there is an immediate impact of acquiring a new device, but that is only for those who have resources. In the end what matters is peace of mind, and peace can be achieved by getting a new device, but there are others who can't." (Group interview).
> "There are cases where a person decides to move and this has an economic cost. What we have seen is that there are no ways to cover it, even in cases of changing devices, so it always usually comes out of the person's own pocket." (Group interview).

Coping

Coping is defined as a holistic process that transcends an individual response to adversity.

According to Aluna, coping is addressed from a cross-disciplinary perspective that integrates the psycho-emotional, organizational and political dimensions of security. This approach seeks to reinforce strategies of resistance and autonomy in facing structural violence, promoting social justice.[38]

Beristain emphasizes that coping in contexts of human rights violations involves active and passive adaptation processes; in this sense, the affected people could develop defense mechanisms that enable them to overcome the lived experiences. These mechanisms can include silence or collective resistance.[39]

---

38 Aluna Acompañamiento Psicosocial. (2021). (2019, December 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 Beristain, 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/

Thus, we understand coping as a collective transformational process that involves a rebuilding of support networks and community resilience, prioritizing human dignity in the face of mechanisms of oppression.

This section describes coping strategies used by the people interviewed.

1.- Changes to habits and routines

On an individual level, the interviewees described a change in their security-oriented habits. When asked how they cope, everyone interviewed mentioned the change in routines as something commonplace.

> "I totally changed my routines, the bars that I would go to before the spying, also after the pandemic, I didn't return to my prior life. If I go somewhere, they could be watching, because usually... sometimes we go to those places in a group." (E3).

Changes in routine involve changes in technology use. People have found ways of coping with the impact of spyware by making changes to routines, dropping the use of social media or changing to more secure forms of communication.

> "The measures I have taken have been to stop using social media or to deactivate my accounts on social media, removing my profile." (E1).

> "Yes, adopting security measures, the ones I could think of at the time. Using a VPN on my cell phone, on my device, making changes to my home router." (E1).

> "With my friends, we stopped messaging. We had to migrate to a different app, we prefer a secure app. I talk to everyone over Signal." (E3).

Another coping mechanism is the use of new communication devices, thus guaranteeing that they are "clean", although this has a high cost for their personal economy, which has already experienced impact:

> "Getting a new device, but that is only for those who have resources. In the end what matters is peace of mind, and peace can be achieved by getting a new device." (Group interview).

1.- Relocation

The affected people talked about changing their residence, which provides security. They seek places where they are not easily recognized or they are not linked to the role they used to have. This gives them peace and the possibility of resting and feeling a little more secure.

> "Living in this house, then moving to another one, separating from my partner, especially when those investigations were being done." (E1).

Two people have coped with the situation by leaving the country to feel safer:

> "We found out about leaving the country at the end of the year." (E5).
> "Around October I began the process of leaving the country, for me, my wife and my son." (E2).

If they do not leave the country, they decide to isolate for a time:

> "There have been people who have decided to isolate themselves for a time. They decided to stop for a few days, a few weeks, to develop a new strategy based on what has been identified because in the end their private spaces were violated, that's why they need this space to build a new strategy." (Group interview).

The people who have been subjected to tension and who suffer psychological effects due to increased stress also experience fear. Changing the environment is one way of putting the tension on hold and, for a time, it provides a sense of peace.

2.- Self-care

Self-care, understood as the ability to recognize one's own physical, emotional, relational and spiritual needs, is a key component of the psychosocial coping mechanisms.[40] Among the interviewees, exercise was identified as a mechanism to reduce anxiety and improve the ability to sleep.

One person said:

> "I tried to balance it with exercise. At that stage I intensified my exercise and saw that I could fall asleep, especially the sleepless nights and all that involved. In addition to the impact that the emotional level also has on the physical level, I intensified it with exercise." (E1).

Exercise reduces stress,[41] leading the person to move about in another environment with the possibility of changing thoughts and improving mood and health in general.

4.- Seeking psychological support

Everyone interviewed said they had received psychological support, although some had already been receiving it, having sought it out from a few organizations. This helped them to work on anxiety, depression and sleep disturbances:

---

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.

> “I already had my former therapist, two years before. I didn’t want to get involved in another process, I coped well because of that, the therapist helped me a lot.” (E5).

> “I already had a psychologist with whom I was working on grief.” (E3).

Psychological accompaniment has provided essential support for the people who had access to receiving it; they have thus been able to count on someone they can trust with specialized care.

5. -Technical assistance

Another way of coping has been to seek the help of a digital security expert, which has enabled them to mitigate some of the stress by understanding what happened and what can be done to face the risky situations:

> “I received advice from experts, but remotely and, because I couldn’t think straight, I did receive accompaniment, but in that situation there were recommendations that I had to implement.” (E1).

Another interviewee stated that receiving training from experts can help to understand the phenomenon better:

> “Strengthening knowledge of how to have tools, you have to know how the enemy thinks, how they execute these things, to know what measures to take. How to lock down all the devices, how we have the knowledge to take care of ourselves more naturally, without turning to emerging things.” (E4).

Technical support works both to avoid loneliness in these times of stress and worry, and to obtain a little more information, which lends control over a new situation that makes them feel intimidated.

6. - Support networks

Support networks are spaces where suffering is acknowledged, the experience is validated and trust is built to begin processes for healing, justice and social transformation. They are not only functional tools, but also spaces for ethical, political and emotional care.[42]

The search for social support, creating ties with people who can understand this type of attack, has been very important for the people interviewed:

> "I went along building my support network with people that I talked to about certain topics or who I could see were affected. What you have to do is connect rather than isolate." (E1).

This is reinforced by the identity group supporting them:

> "The issue of support among the organizations, we have seen that starting three years ago there has been a big effort around organizing to build networks."

"In the journalism community you see a lot of network support, especially in press releases." (Group interview).

---

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

Social support plays a fundamental role in coping:

> "I had a lot of people supporting me, ranging from specialist friends to foundations for journalists. At one event I explained that I could not be there due to mental health problems. They talked with a sister organization and they supported me by paying for the psychiatrists. Another organization of women journalists supported me through the economic impact that all this was creating, and then there were others. And other support, more emotional, from people who were always present." (E1).

As a type of coping, people, especially those in the public eye, publish complaints and protect themselves as a collective. Some interviewees emphasized that one kind of self-care was to organize as a professional group, e.g., journalism, to publicly expose the situation. Actions in solidarity with the affected person include issuing press releases and holding press conferences to show that the journalists are not alone.

Humor and laughter have been used in work environments to ease anxiety, as one woman interviewed explained regarding how violence was played down:

> "My desk had me facing backwards, I used to tell them, I'm the first who will be killed, the others would say, if they get us from the street side the one they'll kill is me. These were the jokes." (E5).

In essence, the groups have developed coping strategies such as whistleblowing, laughter, humor, support, solidarity and mutual defense.

In many cases families have been that support network, as they represent a safe space for the people under surveillance. They turn to their family as the place where they can change routines and disconnect from the civil society environment, to feel supported and sheltered.

> “People decide to seek refuge with their families, which are disconnected from the civil society sphere, so the costs are not as high and they have a safe, trusted space, because they have lodging with family.” (Group interview).

One protection expert explained:

> “It requires extensive work that is always achieved in a network. In our case we are part of a network. But if you work alone, it wouldn’t be a job that you could continue. Technical review is just the first step, but analysis doesn’t solve the problem; you need to work with lawyers, decision-makers, conduct assessments on other angles, to take much more encompassing action.” (Group interview).

7.- Cross-institution support

Institutional support is important in caring for people who have been subject to spyware surveillance:

> “I was in a care program with Reporters without Borders and that also helped me to work on my anxiety. I learned that spying cannot be avoided, it’s very difficult. But there is a way to limit the risks.” (E3).

The organizations look for ways to improve collective care on the teams, such as providing psychological care or connecting their teams with experts who can support security:

> “[The organization] put it out there that if we needed therapy, we had 10 sessions.” (E5).

When asked how they protect themselves from the effects, those who work supporting people who have been infected with spyware said:

> “There is personal work, on my end, around distancing. The work is important to me, but I have managed to distance myself and dissociate to see it as a job and that it doesn’t take over my personal life.” (Group interview).

Individuals and teams have been able to find ways of facing the vulnerability created by the installation of spyware, providing psychological support, strengthening security on computer equipment or cell phones, providing training to people to improve their sense of security. They also expressed the need to work as a network to receive guidance. They have worked to successfully build a network to address legal, technological, psychosocial and logistical issues.

Conclusions

According to the interviews, the goal of installing spyware is more than surveillance; it is control, instilling a sense of vulnerability, creating a feeling of threat and repressing people in the work they do.

In the cases of the people interviewed, the installation of spyware was accompanied by other attacks such as physical tailing, imprisonment of close colleagues, attacks on social media, displacement and exile, events that have an impact on mental health and constitute sequential or cumulative trauma. The psychosocial effects are seen individually, collectively, emotionally, cognitively and physically.

People have experienced changes in family, work and economic life that deepen psychosocial impacts.

The psychosocial impacts stemming from spyware exacerbated levels of anxiety and depression that were identified before this type of attack.

The first reaction they had to the news was of two kinds. Some people reacted with initial shock, intense fear, anxiety and even panic. Others, according to the interviews, had calmer reactions because they had the feeling that this would happen to them.

The effects identified include hypervigilance, which is a state of extreme alert. This is accompanied by anxiety; it affects the ability to concentrate, which has consequences for work performance and on social relationships. They expressed intense fear which can be long-lasting when there is a stimulus that reactivates it, even becoming life threatening.

Life plans were affected; for example, two people went into exile and quit their job. This means adapting to a new culture, a new language (in one case), and new routines. It also means separation from family and friends.

In the family, there can be reactions of censure, as well as families who provide comfort and support. Families have also felt the impact of separations.

The social context in which the attacks are produced is of widespread fear; the population is afraid to express anti-government opinions. This means that friends and people close to the person tend to distance themselves so as not to suffer the same fate.

On work teams, different types of impact were found, ranging from panic to fatigue. In many cases it is necessary to implement new protective measures in a context of insecurity.

The economy of the affected people has also seen impact due to the extraordinary expenses that must be incurred to care for health, implement relocation mechanisms and acquire new electronic devices

The coping strategies identified include:

- Lowering the social media profile, changing routines, frequenting different spaces so that they have a sense of control over the event and its consequences.

- Seeking refuge with their families meant connecting with feelings of well-being, strengthening binding ties and a sense of being out of danger for a time.

- Strengthening the support network with friends or people close to them was also a coping mechanism. Creating networks to feel safe.

- In terms of groups, they also created joint actions for whistleblowing, press releases and press conferences. This provides people with security and a feeling of unity and collectivity.

- In the organizations, cross-institutional support has been strengthened or created, providing spaces for both technological and psychological support to cope with the consequences of spyware. People feel greater backing and for them, this is a very important coping factor.

Recommendations

Work with human rights organizations, journalists and justice operators so that they may prevent future interventions, knowing what to do and how to face a spyware attack using technology and logistics, with the goal of feeling some control over the threats they face, also considering gender-based differences in the attacks.

Provide psychosocial accompaniment and psychological support to people who experience a spyware attack, to address the levels of anxiety, fear and hypervigilance they may feel.

Create support networks with people who have experienced similar situations and who can offer practical advice based on how they lived through and survived the attack. Networks strengthen social ties and feelings of belonging, and they mitigate the need to create isolation.

Facilitate psychosocial support and training in managing emotions for the teams that work with individuals and organizations who have suffered spyware attacks.

Share and strengthen the creation of economic funds to offer people secure communication devices and logistics if they need to move or to install security systems.

In extreme cases, and if people need to leave their country, enable them to have resources to guarantee they can leave their countries and get settled in another place. Also support for legal migration processes.

Create a network with other professionals who provide legal advice in cases of criminalization.

Develop action protocols in cases of spyware attacks, that can serve to guide the organizations who may be subject to this kind of attack, and which consider other types of violence that are inflicted along with surveillance.

Bibliography

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, December 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, December 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, October 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/B978-0-12-816203-3.00004-6Get rights and content

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

Barrientos M., Najarro F. (2024, August 26). 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

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

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).(January 31, 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. [Press release]. 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, 80° 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 Derechos Humanos. (1977). Caso Loayza Tamayo vs. Perú. https://corteidh.or.cr/docs/casos/articulos/seriec_33_esp.pdf

Duque, V. (2020). Hacia una cultura del buen trato y bienestar Prom oviendo 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. & Reyes D. (January 12, 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. 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. (April 30, 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

Kordon, D., & 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, June 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, September 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, October 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


FUNDACIÓN
Acceso