FUNDACIÓN Acceso

Estudo sobre impactos psicossociais e enfrentamentos diante de ataques digitais
(especificamente spyware)

Autoria
Olga Paz, com contribuições significativas de Gabriela Vargas, Dennise Albornoz e Jacobo Mogollón Villar

Coordenação de pesquisa
Fundación Acceso

Ideia original e desenho metodológico
Fundación Acceso

Supervisão técnica e revisão do relatório
Fundación Acceso, The Engine Room

Organização responsável pela publicação
Fundación Acceso

Agradecemos especialmente a todas as pessoas entrevistadas por compartilharem suas experiências, reflexões e tempo, possibilitando a construção coletiva deste estudo.

Data de publicação
Abril de 2025

Landing Page

Conteúdo

Introdução

No contexto latino-americano, a vigilância direcionada a pessoas defensoras de direitos humanos, integrantes do sistema de justiça e jornalistas constitui uma prática histórica e sistêmica. O relatório "Vigilância na América Central: Internet, privacidade e direitos humanos" da Fundación Acceso[1] define a vigilância na internet como o monitoramento, a coleta e a análise de dados on-line, realizados tanto por agentes estatais quanto por agentes privados. Esse paradigma de vigilância abrange o acompanhamento de atividades em redes sociais, o rastreamento de comunicações eletrônicas e o acesso a informações pessoais, muitas vezes sem o consentimento, explícito ou implícito, das pessoas afetadas.

Atualmente, as operações de espionagem foram reconfiguradas e orientadas para a identificação e neutralização das pessoas rotuladas como "inimigos internos", perpetuando uma lógica contrainsurgente de perseguição que, na segunda metade do século XX, era dirigida a setores considerados uma ameaça ao status quo. Durante esse período, regimes autoritários na América Latina classificaram como opositoras diversas pessoas e coletivos, desde organizações revolucionárias formadas no contexto das ditaduras até movimentos sociais, religiosos, pró-democracia e antimilitaristas, além de pessoas defensoras de direitos humanos.

No século XXI, as estruturas estatais que historicamente utilizaram mecanismos de vigilância e repressão demonstraram grande capacidade de adaptação ao ambiente digital. Atualmente, essas estruturas recorrem a tecnologias avançadas para infiltrar dispositivos eletrônicos, acessar informações confidenciais, exercer pressão e intimidar pessoas e coletivos considerados ameaças ao poder estabelecido, seja ele institucional ou vinculado ao crime organizado. A persistência dessas práticas revela que, para além da transformação das ferramentas, mantém-se uma visão estrutural que interpreta a defesa dos direitos humanos como uma forma de oposição política. Essa perspectiva é sustentada por discursos oficiais que apresentam as ações de vigilância e repressão como necessárias para "combater a criminalidade" e preservar a "segurança nacional".

---

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

Entretanto, a realidade demonstra que as tecnologias de espionagem, em especial o spyware, são utilizadas principalmente para perseguir pessoas defensoras de direitos, vigiar opositoras políticas e hostilizar jornalistas e ativistas. Em contextos nos quais não existem salvaguardas legais adequadas, o spyware se converte em um mecanismo de repressão que permite a governos manter controle sobre pessoas e organizaç ões específicas. Essa prática coloca quem é alvo de espionagem em situação de extrema vulnerabilidade, expõe redes de contato, fontes de informação e estratégias de trabalho, e facilita ações voltadas à desarticulação de esforços coletivos e ao silenciamento de vozes dissidentes.

A facilidade de acesso a dados sensíveis, aliada à amplitude e à profundidade da intrusão, bem como à dificuldade de detecção das operações maliciosas, configura um cenário em que a espionagem se torna menos visível. Esse contexto não apenas amplia as possibilidades de violação da privacidade e da segurança, como também produz novas formas de afetação, incluindo impactos no campo psicossocial. Torna-se, portanto, fundamental analisar de maneira aprofundada as consequências dessas tecnologias, tanto em sua dimensão técnica quanto em seus efeitos emocionais e sociais.

O objetivo desta investigação é analisar o impacto do spyware como ferramenta de vigilância estatal na região latino-americana, especialmente contra pessoas defensoras de direitos humanos e jornalistas. Busca-se examinar como essas tecnologias produzem efeitos que ultrapassam o âmbito dos dados e do digital, afetando a segurança física, a saúde, o bem-estar econômico e social, bem como os direitos das pessoas atingidas.

Por meio da análise de casos documentados, pretende-se compreender os impactos psicossociais específicos e as formas de enfrentamento, tanto no plano pessoal quanto no coletivo.

Tecnologias de vigilância (spyware)

O uso de software espião como ferramenta de inteligência e repressão estatal

A crescente disponibilidade de tecnologias avançadas de espionagem tem ampliado a capacidade de alguns governos de exercer controle sistemático sobre pessoas consideradas ameaças ao poder estabelecido. Nesse contexto, o uso de spyware consolidou-se como uma estratégia central, com objetivos específicos dentro de um ciclo de inteligência. A partir dessas práticas, não se limita a coleta de informações, mas também se viabilizam ações de repressão, intimidação e, em muitos casos, assédio digital e físico. Esse ciclo opera com base na seleção prévia de alvos a partir de seu perfil político, de sua atuação na defesa de direitos humanos e de sua participação em organizações percebidas como risco pelas autoridades no poder.

A implementação dessas ferramentas requer estruturasestatais com acesso a recursos financeiros, tecnológicos e, frequentemente, apoio direto ou indireto de pessoas com poder político e econômico.[2]

É fundamental distinguir três práticas relacionadas, porém distintas: a vigilância digital, a espionagem por meio de spyware e os ataques ou o assédio on-line. Cada uma dessas práticas apresenta características específicas, associadas a diferentes objetivos, níveis de intrusão e consequências. Ao mesmo tempo, elas podem ser empregadas de forma combinada, compondo táticas mais amplas de repressão e intimidação, tanto no plano digital quanto no físico.[3]

2 Anistia Internacional (9 de outubro de 2023). Global: O escândalo dos 'Arquivos Predator' revela ataques descarados com software espião contra a sociedade civil, figuras políticas e altos cargos. [Comunicado de imprensa]. https://www.amnesty.org/es/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/.

3 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

A vigilância digital consiste no monitoramento sistemático de atividades on-line, realizado por governos, empresas e agentes privados, com fins de controle político e investigação de estruturas e redes de pessoas. Essas práticas visam à identificação, à exploração comercial e extrativa de dados, bem como ao acompanhamento e à neutralização de pessoas consideradas “sujeitos de interesse”.

O assédio virtual, por sua vez, caracteriza-se como um padrão de comportamento abusivo e agressivo dirigido a uma pessoa ou grupo no ambiente digital. Ele se manifesta por meio de ataques verbais, difamação, ameaças, assédio sexual e disseminação de informações pessoais, reais ou fictícias, com o objetivo de intimidar e causar danos. Diferentemente da vigilância digital, seu propósito central é produzir impactos emocionais, psicológicos e na imagem pública das pessoas afetadas. Esses ataques, no entanto, não se restringem ao âmbito individual, sendo também utilizados como mecanismo para atingir coletivos específicos, como mulheres defensoras, comunidades indígenas, pessoas LGBTQIAPN+ e organizações sociais, com a finalidade de estigmatizar, enfraquecer sua legitimidade e reforçar processos de marginalização no espaço público e político.

O spyware é um tipo de software malicioso, desenvolvido especificamente para se infiltrar de forma silenciosa em dispositivos eletrônicos, com a finalidade de coletar dados sem o conhecimento nem o consentimento das pessoas afetadas.

Esse tipo de ferramenta permite o monitoramento integral de atividades digitais, incluindo o acesso a comunicações criptografadas, a geolocalização em tempo real, a ativação remota de microfones e câmeras, bem como a extração de arquivos e documentos sensíveis. Sua utilização ocorre no âmbito de operações de inteligência direcionadas a pessoas e entidades consideradas fontes relevantes de informação para a análise de dinâmicas organizacionais, capacidades operacionais e padrões de comportamento. A partir dessas práticas, são elaborados mapas de redes com o objetivo de subsidiar processos de tomada de decisão, avaliação de riscos e desenho de ações voltadas ao controle, à neutralização e à desarticulação de pessoas e coletivos monitorados. As informações obtidas por meio dessas invasões podem ser empregadas na formulação e execução de ações de assédio, criminalização, extorsão e difamação, além de facilitar outras formas de agressão nos âmbitos digital, físico, político e jurídico.[4] [5]

4 Oliveira, P. (s.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

5 Hiperderecho. (s.d.). Tecnoresistencias. https://hiperderecho.org/tecnoresistencias/identifica/

Características da espionagem facilitada por spyware

O spyware representa uma evolução estratégica preocupante em relação aos métodos tradicionais de inteligência, em razão de sua capacidade de operar com alto grau de sigilo, persistência e precisão. Diferentemente de práticas mais visíveis e invasivas, como interrogatórios, infiltrações, acompanhamentos presenciais e buscas, ele possibilita o acesso a informações críticas sem alertar a pessoa ou organização alvo, reduzindo os riscos operacionais para as estruturas que o utilizam.
Essa capacidade de funcionamento extremamente discreto amplia o controle dentro do ciclo de inteligência, ao permitir uma vigilância prolongada e silenciosa sobre pessoas ou organizações. Como resultado, ocorre um acúmulo contínuo e detalhado de informações sobre dinâmicas internas, violando princípios fundamentais de privacidade e abrindo espaço para abusos de poder de difícil detecção e fiscalização.[6]

Uma vez instalado, o spyware tem como objetivo central manter sua persistência sem ser identificado. Para isso, utiliza explorações de dia zero, conhecidas como *zero-day exploits*, que correspondem a falhas ainda desconhecidas pelos fabricantes de software e para as quais não existem correções disponíveis. Em muitos casos, a infecção ocorre sem que a pessoa realize qualquer ação, por meio dos chamados *zero-click attacks* (ataques de clique zero), o que torna essas operações particularmente perigosas. Além disso, esses programas empregam métodos sofisticados de evasão, ocultando-se em processos legítimos do sistema, apagando registros de atividade e evitando a detecção por antivírus e outras ferramentas de monitoramento de segurança.[7]

O uso de spyware constitui uma grave violação de direitos fundamentais e do bem-estar integral das pessoas submetidas à vigilância. Seus efeitos não são neutros, pois reproduzem e amplificam desigualdades estruturais já existentes.

Quando direcionado contra mulheres, pessoas LGBTQIAPN+ e coletivos historicamente marginalizados, o spyware adquire características específicas que extrapolam a violação da privacidade. As informações extraídas podem ser instrumentalizadas para chantagens, represálias e ações de difamação que reforçam discursos de ódio e práticas de violência motivadas por gênero, orientação sexual, identidade e autoexpressão.[8]

---

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

7 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

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

A utilização do spyware por governos na América Latina

Cada vez mais governos ao redor do mundo recorrem ao spyware sob o pretexto de combater o crime e o terrorismo.[9] No entanto, investigações demonstram que essas tecnologias são utilizadas principalmente para vigiar jornalistas, ativistas e figuras políticas. Um relatório da Anistia Internacional, publicado em 2023, revelou que o spyware Predator foi utilizado para espionar funcionárias e funcionários da Organização das Nações Unidas, senadoras e senadores dos Estados Unidos, bem como presidentas e presidentes de parlamentos.[10]

Na América Latina, o interesse governamental por essas tecnologias tem se intensificado. Um estudo publicado em 2016 documentou a aquisição do spyware Hacking Team, comercializado sob os nomes Galileo ou DaVinci, por países como Brasil, Chile, Colômbia, Equador, Honduras, México e Panamá. Esse software, originalmente promovido como ferramenta "para a persecução do crime", tem sido utilizado para vigiar pessoas defensoras de direitos humanos, submetendo-as a práticas de assédio, ameaças e ataques coordenados.[11]

O uso de spyware não representa apenas uma ameaça potencial, mas integra estratégias mais amplas de intimidação e controle. Em El Salvador, durante a administração de Nayib Bukele, integrantes da equipe do jornal digital *El Faro* foram vítimas de infecções com o spyware Pegasus entre 2020 e 2021. A análise pericial conduzida pelo The Citizen Lab, em conjunto com a Access Now, identificou que, desde 26 de junho de 2020, integrantes do *El Faro* sofreram ao menos 226 ataques com esse software.[12] [13]

A gravidade do caso levou a Comissão Interamericana de Direitos Humanos a manifestar apoio ao veículo de comunicação e a condenar "qualquer ação invasiva nos dispositivos de comunicação" que não esteja amparada por um marco legal transparente e compatível com as

---

9 UN News. (14 de março de 2023). Counter-Terrorism "rhetoric" Used to Justify Rise of Surveillance Technology: Human Rights Expert. https://news.un.org/en/story/2023/03/1134552

10 Anistia Internacional. (29 de março de 2023). Anistia Internacional denuncia nova campanha de hacking ligada a empresa de software espião mercenário. https://www.amnesty.org/es/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/

11 Pérez de A., Gisela. (2016). Hacking Team: malware para a vigilância na América Latina. Direitos Digitais. https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

12 Bonilla, D. e Reyes D. (12 de janeiro de 2022). In Brief: Pegasus Spying on El Faro. El Faro (http://elfaro.net/especial/in-brief-pegasus-spying-on-el-faro/

13 Scott-Railton, John, et al. (12 de janeiro de 2022) 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/

normas e padrões internacionais de direitos humanos, assegurando os princípios de necessidade e proporcionalidade.[14]

No México, o uso do Pegasus é amplamente documentado. Em 2017, investigações conduzidas pelo The Citizen Lab, pela R3D, pela SocialTIC e pela Article 19 evidenciaram ataques direcionados a jornalistas, pessoas da advocacia, integrantes do poder legislativo e ativistas anticorrupção.[15] Entre 2019 e 2021, novas investigações forenses realizadas pela R3D e pelo The Citizen Lab confirmaram infecções por Pegasus em dispositivos de jornalistas e de pessoas defensoras de direitos humanos, por meio de ataques do tipo "zero-click", que não exigem qualquer interação por parte da pessoa afetada. Essas evidências confirmaram o uso sistemático desse spyware contra integrantes da sociedade civil mexicana, reafirmando um padrão de vigilância orientado à repressão e à intimidação no país.[16]

Apesar da robustez das evidências disponíveis, a regulamentação do spyware permanece inexistente na maioria dos países da região. Investigações também confirmaram o uso de malware em países como Honduras e Guatemala, entre outros, sem que estejam em vigor mecanismos efetivos de proteção legal, supervisão institucional e prestação de contas.[17]

---

14 CIDH (Comissão Interamericana de Direitos Humanos). (31 de janeiro de 2022). A CIDH, RELE e OACNUDH expressam preocupação diante dos achados sobre uso do software Pegasus para espionar jornalistas e organizações da sociedade civil em El Salvador. [Comunicado de imprensa]. https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

15 Scott-Railton, M., Razzak, A., Nigro, D. (2 de outubro de 2022). Identificam novos abusos do software espião Pegasus no México. The Citizen Lab. https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/

16 R3D: Red en Defensa de los Derechos Digitales. (22 de setembro de 2018). O Pegasus continua operando no México, revela um relatório do The Citizen Lab. https://r3d.mx/2018/09/21/pegasus-continua-operando-en-mexico-revela-informe-del-citizen-lab/

17 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

Efeitos psicossociais do spyware

Para compreender os efeitos do spyware no campo psicossocial, é necessário iniciar pela compreensão dessa abordagem. “Não se trata simplesmente de uma soma entre o psicológico e o social, mas de uma perspectiva holística que permite compreender como os processos sociais afetam as pessoas e como elas processam, resistem e reproduzem esses efeitos em suas vidas” (Beristain, 2006, p. 30).[18] Essa abordagem possibilita identificar como experiências traumáticas afetam dimensões individuais e coletivas, produzindo impactos na identidade, nos projetos de vida, na memória coletiva e nos processos de reconstrução social.

Diante dos diferentes impactos provocados por situações de violência e violações de direitos, as pessoas, tanto no plano individual quanto no coletivo, mobilizam diversas formas de resposta que lhes permitem resistir, adaptar-se e atribuir sentido às experiências vividas. Nesse contexto, o enfrentamento é compreendido como o conjunto de estratégias cognitivas, emocionais e comportamentais utilizadas para lidar com o estresse e com as emoções associadas à adversidade, favorecendo processos de resiliência e de reconstrução do tecido social.

Os ataques com spyware produzem consequências significativas. De acordo com o estudo “Experiências emocionais nas vítimas de violações à cibersegurança”, pessoas submetidas à vigilância relataram que sentimentos como raiva, tristeza e insegurança estão associados aos ataques à segurança cibernética. Uma reação recorrente é a paranoia, caracterizada pela sensação constante de estar sob vigilância. Esse estado afeta diretamente a capacidade de confiar no ambiente.

O estudo documenta que esses ataques podem gerar quadros de depressão decorrentes da invasão da privacidade. Além disso, a perda de controle sobre as próprias informações contribui para sentimentos de desesperança.[19]

---

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

19 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

Em outro estudo, intitulado “Ataque, infecção, vigilância e dano”, realizado em 2023, o dano cibernético é definido como a consequência prejudicial de um evento que afeta o bem-estar de uma pessoa. A pesquisa aponta que pessoas afetadas sofrem danos psicológicos severos, como medo, ansiedade, insegurança, paranoia, perda de confiança e isolamento.[20] Relatórios sobre vigilância também indicam que muitas pessoas passam a praticar a autocensura por medo. “Jornalistas e pessoas defensoras de direitos humanos desempenham um papel indispensável em nossas sociedades e, ao sofrerem silenciamento, seus círculos sociais próximos também são impactados.”[21] Outra consequência recorrente é o isolamento social, uma vez que pessoas afetadas podem tornar-se mais cautelosas nas relações sociais, receando que suas interações sejam monitoradas ou interceptadas.[22]

20 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

21 Declaração da Alta Comissionada da ONU para os Direitos Humanos, Michelle Bachelet, sobre o uso de software espião para vigiar jornalistas e pessoas defensoras de direitos humanos | ONU-DH (hchr.org.mx).

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

Metodologia

Este estudo busca compreender o impacto psicossocial da vigilância com spyware nas dimensões familiar, laboral e econômica, bem como as formas de enfrentamento colocadas em prática pelas pessoas afetadas. Para isso, foi adotada uma metodologia qualitativa,[23] composta por cinco entrevistas individuais e uma entrevista em grupo com duas pessoas especialistas em cibersegurança e proteção digital. O objetivo foi explorar as experiências de pessoas que enfrentaram situações de vigilância por meio de spyware.

As entrevistas foram realizadas em formato semiestruturado, tanto individualmente quanto em grupo, de forma virtual, por meio da plataforma meet.greenhost.net, em um ambiente seguro e confidencial. Em cada entrevista, foram relatados os fatos vividos e compartilhadas reflexões pessoais sobre os impactos desses eventos na vida das pessoas entrevistadas. As entrevistas ocorreram entre os dias 11 e 22 de setembro de 2024.

Todas as entrevistas foram conduzidas de forma anônima e estão apresentadas neste documento de maneira codificada. Foram entrevistadas pessoas jornalistas e advogadas que atuam na defesa dos direitos humanos, sendo utilizados nomes fictícios. Todas as pessoas participantes assinaram um termo de consentimento informado, garantindo anonimato e privacidade.

Uma das entrevistas em grupo foi realizada com duas pessoas especialistas em acompanhamento e proteção digital. De forma anônima e confidencial, foram relatados os casos que essas pessoas assessoraram. Os casos atendidos costumam chegar por meio de vínculos organizacionais previamente estabelecidos ou por indicações de organizações aliadas.

23 Enfoque qualitativo, um enfoque apropriado devido ao seu poder para aprofundar “em complexidades e processos” e explorar fenômenos menos conhecidos. Marshall & Rossman. (1999). Designing qualitative research, p. 57. (3rd ed.). Sage

Resultados da investigação

A seguir, são apresentados os principais resultados da investigação, organizados em três eixos. O primeiro aborda as características da vigilância com spyware a partir do ponto de vista das pessoas afetadas. O segundo trata dos principais impactos psicossociais identificados. Por fim, o terceiro eixo descreve as formas de enfrentamento mencionadas nas entrevistas.

Características dos ataques com spyware

a) O uso do spyware em busca do controle social e da censura

Segundo os relatos coletados, o objetivo da instalação de spyware ultrapassa a mera vigilância. As pessoas entrevistadas apontam que o propósito central é o controle, a produção de sensação de vulnerabilidade, a ameaça constante e a intimidação em razão do trabalho que realizam. Uma pessoa especialista que participou da entrevista em grupo destacou que os telefones funcionam como uma extensão do corpo e da vida cotidiana, concentrando informações sensíveis:

> "Os telefones são uma extensão muito importante de nós. Socialmente, as pessoas costumam usá-los 24 horas por dia, sete dias por semana. Neles estão contatos, conversas, fotos, vídeos e localizações. Se essas informações caem nas mãos de pessoas mal-intencionadas, a segurança física pode ser afetada, sobretudo no caso de jornalistas que publicam investigações sobre corrupção e fazem acusações diretas. Evidentemente, isso gera riscos de ameaças contra a pessoa." (Entrevista em grupo)

Uma entrevistada relata que vivencia a vigilância como se estivesse inserida no panóptico descrito por Michel Foucault. O conceito de panóptico refere-se a um modelo de vigilância e controle social inspirado no projeto arquitetônico de Jeremy Bentham, no qual um vigilante pode observar todas as pessoas sem que elas saibam se estão sendo observadas. Para Foucault, trata-se de uma metáfora do poder moderno e das sociedades disciplinares, nas quais a possibilidade constante de vigilância leva à autorregulação do comportamento e à obediência (Foucault, 2002, p. 202):

> "A constante sensação de estar sendo sempre observada, como diz Foucault sobre o panóptico. Vivi todos os meus 20 anos assim. No momento, eu entendia que não estava acontecendo nada concreto, mas o pensamento estava sempre ali." (E5) .

Ela acrescenta:

> "Quando fiz 21 anos, um assessor do presidente publicou a minha localização ao vivo dizendo: 'Aqui estão todos [nome da instituição], para quem quiser vir dar presentes'. Eu estava com amigos e colegas do jornal. Pensava que estava colocando em risco as pessoas ao meu redor." (E5).

O panóptico cumpre sua função quando as pessoas passam a se autorregular e a se autocensurar:

> "Sim, tive muito medo e autocensura, porque penso muitas vezes que o que eu disser, escrever ou até pensar vai me causar problemas, gerar vigilância e esse tipo de coisa. Quando estou na rua, caminhando ou dirigindo, fico pensando que alguém pode estar atrás de mim. É muito frequente. Se o computador fica lento ou o telefone esquenta várias vezes seguidas, penso que alguém está tentando acessar meus dispositivos para saber o que estou fazendo." (E4).

Outro entrevistado sintetiza essa lógica de controle:

> "O nome do software tem a palavra 'espiar' (spy), mas o objetivo não é a espionagem em si, e sim o controle." (E2).

b) O spyware como uma ferramenta de vigilância estatal

As pessoas entrevistadas relataram que a infecção por spyware ocorreu, aparentemente, em razão do envolvimento em projetos que incomodavam o governo. A instalação do software teria como finalidade monitorar relações, movimentos, contatos e comunicações:

> "Nos casos que vi envolvendo jornalistas e pessoas defensoras de direitos humanos, as infecções coincidiam com momentos em que estavam trabalhando em investigações ou casos relacionados ao governo que teriam impacto negativo. O governo realizava espionagem nesses momentos." (E2).

Para outras pessoas entrevistadas, o governo queria saber quem são as fontes[24] das informações publicadas:

> "O que queriam era ter uma ideia da nossa vida. Estavam o tempo todo nos nossos telefones. Isso facilitava conhecer nossos movimentos, mas acredito que o principal interesse era saber quem eram nossas fontes, que informações tínhamos e com quem nos comunicávamos." (E3).

Com certeza o trabalho que estes jornalistas fazem é muito importante para alguns setores que chegam a pagar muito dinheiro para conhecer de perto o trabalho jornalístico. Como explica o entrevistado:

> "Essa espionagem é muito cara. Cada licença custa aproximadamente 50 mil dólares. O software instalado tem um custo muito elevado pela sua capacidade de intervenção." (E4).

Além disso, foram relatadas estratégias de deslegitimação pública, por meio da produção de discursos que buscam desacreditar essas pessoas e apresentá-las como inimigas do governo:

> "O governo produz discursos constantes contra comunicadoras e comunicadores, criando narrativas e cortinas de fumaça para controlar o discurso público. Quando surge uma notícia escandalosa, como negociações com gangues, o governo lança acusações falsas, por exemplo, de violações ou de benefícios obtidos em troca de favores sexuais, para desviar a atenção da opinião pública." (E2).

---

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

Também foi ressaltado que os ataques partem de atores com elevado poder e capacidade de violência:

> "É preciso considerar que a espionagem vem de grupos bastante violentos, como militares e grupos organizados do crime, que também fazem ameaças de morte." (Entrevista com especialistas).

Em síntese, a instalação de spyware configura uma forma de agressão orientada ao controle de múltiplas dimensões da vida das pessoas e dos grupos sociais aos quais pertencem. As pessoas afetadas relatam sensação constante de vigilância e desenvolvem consequências psicossociais como estresse, cansaço, hipervigilância, dificuldade de compreender o que está acontecendo e rupturas nos projetos de vida.

c) A interrelação entre o spyware e a violência física e digital

A vigilância identificada nos casos estudados integra um conjunto mais amplo de agressões direcionadas às pessoas entrevistadas, bem como às organizações ou grupos dos quais fazem parte. Este tipo de vigilância costuma estar associado a outras formas de violência, como espionagem física, ameaças, encarceramentos, processos de criminalização, difamação e ataques em redes sociais:

> "Um dos meus colegas foi detido, então fomos muito afetadas pela sua prisão porque, como estávamos manifestando opiniões, ele foi detido de maneira suspeita, sem o devido processo. Isso nos impactou porque nos demos conta de que o risco podia ser real." (E1).

Também é importante destacar como os ataques de espionagem se somam a outras experiências traumáticas associadas à própria natureza do trabalho realizado, como o contato frequente com a violência, a morte e o desaparecimento de pessoas:

> "Isso quebrou a *piñata* do trauma, porque na última viagem que eu ia [ao meu país] eu dizia: aqui vi um morto, aqui vim quando mataram outro, esta é a casa que queimaram quando mataram tal pessoa. A última reportagem que fiz... foi quando mataram duas pessoas e as tiraram do bairro onde eu cresci. Quando vi que uma moça da minha idade desapareceu no bairro onde eu caminhava todos os dias, aí decidi migrar." (E5).

Outra pessoa entrevistada fala que a vigilância on-line é acompanhada de vigilância física:

> "No decorrer dos meses comecei a experienciar vigilância física no meu bairro, coisa que era muito incomum porque é uma vizinhança onde só moram pessoas da terceira idade, famílias, uma vizinhança onde quase não vive ninguém, comecei a notar pessoas incomuns fotografando as casas da zona ou caminhando pela região, carros particulares não familiares estacionados, viaturas policiais." (E2).

Outra acrescenta:

> "Eu sei que no final, a espionagem fez parte de outro conjunto de situações que me levou a tirar uma licença do trabalho por uns dois meses, para poder fazer um tratamento." (E3).

Uma entrevistada explica a diferença entre a vigilância física e a vigilância com spyware:

> "Na vigilância não digital é possível ter alertas e a detectar, a vigilância na internet é imperceptível e invasiva, já que lidamos com coisas da nossa vida privada nos celulares e existem mais canais para que nos vigiem, pode ser realizada de maneira anônima; é possível ter acesso a outros tipos de informação sobre a nossa vida, ela favorece a impunidade." (E1).

Devido ao fato de que a vigilância com spyware é imperceptível e invasiva, as pessoas se sentem vigiadas, mas sobretudo controladas o tempo todo, questionando a sua profissão e os valores investidos nas suas carreiras; elas se autocensuram e se silenciam.

Impactos psicológicos e psicossociais

Os efeitos dos ataques com spyware, junto a outras agressões, são amplos e se expressam tanto na dimensão psicológica quanto na psicossocial. Entender a profundidade do dano causado às pessoas e comunidades torna necessária a distinção entre as dimensões psicológicas e psicossociais do impacto. Esta distinção, proposta por Elizabeth Lira (2017), é fundamental para abordar de forma integral as sequelas da repressão e das violações aos direitos humanos. Enquanto os **impactos psicológicos** se expressam em sintomas individuais como o medo, a ansiedade e o trauma, os **impactos psicossociais** levam a consequências maiores, que atravessam a confiança coletiva, a vida comunitária, os vínculos e a memória social.

a. Impactos psicológicos

1. Pânico

Num primeiro momento, o impacto leva a pessoa a um estado de incredulidade ou comoção; não se sabe como responder e sente-se sobrecarga e até pânico. Isso faz com que a pessoa se isole ou se paralise. Essas consequências são diferentes do medo, que pode produzir uma reação mais intensa e desorganizada.[25]

Segundo a entrevista realizada com um dos especialistas, as pessoas entram em pânico:

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

> “Pânico total, se uma pessoa tem ideia de que isto lhe acontece, sente pânico total, na maioria das vezes as pessoas nem sequer sabem o que fazer, é uma situação para a qual, em geral, as pessoas não estão preparadas.” (Entrevista em grupo).

> “É tão importante nos concentrarmos nas primeiras horas quando vivemos a espionagem, porque essas primeiras horas foram as que mais geraram uma sobrecarga emocional, é preciso aprender a administrá-la.” (E3).

Uma entrevistada explica:

> “Estar assim com tantas coisas nos pressionado, com o estresse, a gente tem dificuldade para tomar outro tipo de decisões que, estando em um estado normal, não seriam tão difíceis, mas eu que conheço medidas de segurança, me bloqueei, naqueles momentos nem queria lidar com isso, me estressava o fato de pensar nisso.” (E1).

E acrescenta:

> “O que geralmente acontece é se isolar, isolar-se e/ou ficar congelado, paralisada, não saber o que fazer.” (E1).

2. Normalização da violência

Outras pessoas, como mecanismo de defesa, tendem a normalizar a situação, encarando o ataque como algo que poderia acontecer e aconteceu:

> “A violência tende a se tornar algo natural em contextos onde já é cotidiana, onde perdeu seu caráter de excepcionalidade. Esta naturalização acarreta uma aceitação passiva e resignada, e produz um efeito de anestesia emocional que bloqueia a empatia, a indignação e a possibilidade de agir.” (Beristain, 2010, p. 58).[26]

Entretanto, essas pessoas trabalham na mídia, sabem que correm riscos e que podem ser perseguidas e detidas. Para poder sobreviver nessas condições, existe uma espécie de normalização da violência digital:

---

26 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

> “A normalização te diz, bom eu sei que podem me matar. Nos jornalistas, o perfil de risco é mais elevado, estou à mercê de ser a vítima desta situação, como (conformar-se).” (Entrevista em grupo)

Mesmo que seja normalizada, as pessoas não deveriam viver com esse medo constante:

> “Se normaliza. Mas lá fora há milhões de pessoas que vivem sem medo e isso é normal.” (E5).

O que poderia funcionar como um mecanismo de defesa é a “negação”, que consiste em se recusar a aceitar a realidade por temor de que seja dolorosa. Pode ser útil no princípio, mas pode interferir numa vida emocional saudável.[27]

3. Hipervigilância

As pessoas entrevistadas relataram que iniciam uma etapa de hipervigilância que as esgota por estarem o tempo todo em alerta. A hipervigilância é um estado de alerta extremo. Pessoas nesse estado estão constantemente atentas a possíveis ameaças e perigos. Também é um sintoma do Transtorno de Estresse Pós-Traumático (TEPT). É acompanhada de ansiedade e afeta a capacidade de concentração, com consequências no rendimento laboral e nas relações sociais. Estar em um estado constante de alerta causa esgotamento físico e mental. Além disso, pessoas em hipervigilância podem evitar lugares e pessoas, isolando-se.[28]

> “Sensação de hipervigilância, mas já sabia que ia acontecer, há uma cadeia de emoções, a primeira é frustração e decepção. Uma coisa é dizer, eu sabia que podia acontecer, e outra é, já aconteceu.” (Entrevista em grupo).

> “Hipervigilância, mudança de ruas, as mais difíceis, evitar as rotas principais, dirigir por bairros. Quase não saía de casa, na maioria das vezes utilizando precauções que a maioria das pessoas não usaria, nem sequer lhes ocorreria.” (E2).

---

27 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/

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

4. Pensamentos recorrentes

Os pensamentos recorrentes são ideias ou imagens que se repetem na mente. Podem ser involuntários e, frequentemente, estão associados à ansiedade, ao estresse ou ao Transtorno de Estresse Pós-Traumático (TEPT). Podem, ainda, interferir na capacidade de concentração e na vida cotidiana da pessoa.[29]

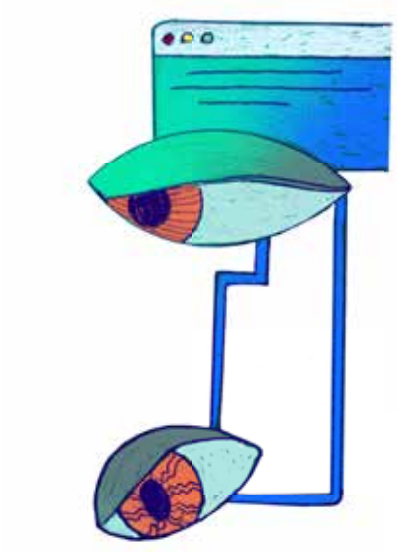
As pessoas iniciam um processo de autoquestionamento, perguntando-se: "O que eu fiz?", e passam a ter pensamentos repetitivos sobre os dados que, possivelmente, foram obtidos de seus dispositivos e sobre como poderiam ser utilizados contra elas:

> "Então começam as interrogações sobre o que souberam do meu parceiro/a, dos meus filhos, filhas e filhes; também há uma sensação bem profunda de raiva, de frustração diante da impunidade, porque não é novo que os governos espionam. Estão surgindo casos e as coisas não mudam, é uma sensação de impotência diante da impunidade." (entrevista em grupo).

Os pensamentos recorrentes também produzem, de forma constante, cenários sobre o que pode acontecer com as informações obtidas:

> "Você cria cenários na cabeça porque tem a certeza do que sabem." (E5)

Todas as pessoas entrevistadas relataram sofrer pensamentos recorrentes desde que souberam que havia spyware instalado em seus dispositivos. As pessoas que apresentaram esse tipo de pensamento também relataram ansiedade e alterações no sono.



29 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. Ansiedade

As pessoas entrevistadas apresentaram diferentes respostas de ansiedade, que interferem significativamente nas atividades cotidianas. A ansiedade aparece como uma reação a eventos percebidos como ameaçadores, caracterizada por preocupação excessiva e persistente, acompanhada de sintomas como tensão muscular, palpitações, dificuldade para respirar e transtornos do sono. As pessoas entrevistadas indicaram como a vigilância pode tornar a ansiedade crônica e intensificá-la:

> "Tive algumas crises de ansiedade, a sensação de estar hiperventilando com uma dor no peito." (E2).
> "Ansiedade sim, estive em constante alerta. Nesses períodos em que me dei conta de que estava sendo vigiada, o que isso produziu em mim foi insônia e estresse, e provocou ou intensificou a ansiedade que eu vinha sentindo depois da quarentena. A pandemia me deixou um transtorno de ansiedade, mas logo me dei conta da vigilância contra mim, e isso se intensificou, fazendo-me retroceder no trabalho de combate à ansiedade e à insônia, também pelo estado de alerta." (E1).

Esta entrevistada, ao compreender o que implicava a instalação de um spyware, percebeu um aumento significativo da ansiedade:

> "Isso nos sobrecarregou, porque chegamos a ter níveis de ansiedade muito altos quando nos explicaram o que é o Pegasus e entendemos o alcance que tinha." (E3).

> "Me diagnosticaram com muita ansiedade, mas ainda não tinham me permitido falar sobre o tema; então fui acumulando e acumulando até que o pote explodiu, e foi no ano seguinte que decidi tirar uma licença [do trabalho]." (E3)

As pessoas entrevistadas relataram que, ao saberem que estavam sendo vigiadas, a ansiedade previamente vivida em decorrência de outros eventos de suas trajetórias se intensificou, chegando, em alguns casos, a causar ataques de pânico.

6. Alterações no sono

As alterações no sono aparecem como uma resposta frequente a essas experiências, derivadas de altos níveis de ansiedade ou angústia. Podem se manifestar como insônia, dificuldade persistente para regular o sono ou sonolência constante, além de despertares em horários incomuns e alterações no ritmo do sono:

> “Insônia, sempre tive problemas de insônia. Naqueles anos, sim, eu tinha insônia e ela se intensificou muito naqueles dias, a ponto de dormir somente por cansaço, nem sequer por necessidade; o corpo faz isso.” (E2).

Outra entrevistada relatou a presença de pesadelos:

> “A ansiedade se transformou em sonhos intensos; sonhava que me perseguiam ou que me detinham, sonhava que os meus amigos estavam em perigo.” (E3).

Esta pessoa, vivendo no exílio, sofre com pesadelos recorrentes, e a ansiedade aumenta quando regressa ao seu país de origem. Por exemplo, manifesta medo de ser presa por questões administrativas:

> “Faz anos que tenho pesadelos [com o meu país] e, quando fui lá escondida, passei mal, mal de verdade. Fico checando se não devo impostos, se não vão me prender por cinco dólares. Eu nunca digo às minhas amigas a data em que chego, aviso à minha mãe por ligação, nunca digo quando chego.” (E5).

7. Depressão

Duas pessoas entrevistadas relataram sofrer de depressão. Em contextos de violência sociopolítica, a depressão pode se manifestar de diferentes formas, como tristeza persistente, vontade de chorar, irritabilidade, isolamento, desânimo, dificuldades para dormir, autocrítica e pessimismo.[30]

Em alguns casos, a depressão já existia anteriormente, mas foi reativada ou agravada pela vigilância:

> “Eu estive em uma depressão nos últimos meses por causa de coisas que sofri na minha infância, acredito que todas estas situações também a desencadearam.” (E4).

> “Problemas de depressão..., depois desse diagnóstico me qualificaram com depressão.” (E2).

> “No meu caso, pela ansiedade ou pela insônia, ou pela depressão, havia dias que não queria fazer nada.” (E1).

---

30 Kekre, C., Fisher.M, kreke, A. (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

As pessoas entrevistadas vivenciaram muitas dessas consequências; suas vidas foram profundamente impactadas, afetando os âmbitos familiar, social e laboral.

8. Medo

Três das pessoas entrevistadas relataram sentir medo. Segundo Elizabeth Lira, o medo pode desencadear comportamentos específicos que podem ser descritos como processos adaptativos diante de situações ameaçadoras. A experiência de risco constante na vida cotidiana afeta subjetivamente a pessoa e a forma como ela se percebe e percebe o ambiente ao seu redor. O medo pode se tornar permanente, especialmente quando as circunstâncias percebidas como ameaçadoras à vida se tornam crônicas.

O medo levou as pessoas a se autocensurarem.

> "Eu tinha muito medo, eu me autocensurava, porque muitas vezes pensava que o que eu dizia, o que eu escrevia ou o que eu pensava poderia me causar problemas, com que eu me seguissem e coisas do tipo." (E4).

Ou então, elas paravam de fazer coisas que costumavam fazer regularmente.

> "Eu não queria mais falar ao telefone porque estava com medo." (E5).

O medo também surge da possibilidade de seus familiares sofrerem ataques.

> "Eu tinha alguns projetos de podcast, mas quando minha esposa e meu filho voltaram (para o nosso país de origem), eu desisti deles por medo. Mesmo estando aqui (no exílio), eles estão lá e são alvos fáceis; eles poderiam atacar meu pai, minhas irmãs, meu filho ou minha esposa." (E2).

Embora essa pessoa esteja fora do país há mais de dois anos, suas preocupações não diminuíram. Ela sente medo, ansiedade e sensação de ameaça, e acredita que o governo ainda pode lhe causar danos. Vive com uma sensação generalizada de insegurança que provoca medo constante. Por exemplo:

> "Tive que ir ao consulado (do meu país) para renovar meu passaporte aqui onde moro. Eu estava chorando no consulado

> porque tive que informar meu endereço e número de telefone atuais. É um procedimento normal e sei que ninguém no consulado quer me fazer mal. As pessoas que aparecem nos jornais são diferentes, mas isso não significa que eu não tenha sentido medo enquanto estava lá." (E5).
>
> "Não acho normal ou saudável começar a chorar ao renovar o passaporte." (E5).

Embora o medo seja uma emoção desencadeada pela percepção de perigo, funcionando como uma reação de alerta diante de uma ameaça e ativando respostas como lutar, travar ou fugir, o problema para as pessoas entrevistadas afetadas por spyware é que elas não sabem quem está por trás da ameaça.

9. Efeitos no corpo e na saúde

As pessoas entrevistadas também relataram problemas de saúde, dores corporais e padecimentos que podem se tornar crônicos, como colite, dores de cabeça e dores no pescoço. Para Van der Kolk, que desenvolve pesquisas sobre as marcas do trauma nas emoções e no corpo, existe uma relação direta entre o impacto psicológico do estresse e do trauma e suas manifestações corporais, partindo da compreensão de que mente e corpo funcionam de forma integrada.[31]

Esses efeitos no corpo, em alguns casos, já existiam anteriormente, mas a vigilância e outras formas de violência associadas contribuíram para seu agravamento. Como explica uma das pessoas entrevistadas:

> "Antes, por muito tempo, eu sofria de colite, no entanto, com todo este transtorno, ela voltou. Depois, tive problemas de alimentação que têm sua origem na saúde mental." (E2).
>
> "Dor no corpo, dor de cabeça, dormência no rosto, fiz uso de medicamentos." (E4).
>
> "Me causou um problema maior nas costas e no pescoço, fui diagnosticada com cervicalgia e desarticulação do pescoço. Fizeram vários exames porque queriam desc artar problema artrítico. O psiquiatra me disse que eu tenho transtorno somatoforme porque somatizo parte dos problemas que estão ao meu redor." (E3).

---

31 Van der Kolk, Bessel A. (2020). *O corpo guarda as marcas: Cérebro, mente e corpo na superação do trauma*. Traduzido por Montse Foz Casals, 3ª edição., Editorial Eleftheria.

b. Impactos psicossociais

1. Isolamento social

Este tipo de efeito é um dos mais significativos do dano psicossocial, pois impossibilita a elaboração coletiva do sofrimento, aumenta o medo e dificulta os processos de recuperação e reconstrução do tecido social.[32] Todas as pessoas entrevistadas relataram uma sensação generalizada de insegurança que provoca evasão de lugares e de pessoas. Isso repercute diretamente no apoio social, uma vez que tendem a se isolar justamente de quem poderia oferecer apoio e solidariedade:

> "Não posso visitar lugares que eu frequentava antes, nem me sentir totalmente livre e em paz. Sinto uma paranoia de controle no entorno, como se alguém estivesse nos escutando, sem a sensação de que posso falar tranquilamente no telefone." (E1).

Sofrer um ataque com spyware é uma experiência delicada e, para não colocar em risco pessoas ao redor, como contatos, familiares e fontes de informação, as pessoas afetadas foram aconselhadas a não falar sobre o ocorrido. Isso impede o início de um processo de alívio emocional e a construção de vínculos saudáveis:

> "Foi duro porque já tinham nos dado recomendações de que não podíamos falar com ninguém, então no início estavam ali somente nós. Um grupo muito pequeno que estava a par dos ocorridos, mas depois nos demos conta, minha companheira e eu, que era algo maior. Eu sei que no final a espionagem fez parte de outras situações que causaram muita ansiedade, mas essa foi a cereja do bolo que me levou a uma licença [do trabalho], de uns dois meses, para poder fazer um tratamento." (E1).

Da mesma forma, os espaços de lazer também são afetados. Por exemplo, um grupo de jornalistas decidiu tomar precauções ao frequentar espaços públicos:

> "Sempre temos que nos comportar como jornalistas, é uma situação muito terrível e não podemos nos comportar como uma pessoa normal. O fato de que algo tão básico como tomar uma taça de vinho ou dirigir um carro, embora permitido, gere um alerta de não dirigir com nem sequer uma gota de álcool no organismo, evitando qualquer comportamento que possa comprometer nossa integridade ou criar uma onda de dizeres contra nós, é preocupante. (E4).

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

2. Projeto de vida

O chamado projeto de vida refere-se ao desenvolvimento integral de uma pessoa, considerando sua vocação, aptidões, contextos, potencialidades e aspirações, que lhe permitem projetar expectativas razoáveis e ter condições de alcançá-las.[33] Por isso, o impacto psicossocial pode levar à ruptura de planejamentos sobre o futuro, ou seja, à impossibilidade de continuar com planos, sonhos e vínculos que davam sentido à existência.[34]

Nas entrevistas realizadas, observam-se diferentes níveis de impacto no projeto de vida. No âmbito laboral, três pessoas deixaram seus trabalhos; duas passaram por separações ao sair para o exílio, o que implicou deixar familiares e amizades. Deixar am sua terra, seus costumes e seus lares.

Ao longo da vida, as pessoas tendem a estabelecer metas de longo prazo e expectativas de acordo com suas possibilidades de desenvolvimento integral. Um exemplo de impacto no projeto de vida aparece no relato desta entrevistada. Durante os anos dedicados ao trabalho, ela não pôde realizar experiências comuns a pessoas da sua idade; embora tivesse um emprego, todas as suas relações pessoais estavam atravessadas pelas ameaças do Estado:

> "Eu já não queria estar trabalhando, dediquei 20 anos ao jornalismo, e eu pensava, 'poxa, há um monte de coisas que não vivi ainda e há um monte de coisas que vivi que não devia ter vivido." (E5).

O projeto de vida torna-se, assim, uma das maiores vulnerabilidades das pessoas, uma vez que a própria profissão possibilita agressões, vigilância e controle:

> "Muitos sentimentos de solidão e também o fato de que o trabalho que fazemos está desvalorizado e perdeu todo o sentido. Estou fazendo um trabalho que praticamente não serve para nada porque não acreditam nele, isso é muito grave, acredito que é um tipo de solidão, o fato de pensar num trabalho que não vale tanto, então a gente se sente abandonado." (E4).

Uma das pessoas entrevistadas começou a trabalhar aos 19 anos em um jornal voltado à defesa dos direitos humanos. Posteriormente, dedicou-se a temas como memória histórica, violência de gênero e direitos humanos. Com o governo de Nayib Bukele, começaram as suspeitas,

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

34 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

a vigilância e as ameaças nas redes sociais. Em setembro de 2021, recebeu uma mensagem em seu telefone celular informando que havia um spyware instalado, e posteriormente foi confirmado que havia sido infectada com o Pegasus.

O impacto foi forte e em muitas dimensões da vida:

> "Não publico mais em redes sociais, larguei meu trabalho, muita coisa me levou a trabalhar mais nos bastidores. Os fatores internos também influenciam, mas a espionagem estatal foi a gota d'água, eu disse 'já não tenho mais nada para fazer aqui.' Saber que não só têm minhas informações, mas informações sobre a minha família, minha mãe, meus sobrinhos e sobrinhas. Minha mãe não queria falar no telefone porque tinha medo." (E5).

> "Uma falta absoluta de liberdade e do sentido de segurança. Foi horrível ter a confirmação, mesmo que eu já tivesse dúvidas." (E5).

O exílio é um dos fatores que mais afetam o projeto de vida: a mudança de país, de cultura e de idioma, a perda da vida cotidiana e da proximidade com familiares. Todos esses aspectos exigem que as pessoas se reinventem e, em um dos casos, que mudem completamente de área profissional.

Duas das pessoas entrevistadas encontram-se em situação de exílio, o que gerou um custo elevado em suas vidas econômicas e emocionais, além de novos desafios relacionados ao deslocamento e à separação familiar. Embora o exílio possa oferecer maior segurança pessoal, outros elementos que dão sentido à vida desaparecem, como o convívio familiar, as amizades e os espaços relacionais.

O exílio e o deslocamento do lugar de origem podem provocar um impacto profundo no projeto de vida de pessoas forçadas a abandonar seus lares e suas famílias. Elas podem vivenciar uma série de situações, como a perda de conexão com outras pessoas, a incerteza e a falta de controle sobre o futuro, a separação de entes queridos e a adaptação a um novo ambiente. Pessoas em situação de exílio frequentemente relatam forte nostalgia em relação à sua casa e à vida anterior.[35]

35 São as consequências que as experiências e vivências das agressões têm sobre as emoções e o estado mental das entrevistadas.

3. Família

Em geral, as famílias vivem nos mesmos contextos que as pessoas afetadas, por isso conhecem os riscos que seus familiares enfrentam ao realizar trabalho de defesa de direitos ou jornalismo. A família sofre pelos ataques que seus entes vivem. Com a intenção de proteger quem amam, muitas vezes pedem que desistam de seu projeto de vida. Isso faz com que as pessoas afetadas prefiram se silenciar no espaço familiar, o que intensifica o isolamento e os sentimentos de solidão:

> “Na família, sim, me senti um pouco sozinha porque precisava de pouco mais de apoio e o que foi uma bronca. Foi um convite a me censurar, por isso, da parte deles, sim, me senti sozinha, no compromisso de não comentar qualquer coisa com alguém por medo de que aquilo se voltasse contra mim, vivi a mesma situação com amigos.” (E1).

Para pessoas que vivenciam ataques de espionagem, o sofrimento da família ou de pessoas próximas é fonte de ansiedade e de estresse adicional; por isso, optam pelo distanciamento:

> “Me afastei dos meus amigos, da minha família, mudei de casa, foi um momento bem estressante porque tive que fazer várias mudanças pessoais, familiares, profissionais nem tanto, porém tive que adotar medidas de segurança.” (E1).

As amizades e familiares também se afastam por medo de sofrer a espionagem e suas consequências:

> "Nos isolamos socialmente devido ao medo generalizado. Existe uma espécie de rejeição, e é possível ver isso, muitas pessoas querem manter distância." (E4).

Como resultado deste distanciamento, o círculo social se reduz às pessoas com as quais se compartilha uma relação de trabalho ou de ativismo:

> “Nota-se a distância, então a única coisa que fazemos é nos relacionar mais com colegas.” (E4).

No entanto, há outras famílias que podem oferecer refúgio e apoio às pessoas vigiadas, precisamente, por estarem desconectadas da sociedade civil.

As famílias também podem ser afetadas pelas separações, sobretudo pelo exílio.

4. Impacto de gênero

As entrevistas realizadas indicaram ataques com conteúdo explícito de violência de gênero direcionados a mulheres defensoras. Conforme aponta pesquisa da Anistia Internacional, ataques com spyware dirigidos a pessoas da comunidade LGBTQIAPN+ também produzem riscos diferenciados. Ao tratar de conteúdos violentos com discriminação baseada em gênero, predominam estereótipos atribuídos às mulheres, com conteúdo machista e discursos que historicamente foram utilizados para desqualificá-las, como insultos que as rotulam de "prostitutas" e práticas de violência sexual.

As mulheres entrevistadas dizem que os ataques contra elas têm conteúdo de violência sexual. Este assédio tem a ver com as agressões nas redes sociais e um discurso que, geralmente, está direcionado à criação de um consenso sobre estereótipos de gênero:

> "Os ataques contra mulheres são de cunho sexual e, em geral, as ativistas mulheres sofreram mais ataques sexuais." (E1).

Outra entrevistada opina:

> "Até para nos atacar nos discriminam, homens aguentam serem chamados de idiotas e estúpidos, mas ninguém fala pra eles: 'vou te estuprar'; isso acontece com as mulheres." (E5).

A violência contra as mulheres exercida em redes tem como objetivo deixá-las paralisadas e usar aspectos físicos e sexuais para ataca-las. Elas também são difamadas e ameaçadas de estupro e morte:

> "Os ataques são agressivos, mas muitas vezes a reação que se tem desse ataque pode chegar a ser muito cruel quando se é mulher, porque o que querem é destruir a pessoa de modo que se sinta em risco e agredida." (E3).

Essas agressões buscam paralisar mulheres por se atreverem a ocupar uma esfera pública historicamente reservada aos homens; além disso, os ataques procuram deslegitimá-las por serem mulheres, e não pelo conteúdo de seu trabalho.

5. Equipes e ambiente de trabalho

Nas equipes de trabalho, o spyware produz diversos efeitos, como medo, sobrecarga e cansaço. Quando as pessoas rompem o silêncio e relatam o que ocorreu, isso pode gerar uma cadeia de pânico que se prolonga no tempo e altera o funcionamento das organizações:

> "Numa organização, a primeira coisa que se faz é contar, e isso cria uma cadeia de pânico, de como comprometeram a pessoa e, 'eu trabalhei com ela há dois dias', então, isso leva as equipes a se sentirem inseguras." (entrevista em grupo).

A espionagem gera desconfiança. Ela muda a confiança básica entre as pessoas dentro das organizações.

> "Isso tem sequelas a longo prazo, são duradouras. Há um trabalho posterior de conscientização sobre o uso da tecnologia, porque os alicerces que as organizações se baseavam para trabalhar desmoronam." (entrevista em grupo).

Outro fator que afeta a equipe de trabalho é o cansaço; o trabalho precisa ser feito todos os dias, mas com novas medidas de segurança e cuidado, exaurindo as equipes.

> "Estamos lidando com isso como uma inércia, estamos cansados, a equipe está cansada, estamos lidando com o trabalho, mas, além disso, com esta situação, pensando que 'hoje atacam um, hoje podem estar vigiando desta maneira', então, [nestas circunstâncias] como se discute sobre normas de segurança? A segurança é priorizada numa sociedade que deveríamos estar pensando sobre como fazer nosso trabalho melhor." (E4).

Da mesma forma, há um impacto econômico nas equipes de trabalho. Um entrevistado mostrou preocupação com as despesas extras da organização que o contratou:

> “Do meu ponto de vista profissional, isso afetou as coisas de diferentes maneiras. Ela [a organização] tem um ônus financeiro associado à minha contratação. Ao contratar uma pessoa [local], ela não precisaria pagar um advogado de imigração” (E2).

Há ainda o receio de que a organização sofra novos ataques ou exposição midiática:

> “Ao contratar alguém que já foi vítima, em primeiro lugar, ela [a organização] corre o risco de que, se meu celular for hackeado, as conversas de trabalho sejam tornadas públicas. Afinal, conversas de trabalho são inevitáveis. Por outro lado, o governo, com os dados coletados ou a vigilância física, teria um impacto na mídia” (E2).

Também ocorre uma paralisia temporal nas equipes, sobretudo após a conclusão da análise inicial dos casos:

> "Há uma paralisia temporal, sobretudo quando finalizamos a análise inicial, porque, geralmente, quando há uma pessoa vigiada, primeiro é preciso fazer a análise de até onde foi o alcance do impacto. É necessário identificar quais outras pessoas foram comprometidas dentro da organização (entrevista em grupo).

As pessoas dizem que não conseguem se concentrar como antes e que devem dedicar horas de trabalho ao seu bem-estar psicológico.

> "Além disso, o desempenho no trabalho é um pouco impactado, não só me tira anos de vida e de vida útil, mas tenho vivido situações em que meu desempenho não é o melhor, nem o adequado, porque estou sobrecarregado, e não é possível mudar isso. Não posso evitar que o Estado me persiga, não posso resolver sozinho todos os problemas de saúde mental que surgiram e pioraram com esta situação, então, isso também me pressiona a tentar me manter são." (E2).

> "Sinto que, diferentemente de 5 anos atrás, o rendimento, a produção diminuíram, a gente investe tempo em se curar, em se recuperar, e deixa de lado todo o resto no trabalho. Depois disso, dediquei-me a resolver meus problemas pessoais, não é por comodidade, surgiram coisas que a gente não sabe controlar." (E4).

Existe um impacto econômico nas equipes de trabalho, como a preocupação com os gastos extras que a organização contratante precisa ter. Um especialista entrevistado diz que elus recebem apoio psicoemocional:

> "Têm coisas que estão fora do nosso controle, às vezes aconteceram casos de vigilância e esses cenários são mais estressantes e devemos ter mecanismos caso alguém que precise. Por parte dos doadores, temos um fundo de resposta rápida para apoiar estas situações." (entrevista em grupo).

Ele acrescenta:

> "Esgotamento por empatia. As pessoas que acabaram de chegam devem conhecer os riscos, elas podem ter um burnout, um esgotamento por empatia, é importante enfatizar isso." (entrevista em grupo).

As equipes de trabalho enfrentam desconfiança, cansaço, insegurança e dificuldades econômicas e logísticas, sendo obrigadas a reajustar finanças, processos organizacionais e a buscar apoio psicológico e técnico em segurança.

6. Impacto econômico

A situação econômica das pessoas afetadas também foi impactada pelos gastos adicionais com saúde, mudanças de residência ou de país, além da aquisição de novos dispositivos eletrônicos:

> “Exames e tratamentos que são caros, meu médico me disse quando vi o psiquiatra, que estava deixando todo o meu salário em tratamento, disse, reavalie se quer continuar [trabalhando].” (E1).

Também foi mencionada a compra de novos equipamentos devido à desconfiança em relação aos dispositivos previamente infectados:

> “Então, existe um impacto imediato de adquirir um novo dispositivo, mas isso é só para os que têm recursos. No final, o que conta é a paz mental, e a paz pode ser obtida por outro celular, mas há outros que não poderão [comprar].” (entrevista em grupo).

> “Há casos em que uma pessoa decide se mudar e, isso tem um custo econômico, o que vimos é que não existem maneira de gestão, mesmo em casos de troca de celular, de modo que sempre costuma vir das próprias economias da pessoa.” (entrevista em grupo).

Enfrentamentos

O enfrentamento é concebido como um processo integral e holístico que transcende a resposta individual diante das dificuldades.

A partir da perspectiva da Aluna, o enfrentamento é abordado por meio de um olhar transdisciplinar que integra dimensões psicoemocionais, de segurança, organizacionais e políticas. Essa abordagem busca fortalecer estratégias de resistência e autonomia frente às violências estruturais, promovendo a justiça social.[36]

Beristain destaca que o enfrentamento em contextos de violações de direitos humanos envolve processos de adaptação ativa e passiva. Nesse sentido, pessoas afetadas podem desenvolver mecanismos de defesa que lhes permitam lidar com as experiências vividas, incluindo o silêncio e a resistência coletiva.[37]

---

36 Aluna Acompañamiento Psicosocial. (2021). (2019, dezembro 3) Impactos psicosociais da defesa dos direitos humanos sobre as mulheres defensoras. PBI México. https://pbi-mexico.org/es/noticias/impactos-psicosociales-de-la-defensa-de-los-derechos-humanos-sobre-las-mujeres-defensoras

37 Martín Beristain, C. (2017). Metodologias de investigação, busca e atenção às vítimas: Do caso Ayotzinapa a novos mecanismos na luta contra a impunidade. 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/

Assim, compreende-se o enfrentamento como um processo coletivo e transformador, que envolve a reconstrução de redes de apoio e a resiliência comunitária, colocando a dignidade humana frente aos mecanismos de opressão.

Nesta seção, descrevem-se as estratégias de enfrentamento utilizadas pelas pessoas entrevistadas.

1. Mudanças de hábito e rotina

As pessoas descrevem mudanças em seus hábitos para se sentirem mais seguras. Ao serem questionadas sobre como enfrentam a situação, todas as pessoas entrevistadas mencionaram a mudança de rotina como algo generalizado.

> "Mudei totalmente minha rotina, os bares que eu frequentava antes da espionagem, também depois da pandemia, não voltei à minha vida anterior, se vou a algum lugar, podem estar vigiando, porque geralmente... às vezes andamos em grupos nesses lugares." (E3).

As mudanças de rotina envolvem alterações no uso da tecnologia. As pessoas encontraram formas de enfrentar o impacto do spyware realizando mudanças, deixando de usar redes sociais ou migrando para meios de comunicação mais seguros.

> "As medidas que tomei foram deixar de usar as redes sociais e desativar minhas contas em redes sociais, diminuir a exposição." (E1).

> "Sim, adotar medidas de segurança, as que me vinham à cabeça naquele momento. Usar uma VPN, no meu celular, no meu computador, fazer mudanças no roteador de casa." (E1).

> "Com meus amigos, paramos com as mensagens. Tivemos que migrar de aplicativo, preferimos um aplicativo seguro. Falo com todo mundo pelo Signal." (E3).

Outro mecanismo de enfrentamento é o uso de novos dispositivos de comunicação, garantindo que estejam "limpos", embora isso tenha um custo alto.

> "Comprar um novo celular/computador, mas isso é só para os que têm recursos, no final o que conta é a paz mental e, a paz, pode ser dada por outro dispositivo." (entrevista em grupo).

2. Mudança

As pessoas afetadas falaram em mudar de residência. Isso traz mais segurança, buscando lugares onde não sejam reconhecidas com facilidade ou não sejam associadas à função que desempenhavam. Isso lhes dá tranquilidade e a possibilidade de descansar e se sentirem um pouco mais seguras.

> "Morar nesta casa, depois mudar para outra, separar-me do meu parceiro, sobretudo quando estava fazendo essas investigações." (E1).

Duas pessoas enfrentaram a situação saindo do país para se sentirem mais seguras.

> "Soubemos da saída do país no final do ano." (E5).

> "Em outubro comecei a tramitar minha saída do país, a minha, da minha esposa e filho." (E2).

Se não saem do país, decidem se isolar por um tempo.

> "Houve pessoas que decidiram se isolar por um tempo, decidem parar por alguns dias, algumas semanas para elaborar uma nova estratégia com base no que foi identificado, porque no final seus espaços privados foram violados, por isso necessitam deste espaço para criar uma nova estratégia." (entrevista em grupo).

As pessoas que estiveram submetidas a tensão e sofrem efeitos psicológicos devido ao estresse elevado, sentem, além disso, medo. Mudar de ambiente é uma forma de dar um alívio à tensão e, por um tempo, gera uma sensação de tranquilidade.

3. Autocuidado

O autocuidado, entendido como a capacidade de reconhecer as próprias necessidades físicas, emocionais, relacionais e espirituais, constitui um componente fundamental dentro dos mecanismos de enfrentamento psicossocial.[38] Nas pessoas entrevistadas, o exercício físico foi identificado como uma ferramenta para diminuir a ansiedade e dormir melhor.

---

38 Equipo de Acción Psicosocial y Acción Comunitaria. (2013). Reparar o invisível: Desafios para uma atenção psicossocial transformadora. Bogotá: Ediciones Antropos.

Uma pessoa disse:

> “Tentei equilibrá-lo com exercício. Nessa fase eu intensifiquei meus exercícios e vi que podia conciliar o sono, sobretudo as noites mal dormidas e tudo o que implicava. Além do impacto que o emocional também tem o físico, trabalhei isso com o exercício.” (E1).

O exercício reduz o estresse,[39] leva a pessoa a estar em outro lugar com a possibilidade de mudar de pensamentos, melhorar o estado de ânimo e a saúde em geral.

4. Apoio psicológico

Todas as pessoas entrevistadas dizem ter recebido apoio psicológico. Embora algumas já o estivessem recebendo, buscaram esse apoio por meio de algumas organizações. Isso as ajudou a trabalhar a ansiedade, a depressão e os transtornos do sono.

> “Eu já tinha minha terapeuta anterior, dois anos antes, não quis me enfiar em outro processo, enfrentei bem por isso, a terapeuta me ajudou muito.” (E5).

> “Eu já tinha um psicólogo com quem estava trabalhando lutos.” (E3).

O acompanhamento psicológico tem sido um apoio fundamental para as pessoas que tiveram acesso a ele, permitindo-lhes contar com alguém em quem podem confiar, com atendimento especializado.

5. Suporte técnico

Outra forma de enfrentamento é a busca por ajuda de pessoas especialistas em segurança digital para mitigar parte do estresse, ao compreender o que aconteceu e o que pode ser feito para enfrentar as situações de risco.

> “Tive aconselhamento de pessoas especializadas, mas de forma remota e, por não ter cabeça [para pensar], sim tive acompanhamento, mas nessa situação eram recomendações que eu tinha que implementar.” (E1).

Outro entrevistado afirma que fazer uma formação com especialistas pode ajudar a compreender melhor o que está acontecendo:

---

39 Lazarus, R. S., Valdés, M., Folkman, S. (1986). Estresse e processos cognitivos. Martínez Roca.

> “Melhorar o conhecimento sobre ferramentas, é preciso saber como o inimigo pensa, como executam estas coisas, para saber quais medidas tomar. Como colocar senhas em todos os dispositivos, como podemos ter o conhecimento para nos cuidarmos de forma mais natural, sem recorrer a coisas emergenciais.” (E4).

O suporte técnico funciona tanto para reduzir a solidão nesses momentos de estresse e preocupação quanto para obter mais informações, oferecendo maior sensação de controle diante de uma situação nova e intimidadora.

6. Rede de apoio

As redes de apoio são espaços onde o sofrimento é reconhecido, a experiência vivida é validada e existe confiança para iniciar processos de cura, justiça e transformação social. Não são apenas ferramentas funcionais, mas também espaços de cuidado ético, político e emocional.[40]

A busca por apoio social e a criação de vínculos com pessoas que podem entender esse tipo de agressão são muito importantes para as pessoas entrevistadas.

> "Eu fui construindo minha rede de apoio com pessoas com quem eu conversava sobre certos assuntos ou que eu vi que eram afetadas. O que se deve fazer é se conectar em vez de se isolar." (E1).

Isso é reforçado pelas pessoas de pertencimento com as quais nos identificamos:

40 Equipo de Acción Psicosocial y Acción Comunitaria. (2013). Reparar o invisível: Desafios para uma atenção psicossocial transformadora. Ediciones Antropos.

> "No apoio entre as organizações, vimos que, há três anos, acontece um grande esforço das organizações para formar redes."

> "Na comunidade de jornalistas é muito comum o apoio em rede, sobretudo em comunicados de imprensa." (entrevista em grupo).

O apoio social desempenha um papel fundamental no enfrentamento:

> "Tive muitos apoios, de amizades especialistas a fundações para jornalistas. Expliquei que não podia estar em um evento por problemas de saúde mental, falaram com uma organização aliada e me apoiaram com o pagamento de psiquiatras. Outra organização de mulheres jornalistas me apoiou com o impacto econômico que eu estava tendo e daí tive outros. E outros apoios, mais emocional, de pessoas que sempre estiveram presentes." (E1).

Como forma de enfrentamento, pessoas, sobretudo as que têm atuação pública, denunciam e se protegem coletivamente. Algumas entrevistas enfatizaram que, entre as formas de cuidado, é importante se agrupar como categoria, por exemplo, no jornalismo, para realizar denúncias públicas. Algumas das ações de solidariedade com a pessoa afetada incluem comunicados e coletivas de imprensa para mostrar que jornalistas não estão sós.

O humor e o riso são usados em ambientes de trabalho para reduzir a ansiedade, como explica uma entrevistada sobre como a violência era satirizada.

> "Minha mesa estava de costas, eu dizia a eles, 'eu sou a primeira que vão matar', os outros diziam, 'se nos pegar do lado da rua, quem vão matar sou eu'. Essas eram as piadas." (E5).

Em resumo, os grupos desenvolveram estratégias de enfrentamento como denúncia, riso, humor, apoio, solidariedade e defesa mútua.
Em muitos casos, as famílias são a rede de apoio, pois representam um espaço seguro para as pessoas vigiadas. Elas recorrem à família como o lugar onde podem mudar rotinas e se desconectar da sociedade civil, sentir-se apoiadas e acolhidas.

> "As pessoas decidem se refugiar com suas famílias, as que estão desconectadas da sociedade civil, então os custos não são tão altos e têm um espaço seguro de confiança, porque têm o acolhimento delas." (entrevista em grupo).

Um especialista em proteção explica:

> "Requer-se um trabalho amplo que sempre é feito em rede, no nosso caso fazemos parte de uma rede. Mas se você trabalha sozinha, o trabalho não pode ser levado adiante. A revisão técnica é só o primeiro passo, mas a análise não resolve o problema, é necessário trabalhar com advogados, advogadas, tomadoras de decisões, fazer avaliações a partir de outros âmbitos, para agir de forma muito mais ampla." (entrevista em grupo).

7. Apoio entre instituições

O apoio institucional é importante para o cuidado das pessoas afetadas por spyware.

> "Estive em um programa de cuidado com repórteres sem fronteiras e isso também me ajudou a trabalhar minha ansiedade, aprendi que a espionagem pode ser evitada, que é muito difícil. Mas há maneiras de limitar os riscos." (E3).

As organizações buscam melhorar o cuidado coletivo nas equipes, oferecendo atendimento psicológico e conectando as equipes a pessoas especialistas que podem auxiliar na segurança.

> "[a organização] disse que, se precisássemos de terapia, tínhamos 10 sessões." (E5).

Ao perguntar para quem trabalha apoiando pessoas afetadas por spyware como se protegem dos impactos, ouvimos:

> "Há um esforço pessoal, do meu lado, de distanciamento, para mim o trabalho é importante, mas consegui me distanciar e me dissociar para o entender como trabalho e que não entre na minha vida pessoal." (entrevista em grupo).

As pessoas e as equipes conseguiram encontrar formas de enfrentar a vulnerabilidade gerada pela instalação de spyware, oferecendo apoio psicológico, reforçando a segurança de dispositivos eletrônicos e celulares e promovendo capacitações para aprimorar práticas de segurança. Também expressam a necessidade de trabalhar em rede para garantir apoio. Estão se empenhando para formar redes capazes de abordar aspectos legais, tecnológicos, psicossociais e logísticos.

Conclusões

Segundo as entrevistas realizadas, o objetivo da instalação de spyware vai além da vigilância. O propósito é o controle, fomentar o sentimento de vulnerabilidade, criar uma sensação de ameaça e reprimir as pessoas pelo trabalho que realizam.

Nos casos das pessoas entrevistadas, a instalação de spyware veio acompanhada de outras agressões, como monitoramento físico, prisões de colegas próximas, ataques em redes sociais, deslocamentos e exílio, eventos que impactam a saúde mental e constituem um trauma sequencial e acumulativo. Os efeitos psicossociais se refletem nos âmbitos individual, coletivo, emocional, cognitivo e físico.

As pessoas viveram mudanças profundas na vida familiar, profissional e econômica, o que intensificou os impactos psicossociais. Os impactos psicossociais decorrentes do spyware aprofundaram níveis de ansiedade e depressão que, em alguns casos, já existiam antes dessas agressões.

A reação inicial diante da notícia apresentou dois padrões. Algumas pessoas reagiram com comoção, medo intenso, ansiedade e até pânico. Outras relataram reações mais contidas, por já esperarem que isso pudesse acontecer.

Entre as consequências identificadas está a hipervigilância, caracterizada por um estado de alerta extremo. Ela é acompanhada de ansiedade, afeta a capacidade de concentração e impacta o desempenho profissional e as

relações sociais. O medo intenso pode persistir e ser reativado por estímulos específicos, chegando a ser percebido como uma ameaça vital.

O projeto de vida foi profundamente impactado. Duas pessoas partiram para o exílio e deixaram seus trabalhos, sendo obrigadas a se adaptar a uma nova cultura, a outro idioma e a novas rotinas. Isso também resultou na separação de famílias e amizades.

No âmbito familiar, podem ocorrer reações de censura, assim como manifestações de acolhimento e apoio. As famílias também foram impactadas pelas separações.

O contexto social em que os ataques ocorrem é marcado por medo generalizado. A população evita expressar opiniões críticas ao governo, o que leva ao afastamento de amizades e pessoas próximas, por receio de sofrer represálias semelhantes.

Nas equipes de trabalho, os impactos variaram entre pânico e cansaço, sendo frequente a necessidade de implementar novas medidas de proteção diante da insegurança.

A economia das pessoas afetadas também foi impactada pelos gastos relacionados ao cuidado com a saúde, aos deslocamentos e à compra de novos dispositivos eletrônicos.

Entre os enfrentamentos identificados estão:

-Diminuir a exposição em redes sociais, alterar rotinas e circular por lugares diferentes, buscando recuperar alguma sensação de controle sobre o ocorrido e suas consequências.

-Refugiar-se junto à família como forma de reconexão com o bem-estar, fortalecimento de vínculos afetivos e sensação temporária de proteção.

-Fortalecer redes de apoio com amizades e pessoas próximas, o que constitui um importante mecanismo de enfrentamento e segurança coletiva.

-Em nível grupal, realizar ações conjuntas de denúncia, comunicados públicos e coletivas de imprensa, fortalecendo o sentimento de unidade e proteção coletiva.

-No âmbito organizacional, foram fortalecidos ou criados apoios interinstitucionais, proporcionando apoio, tanto tecnológico quanto psicológico, para enfrentar as consequências do spyware. As pessoas se sentem mais apoiadas e isso constitui, para elas, um fator de enfrentamento muito importante.

Recomendações

Trabalhar com organizações de direitos humanos, jornalistas e pessoas que atuam na justiça para prevenir futuras intervenções, orientar sobre como agir diante de ataques com spyware e fortalecer capacidades tecnológicas e logísticas, considerando também as especificidades de gênero nas agressões.

Fornecer acompanhamento psicossocial e apoio psicológico às pessoas que sofrem ataques com spyware, visando reduzir ansiedade, medo e hipervigilância.

Criar e fortalecer redes de apoio com pessoas que vivenciaram situações semelhantes, possibilitando trocas baseadas na experiência prática. Essas redes fortalecem vínculos sociais, promovem pertencimento e reduzem o isolamento.

Facilitar **acompanhamento psicossocial e formação em gestão emocional** para equipes que trabalham com pessoas e organizações que sofreram ataques com spyware.

Socializar e fortalecer a criação de fundos econômicos para oferecer às pessoas dispositivos de comunicação seguros, logística se necessitarem se mobilizar e instalar sistemas de segurança.

Em casos extremos, quando houver necessidade de saída do país, garantir recursos para o deslocamento e a instalação em outro território, bem como apoio em processos legais de migração.

Criar redes com profissionais que ofereçam assessoria jurídica em casos de criminalização.

Elaborar protocolos de atuação diante de ataques com spyware, que sirvam como guia para organizações suscetíveis a esse tipo de agressão e considerem as múltiplas violências associadas à vigilância.

Bibliografia

Access Now. (3 de maio de 2023). 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. (27 de março de 2021). 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). (3 de dezembro de 2019) 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. (16 de maio de 2024). 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. (14 de dezembro de 2023). ¿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. (9 de outubro de 2023) 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. y Durand, V. M. (2003): Psicopatología. Thomson.
Barrientos M., Najarro F. (26 de agosto de 2024). 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. (11 de março de 2025)
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).(31 de janeiro 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 imprensa].
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 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 janeiro 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.
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

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). (27 de janeiro de 2022). 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. (15 de junho de 2021). 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. (22 de setembro de 2018). 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. (12 de janeiro de 2022) 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. (2 de outubro de 2022). 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. (5 de junho de 2023). 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. (14 de março de 2023). 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