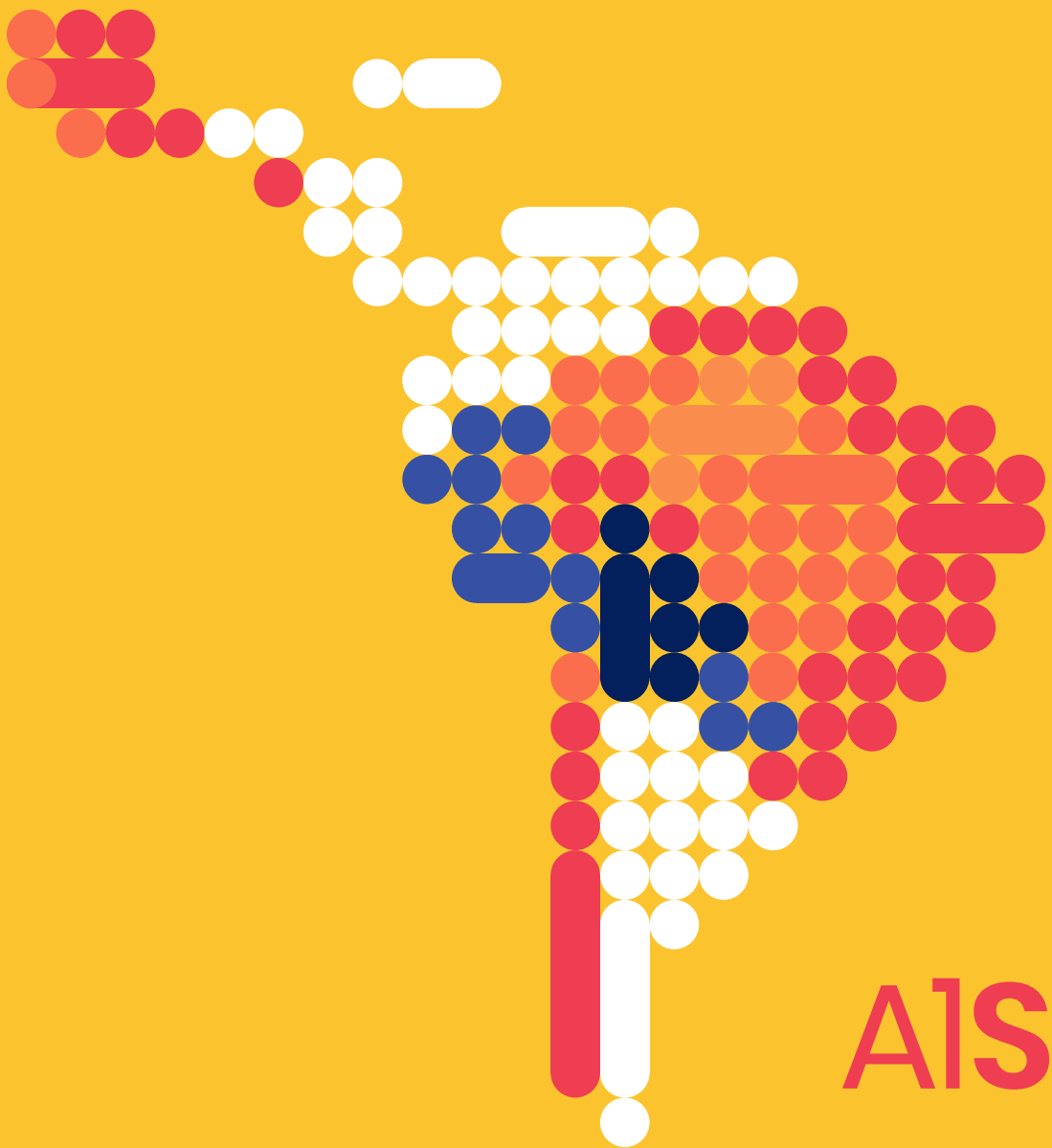
Tendências e práticas de vigilância na América Latina.

Estudos de caso de Brasil, Chile, Colômbia, El Salvador, México, Peru e Paraguai



AlSur

Tendências e práticas de vigilância na América Latina.

Estudos de caso de Brasil, Chile, Colômbia, El Salvador, México, Peru e Paraguai

COORDENAÇÃO:
Silvia Calderón, Instituto Panamericano de Direito e Tecnologia (IPANDETEC)
Ana Gaitán, Rede em Defesa dos Direitos Digitais (R3D)

AUTORIA E REVISÃO:
Helena Secaf - Centro de Pesquisa InternetLab
Vitor Vilanova - Centro de Pesquisa InternetLab
María Parra - *Fundação Karisma*
Lucia Camacho - Direitos Digitais
Laura Mantilla - Direitos Digitais
Maricarmen Sequera - TEDIC
Dilmar Villena - Hiperderecho
Ana Gaitán - Rede em Defesa dos Direitos Digitais (R3D)
Silvia Calderón - Instituto Panamericano de Direito e Tecnologia (IPANDETEC)

REVISÃO:
Camila Leite - Instituto de Defesa de Consumidores (IDEC)
Luã Cruz - Instituto de Defesa de Consumidores (IDEC)

DESIGN:
Marcelo Lazarle

ELABORADO PARA O CONSÓRCIO: AlSur

COM O FINANCIAMENTO DE: CHARLES STEWART MOTT FOUNDATION

Junho 2025

AlSur

"AlSur" é um consórcio de 11 organizações que trabalham na sociedade civil e no âmbito acadêmico na América Latina e que buscam com seu trabalho conjunto fortalecer os direitos humanos no entorno digital da região.

ORGANIZAÇÕES QUE COMPÕEM O AL SUR

- Associação pelos Direitos Civis (ADC) - Argentina
- Centro de Estudos em Liberdade de Expressão e Acesso à Informação (CELE) - Argentina
- Coding Rights - Brasil
- Direitos Digitais - Regional
- *Fundação Karisma* - Colômbia
- Hiperdireito - Peru
- Instituto Brasileiro de Defesa do Consumidor (IDEC) - Brasil
- Instituto Panamericano de Direito e Tecnologia – América Central
- InternetLab - Brasil
- Rede em Defesa dos Direitos Digitais (R3D) - México
- TEDIC - Paraguai

Índice

ÍNDICE DE TABELAS

Siglas

SIGLA	DEFINIÇÃO
ABIN	Agencia Brasileira de Inteligência
ADO	Ação Direta de Inconstitucionalidade por Omissão [Brasil]
ADPF	Arguição de Descumprimento de Preceito Fundamental [Brasil]
AFDD	Agrupação de Familiares de Detentos Desaparecidos [Chile]
AFEP	Agrupação de Familiares de Executados Políticos [Chile]
ANEF	Agrupação Nacional de Empregados Fiscais [Chile]
Bacib	Batalhões de Inteligência cibernética [Colômbia]
BIPE	Brigada de Investigações Policiais Especiais [Chile]
CADH	Convenção Americana de Direitos Humanos
Caso CAJAR	Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia
CIDH	Comissão Interamericana de Direitos Humanos
CNPP	Código Nacional de Procedimentos Penais [México]
Corte IDH	Corte Interamericana de Direitos Humanos
Córtex	Plataforma Integrada de Operações y Monitoramento de Segurança Pública [Brasil]
CUT	Central Unitária de Trabalhadores [Chile]
DIGIMIN	Departamento General de Inteligência [Peru]
DINI	Departamento Nacional de Inteligência [Peru]
FEADLE	Procuradoria Especial para Crimes contra a Liberdade de Expressão [México]
FECH	Federação de Estudantes da Universidade de Chile
FEDEUNAP	Federação de Estudiantes da Universidade Arturo Prat [Chile]
FGN	Corregedoria Geral da Nação [Colômbia]
FLIP	Fundação para a Liberdade de Imprensa
ISP	Internet Service Provider (Provedor de Serviços de Internet)
LGN	Lei da Guarda Nacional [México]
MJSP	Ministério de Justiça e Segurança Pública [Brasil]
MP	Ministério Público
OSIPTEL	Órgão Supervisor de Investimentos Privados em Telecomunicações [Peru]
PDI	Polícia Investigativa [Chile]
PGN	Procuradoria-Geral da Nação [Colômbia]
PGR	Procuradoria-Geral da República [Brasil]
PNP	Polícia Nacional do Peru
RdC	[Jornalista de] Rotas de Conflito [Colômbia]
RELE	Relatoria Especial para a Liberdade de Expressão
SEDENA	Secretaria de Defesa Nacional [México]
SEIDO	Sub-procuradoria Especializada em Investigação do Crime Organizado [México]
SEOPI	Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública [Brasil]
TEDH	Tribunal Europeu de Direitos Humanos
OACNUDH	Escritório Regional do Alto Comissariado das Nações Unidas para os Direitos Humanos para a América Central, República Dominicana e Caribe
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas

INTRODUÇÃO

Tanto a Assembleia Geral como o Conselho de Direitos Humanos das Nações Unidas (doravante, ONU) têm sublinhado que o direito à privacidade é um dos fundamentos das democracias e da liberdade de expressão pessoal e, como tal, desempenha um papel essencial na proteção e promoção de outros direitos, incluindo os direitos à liberdade de opinião, expressão, religião, reunião e associação.[1]

Dada a interligação dos direitos humanos, os efeitos adversos das violações da privacidade podem acarretar também violações de direitos como a igualdade perante a lei, o direito à vida, à liberdade e à integridade pessoal, a um julgamento justo e ao devido processo legal, o direito à liberdade de expressão, de protesto e de associação, à liberdade de circulação, ao mais alto nível possível de saúde e ao acesso ao trabalho e à segurança social, entre outros.[2]

Nessa linha, tanto o Alto Comissariado das Nações Unidas para os Direitos Humanos quanto a Relatoria Especial da ONU sobre a promoção e proteção do direito à liberdade de opinião e expressão determinaram que a vigilância das comunicações privadas tem repercussões na sociedade civil e no discurso democrático.[3] O risco de ser um objeto de vigilância e o desejo de evitar ser alvo da mesma levam as pessoas a se autocensurarem. Quando as pessoas se sentem vigiadas, elas alteram e limitam a forma como se expressam e se comunicam com outras pessoas. Devido a esse *"efeito intimidatório" (chilling effect)*, as tecnologias de vigilância não afetam apenas as pessoas cujos dados são coletados, mas toda a sociedade, ao interferir direta e indiretamente na livre troca e evolução de ideias.[4]

Historicamente, as atividades de inteligência realizadas na América Latina, seja por autoridades civis, policiais ou militares, longe de servir aos interesses gerais da sociedade, constituíram-se elas próprias como um risco para o respeito à dignidade e aos direitos das pessoas.

Atualmente, tem sido documentado o uso progressivo por parte dos governos de tecnologias para a vigilância das comunicações com o objetivo de reprimir, censurar e perseguir defensores dos direitos humanos, jornalistas, ativistas sociais e opositores políticos.[5] Essa vigilância colocou em risco sua vida e integridade pessoal e impediu a denúncia e a prestação de contas de atos de corrupção e violações dos direitos humanos cometidos por autoridades públicas e pessoas ou instituições privadas.

---

1 Nações Unidas. Assembleia Geral. (2017). Resolução A/RES/71/199 O direito à privacidade na era digital. Disponível em: https://documents.un.org/doc/undoc/gen/n16/455/37/pdf/n1645537.pdf,
Nações Unidas. Assembleia Geral. (2018). Resolução A/RES/73/179. O direito à privacidade na era digital. Disponível em: https://docs.un.org/es/A/res/73/179 y,
Nações Unidas. Assembleia Geral. (2017). Resolução A/HRC/RES/34/7. O direito à privacidade na era digital. Disponível em: https://docs.un.org/es/A/HRC/RES/34/7

2 Huszti-Orbán, K., Ní Aoláin, F. (2020). Uso de dados biométricos para identificar terroristas: Melhores práticas ou negócios arriscados?. Disponível em:
https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf

3 Veja, por exemplo, Assembleia Geral de Nações Unidas (2016). Resolução A/HRC/32/38. Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e de expressão. Disponível em: https://docs.un.org/es/a/hrc/32/38

4 Nações Unidas. Assembleia Geral. (2013). Resolução A/HRC/23/40. Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e de expressão, Frank La Rue. Parágrafo. 24. Disponível em: https://docs.un.org/es/A/HRC/23/40

5 Nações Unidas. Assembleia Geral. (2019). Resolução A/HRC/41/35. Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e de expressão. Parágrafo. 24. Disponível em: https://docs.un.org/es/A/HRC/41/35

Da mesma forma, a maioria das medidas de vigilância atuais envolve a coleta e o armazenamento massivo e indiscriminado de informações sobre as comunicações privadas de milhões de pessoas, a grande maioria das quais não está envolvida na prática de atos criminosos. O acesso ao conteúdo de nossas comunicações, bem como a análise dos metadados associados a elas, como os dados de localização, confere ao Estado um alto poder invasivo e controle sobre todas as pessoas, além de atentando contra a autonomia e a participação cívica.

Além disso, as tecnologias disponíveis para realizar essas atividades estão se tornando cada vez mais sofisticadas. A proliferação de tecnologias de vigilância em massa, como antenas falsas, terceirização de vigilância em massa ou tecnologias de vigilância focada altamente invasivas e evasivas, como *spyware*, é indicativa da pouca clareza e precisão sobre os métodos de vigilância que atualmente podem ser considerados compatíveis com as normas de direitos humanos.

Assim, o presente relatório, *Tendências e práticas de vigilância na América Latina*, é particularmente relevante no contexto em que nos encontramos: democracias em deterioração, proliferação do crime organizado e aumento do autoritarismo. Diante da massificação sem controles das tecnologias de vigilância das comunicações, é essencial pressionar por um maior escrutínio, controle e regulamentação dessas ferramentas.

Por isso, este relatório documenta algumas das maneiras pelas quais diversas tecnologias de vigilância são utilizadas de forma opaca, secreta, discricionária e abusiva por autoridades sem poderes legais e sem garantias adequadas para prevenir, mitigar ou remediar tais abusos.

É importante esclarecer que, ao nos referirmos às tendências e práticas de vigilância, essa categoria abrange todas as técnicas e tecnologias de propriedade ou uso estatal com capacidade de interferir, limitar ou afetar o exercício do direito à privacidade, independentemente de sua implantação estar ou não amparada pelo marco legal local.

Entre as técnicas e práticas de vigilância, aquelas que se concentram nas comunicações privadas são apenas uma tipologia entre uma taxonomia mais complexa de modalidades de vigilância. Portanto, embora o relatório se concentre nas comunicações privadas, ele também explora outras modalidades e técnicas de vigilância estatal que geram preocupação por seu impacto em direitos humanos.

Por exemplo, entre as técnicas e tecnologias de vigilância focadas nas comunicações,[6] entre elas estão a interceptação de comunicações por meio de seus intermediários, os provedores de serviços de internet; a solicitação de dados e metadados dos assinantes de serviços de telecomunicações; a interceptação direta e direcionada de comunicações pelos Estados, por exemplo, através do uso de software malicioso – *spyware*; o uso de técnicas de vigilância focadas no monitoramento de redes sociais e da internet – como o ciberpatrulhamento –; o uso de tecnologias que interceptam sinais da infraestrutura de comunicações e dispositivos móveis – como stingrays ou IMSI-Catchers –, entre outros.

No entanto, existem outras formas de vigilância estatal cujo foco não recai sobre as comunicações, mas sim no rastreamento de pessoas, como, por exemplo, a implantação e o uso de sistemas de reconhecimento facial – que exploramos em um relatório da AlSur de 2021[7] e em outro mais publicado em 2025[8]–; bem como a implantação e utilização de sistemas de reconhecimento de matrículas de veículos, entre outros.

---

6 Diferentes modalidades de vigilância massiva focadas nas comunicações das pessoas se abordam nos relatórios A/HRC/23/40 de abril de 2013; e no relatório A/HRC/41/35 de maio de 2019, ambos da Relatoria Especial para a Liberdade de Expressão das Nações Unidas.

7 Venturini, J.; Garay, V. (2021). Reconhecimento facial na América Latina. Tendências na implementação de uma tecnologia perversa. AlSur. Disponível em: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

8 Será publicado em breve.

Este relatório é resultado da investigação sobre práticas de vigilância na América Latina realizada pelas organizações da AlSur na Colômbia, Chile, Peru, México, Paraguai e Brasil. A investigação foi realizada através do monitoramento e documentação que cada uma das organizações participantes realizou em seu respectivo país. A pesquisa delimitou seu alcance temporal desde o ano de 2016 – quando o uso de medidas de vigilância das comunicações começou a se tornar exponencialmente visível na região – até o final de 2024.

É importante mencionar que, em muitos casos, a legalidade de seu uso é questionável e, na maioria dos casos, existe uma opacidade generalizada em relação ao seu uso. No entanto, a compilação também incluiu dados sobre o panorama legislativo, ações do governo e entidades de segurança, administrativas e judiciais.

No *capítulo 1*, o relatório compila os padrões de direitos humanos aplicáveis à vigilância das comunicações. O *capítulo 2* identifica as normas e procedimentos que regulam a vigilância das comunicações em diferentes países da região. O *capítulo 3* documenta casos emblemáticos em que foram utilizadas técnicas de vigilância das comunicações na região. Por fim, o *capítulo 4* faz um diagnóstico das tendências e práticas na América Latina, com o objetivo de destacar as deficiências normativas, a opacidade e as irregularidades na aquisição de tecnologias de vigilância, a vigilância ilegal e a impunidade que têm existido em relação à vigilância das comunicações. O relatório encerra com a apresentação de conclusões e recomendações para os Estados sobre a regulamentação da matéria.

CAPÍTULO UM: NORMAS DE DIREITOS HUMANOS APLICÁVEIS À VIGILÂNCIA DE COMUNICAÇÕES

O direito à privacidade e à proteção de dados pessoais são direitos humanos fundamentais, embora nem sempre sejam reconhecidos como distintos e autônomos, apesar de sua relação e interdependência. Trata-se de direitos reconhecidos em amplos instrumentos de direitos humanos, tanto no âmbito internacional[9] quanto no regional.[10]

A nível interamericano, o Tribunal Interamericano de Direitos Humanos (doravante, "Tribunal IDH") definiu a vida privada como um direito que: "abrange uma série de fatores relacionados com a dignidade do indivíduo, incluindo, por exemplo, a capacidade de desenvolver a própria personalidade e aspirações, determinar a própria identidade e definir as próprias relações pessoais."[11]

Em uma interpretação mais recente do conteúdo da CADH e do corpus iuris interamericano[12], A Corte Interamericana de Direitos Humanos estabeleceu que as normas internacionais de proteção de dados pessoais exigem que o seu processamento ocorra somente com o consentimento livre e informado do titular dos dados ou com base em um marco normativo que autorize tal processamento.[13]

A proteção que todas as pessoas têm, nos termos do direito internacional dos direitos humanos, a uma vida privada e familiar sem interferências arbitrárias, bem como à proteção de seus dados pessoais, se estende às suas comunicações digitais.[14] Assim, a Corte IDH também se pronunciou sobre a proteção da vida privada no âmbito do processo de comunicação, incluindo os metadados, enfatizando que seus critérios "têm plena aplicação em torno de atividades de inteligência que envolvam a vigilância [desses metadados]".[15]

No entanto, o direito à privacidade não é um direito absoluto, e o uso de atividades de inteligência pode ter fins legítimos e ser um meio útil para a investigação de crimes e o combate a ameaças à segurança nacional. As limitações legítimas ao direito à privacidade devem estar alinhadas com os padrões de direitos humanos. Nesse sentido, a Corte IDH determinou que "as medidas destinadas a controlar as atividades de inteligência devem ser especialmente rigorosas, uma vez que, dadas as condições de sigilo sob as quais essas atividades são realizadas, elas podem levar à prática de violações dos direitos humanos e de crimes penais.[16]

---

9 Declaração Universal dos Direitos Humanos (art. 12), o Pacto Internacional de Direitos Civis e Políticos (art. 17), a Convenção sobre os Direitos da Criança (art. 16), a Convenção Internacional sobre a Proteção dos Direitos de todos os Trabalhadores Migrantes e de seus Familiares (art. 14), incluída a Observação Geral Nro.16 do Comitê de Direitos Humanos da ONU de 1988, entre outros instrumentos universais dos direitos humanos.

10 Convenção Americana de Direitos Humanos (doravante, "CADH"), Convenção Interamericana sobre a Proteção dos Direitos Humanos dos Idosos, art. 11; art 12, c, ii.; enriquecido, ainda, pelos Princípios Atualizados sobre a Privacidade e a Proteção de Dados Pessoais de 2021, entre outros.

11 Corte IDH. Caso Artavia Murillo e outros (Fecundação in vitro) Vs. Costa Rica. Exceções Preliminares, Fundo, Reparações e Custas. Sentença de 28 de novembro de 2012. Parágrafo. 143.

12 Integrado, ainda, pelos "Princípios Atualizados do Comitê Jurídico Interamericano sobre a Privacidade e a Proteção de Dados Pessoais, com Anotações", OEA/Ser.D/XIX.20, janeiro de 2022.

13 Corte IDH. Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia, Sentença de 18 de outubro de 2023, Exceções Preliminares, Fundo, Reparações e Custas, parágrafo. 573.

14 Distintos órgãos de direitos humanos adotaram uma perspectiva expansiva sobre o que entra no âmbito de proteção da intimidade no contexto digital, incluindo: a vigilância audiovisual (El Haski c. Bélgica [2012] TEDH 2019; (2013) 56 EHRR 31, [102]); os metadados (Malone c. Reino Unido [1984] TEDH 10; (1985) 7 EHRR 14, [84]); e a informação de geolocalização (Uzun c. Alemanha [2010] TEDH 2263; (2011) 53 EHRR 24, [12]-[13]).

15 Corte IDH. Caso Escher e outros Vs. Brasil, supra, parágrafo. 114; e parágrafo 543.

16 Corte IDH. Caso Myrna Mack Chang Vs. Guatemala. Fundo, Reparações e Custas. Sentença de 25 de novembro de 2003. Série C Nro. 101, parágrafo. 284.

Assim, para que as restrições aos direitos à privacidade e à proteção de dados pessoais cumpram as normas nacionais, regionais [17],[18],[19] e internacionais[20] na matéria e proíbam medidas de vigilância ilegais e arbitrárias, devem ser cumpridos os requisitos de legalidade, finalidade legítima, adequação, necessidade e proporcionalidade[21], o que, por sua vez, implica o estabelecimento de garantias adequadas para prevenir, evitar e remediar o exercício abusivo das mesmas.

I. Princípio da reserva da lei: Definição clara, precisa e detalhada das autoridades competentes, do procedimento e das circunstâncias em que podem ser realizadas medidas de vigilância.

Segundo a Corte IDH, a reserva da lei ou a expressão "leis", às quais a CADH se refere como meio habilitador para a limitação de direitos (art. 30), vai além do princípio da legalidade formal, abrangendo todos os atos normativos legítimos, focados no bem comum e emanados de órgãos constitucionalmente e democraticamente eleitos.[22]

Por sua parte, a Declaração Conjunta sobre Programas de Vigilância e seu Impacto na Liberdade de Expressão sustenta que:

> Os Estados devem garantir que a interceptação, a coleta e a utilização de informações pessoais (...) sejam claramente autorizadas pela lei, a fim de proteger a pessoa contra interferências arbitrárias ou abusivas nos seus interesses privados. A lei deve estabelecer limites quanto à natureza, ao âmbito e à duração deste tipo de medidas, às razões para as ordenar, às autoridades competentes para as autorizar, executar e supervisionar e aos mecanismos legais para as contestar.[23]

---

17 Princípios Internacionais sobre a Aplicação dos Direitos Humanos à Vigilância das Comunicações. Disponível em: https://necessaryandproportionate.org/es/necesarios-proporcionados

18 CIDH. Relatoria Especial para a Liberdade de Expressão. Liberdade de Expressão e Internet. 31 de dezembro de 2013. OEA/Ser.L/V/II, parágrafo 165.

19 Corte IDH, Caso Myrna Mack Chang v. Guatemala, supra. Caso Myrna Mack Chang v. Guatemala, supra; Caso Maritza Urrutia v. Guatemala. Mérito, Reparações e Custas. Sentença de 27 de novembro de 2003. Série C No. 103; Caso Huilca Tecse v. Peru. Mérito, Reparações e Custas. Sentença de 3 de março de 2005. Série C No. 121; Caso Blanco Romero e outros contra Venezuela. Mérito, Reparações e Custas. Sentença de 28 de novembro de 2005. Série C No. 138; Caso Goiburú e outros Vs. Paraguai, supra; Caso La Cantuta Vs. Mérito, Reparações e Custas. Sentença de 29 de novembro de 2006. Série C No. 162; Caso Escher et al. v. Brasil, supra; Caso Anzualdo Castro v. Peru. Objeção Preliminar, Mérito, Reparações e Custas. Sentença de 22 de setembro de 2009. Série C No. 202; Caso Gelman v. Uruguai. Mérito e Reparações. Sentença de 24 de fevereiro de 2011. Série C No. 221; Caso González Medina e familiares v. República Dominicana. Exceções Preliminares, Mérito, Reparações e Custas. Sentença de 27 de fevereiro de 2012. Série C No. 240; Caso Gudiel Álvarez e outros ("Diário Militar") Vs. Guatemala, supra; Caso García e familiares mais próximos Vs. Guatemala, supra; Caso Irmãos Landaeta Mejías e outros Vs. Venezuela, supra; Caso Rodríguez Vera e outros (Desaparecidos do Palácio da Justiça) Vs. Colômbia, supra; Caso da Família Julien Grisonas Vs. Argentina, supra; Caso Maidanik e outros Vs. Mérito e Reparações. Sentença de 15 de novembro de 2021. Série C No. 444; Caso Movilla Galarcio et al. v. Colômbia, supra, e Caso Deras García e outros Vs. Honduras. Fundo, Reparações e Custas. Sentença de 25 de agosto de 2022. Série C No. 462.

20 Nações Unidas. Assembleia Geral. (2010). Resolução A/HRC/14/46. Relatório de Martin Scheinin, Relator Especial sobre a promoção e proteção dos direitos humanos e liberdades fundamentais no combate ao terrorismo. Disponível em: https://docs.un.org/es/A/HRC/14/46; Nações Unidas. Assembleia Geral. (2013). Resolução A/HRC/23/40. Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, Frank La Rue. Disponível em: https://docs.un.org/es/A/HRC/23/4; Nações Unidas. Assembleia Geral. (2014). Resolução A/HRC/27/37. The right to privacy in the digital age, Relatório do Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos. Disponível em: https://docs.un.org/es/A/HRC/27/37 e; Nações Unidas. Assembleia Geral. (2020). Resolução A/RES/75/176. O direito à privacidade na era digital. Disponível em: https://docs.un.org/es/A/RES/75/176

21 Corte IDH, Caso Tristán Donoso v. Panamá, supra, par. 56. Caso Tristán Donoso v. Panamá, supra, par. 56, e Caso Fernández Prieto e Tumbeiro v. Argentina. Mérito e Reparações. Sentença de 1º de setembro de 2020. Série C No. 411, par. 105.

22 Corte IDH. Parecer OC-6/86 de 9 de maio de 1986. A expressão "leyes" no artigo 30 da Convenção Americana sobre Direitos Humanos. Disponível em: https://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf

23 CIDH. (2013). Declaração conjunta sobre programas de vigilância e seu impacto na liberdade de Expressão. Disponível em: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

A Relatoria para a Liberdade de Expressão (doravante RELE) estabeleceu que, no contexto das medidas de vigilância, a lei deve ser suficientemente clara em seus termos para fornecer aos cidadãos uma indicação adequada sobre as condições e circunstâncias em que as autoridades estarão facultadas a recorrer a tais medidas.[24] De igual maneira, salientou que:

> As *normas legais vagas ou ambíguas* que conferem amplos poderes discricionários são incompatíveis com a Convenção Americana, pois *podem sustentar potenciais atos de arbitrariedade que se traduzem na violação do direito à privacidade ou do direito à liberdade de pensamento e expressão* garantidos pela Convenção.[25]

Na mesma linha, a Corte IDH indicou que a primeira exigência no exercício de atividades de inteligência refere-se justamente ao *princípio da reserva* da lei para a proteção eficaz dos direitos e ao "controle adequado do exercício das competências dos órgãos" estatais.[26]

No que diz respeito aos controles e limitações a que devem estar sujeitas as atividades de inteligência, a Corte Interamericana de Direitos Humanos determinou mais recentemente que as atividades de inteligência devem ser regulamentadas com a maior precisão possível, definindo os métodos autorizados para coletar informações, os objetivos, as pessoas e atividades sujeitas a vigilância, o grau de suspeita que justifica a obtenção, os prazos permitidos para essas medidas e os métodos de supervisão e controle.[27]

Além disso, no caso de ser permitido o intercâmbio de informações entre órgãos de inteligência, devem ser especificadas condições claras, fins legítimos, autoridades competentes e garantias para proteger especialmente os dados pessoais.[28]

Da mesma forma, é necessário que todas as atividades sejam formalizadas por meio de processos numerados, incluindo controles sobre o acesso aos sistemas, e que o processamento de dados pessoais conte com registros que identifiquem: i. os responsáveis; ii. os fins do processamento; iii. a base legal; iv. os prazos de conservação; e v. os métodos utilizados, bem como um histórico de todas as ações realizadas sobre esses dados.[29]

Da mesma forma, em termos de coleta de dados pessoais, a Corte IDH prevê que as competências dos serviços de inteligência (que geralmente são exercidas sem o consentimento do titular) devem basear-se em leis que descrevam:

> a) os motivos que justificam a existência de arquivos com dados pessoais por parte dos órgãos de inteligência; tais motivos, de acordo com os fins próprios das atividades de inteligência, deverão limitar a atuação das autoridades nesta matéria; b) os tipos e classes de dados pessoais que as autoridades estão autorizadas a conservar em seus arquivos, e c) os parâmetros aplicáveis para a utilização, conservação, verificação, retificação, eliminação ou revelação desses dados [...].[30]

---

24 Corte IDH. Caso Escher e outros vs. Brasil. Exceções Preliminares, Fundo, Reparações e Custas. Sentença de 6 de julho de 2009. Série C No. 200.

25 CIDH. Relatoria Especial para a Liberdade de Expressão. Liberdade de Expressão e Internet. 31 de dezembro de 2013. OEA/Ser.L/V/II.

26 Corte IDH. Parecer OC-6/86, supra, parágrafo 24. Reiterado em Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia, Sentença de 18 de outubro de 2023, Exceções Preliminares, Fundo, Reparações e Custas. Parágrafo 529.

27 Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia, Sentença de 18 de outubro de 2023, Exceções Preliminares, Fundo, Reparações e Custas, parágrafo 520.

28 Ibidem, parágrafo 539.

29 Ibidem, parágrafo 540.

30 Ibidem, parágrafo 577.

II. Princípios da necessidade e da proporcionalidade: garantias contra abusos.

Presume-se *(i)* uma finalidade constitucionalmente válida (de interesse jurídico preponderante e necessário numa sociedade democrática), *(ii)* adequação (adequação da restrição no direito à sua finalidade), *(iii)* necessidade da medida (o meio menos propenso a violar os direitos humanos) e *(iv)* seu estudo de proporcionalidade em sentido estrito (entre o grau de intervenção no direito fundamental que a medida legislativa examinada supõe e o grau de realização do objetivo por ela perseguido).

Por fim, é necessário que existam *(v) garantias*, como o controle judicial (prévio ou imediato às medidas invasivas), transparência e supervisão independente (com prestação de contas) e o direito de notificação (às pessoas afetadas quando a vigilância tiver sido concluída).

1. Finalidade constitucionalmente válida

Embora a interceptação de comunicações e outras invasões da privacidade das pessoas sejam, em muitos casos, interferências na privacidade que perseguem fins legítimos, como a investigação de crimes graves e a proteção da segurança nacional, também é claro que existem riscos inerentes de abuso.

Portanto, em primeiro lugar, as medidas de vigilância devem identificar os objetivos que perseguem para depois determinar se são constitucionalmente válidas.[31] Assim, as leis só deveriam permitir a vigilância das comunicações por parte de autoridades estatais específicas para atingir um objetivo legítimo que corresponda a um interesse jurídico preponderante e necessário em uma sociedade democrática. Nas palavras do Conselho de Direitos Humanos, a vigilância legal e específica das comunicações digitais pode ser uma medida necessária e eficaz para atividades de inteligência por motivos de segurança nacional, prevenção do terrorismo ou outros crimes. Pode ser um objetivo legítimo, desde que o grau de interferência seja compatível com a necessidade e o benefício da medida para o objetivo e que seja respeitado o artigo 17 do Pacto.[32]

Na mesma linha, na referida Declaração Conjunta sobre Programas de Vigilância e seu Impacto na Liberdade de Expressão, sustenta-se que:

> Quando a segurança nacional for invocada como motivo para vigiar a correspondência e os dados pessoais, a lei deve especificar claramente os critérios a serem aplicados para determinar os casos em que esse tipo de limitação é legítimo. Sua aplicação só deve ser autorizada quando houver um risco real aos interesses protegidos e quando esse dano for superior ao interesse geral da sociedade em manter o direito à privacidade, à liberdade de expressão e à circulação de informações.[33]

Nesse sentido, a Corte IDH especifica que os objetivos acima se revelam como "fins legítimos", em função de sua correspondência com um Estado de Direito que sempre zela pela proteção dos direitos das pessoas.[34] Assim, enunciados vagos e imprecisos não poderão justificar a atuação dos órgãos de inteligência, pois isso implicaria afastar-se desses fins, ou mesmo contradizê-los ou anulá-los.[35]

---

31 SCJN. Recurso de revisão 237/2014. Relator: Arturo Zaldívar Lelo de Larrea. Aprovado por maioria de votos. Deste precedente surge a Tese Isolada 1a. CCLXV/2016 (10a.) PRIMEIRA ETAPA DO TESTE DE PROPORCIONALIDADE. IDENTIFICAÇÃO DE UMA FINALIDADE CONSTITUCIONALMENTE VÁLIDA. Registro 2013143

32 Nações Unidas. Assembleia Geral. (2014). Resolução A/HRC/27/37. O direito à privacidade na era digital. parágrafo 24.

33 CIDH. (2013). Declaração conjunta sobre programas de vigilância e seu impacto na Liberdade de Expressão. Disponível em: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2

34 Corte IDH. Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia, Sentença de 18 de outubro de 2023, Exceções Preliminares, Fundo, Reparações e Custas. Parágrafo 533.

35 Ibidem, parágrafo 532.

2. Idoneidade da medida

Em segundo lugar, o grau de *adequação* determina se a medida contestada é adequada para atingir os objetivos perseguidos pelo legislador ou pela autoridade.[36] Ou seja, deve existir uma relação entre a restrição no direito e o objetivo que essa afetação persegue.

O exame de adequação pressupõe a comprovação de um nexo causal entre a medida da autoridade e sua finalidade imediata. A Suprema Corte de Justiça da Nação do México indicou que essa conexão causal entre o meio e o fim "deve ser estabelecida com premissas empíricas obtidas a partir de conhecimentos gerais aceitos na sociedade e conhecimentos especializados da ciência e da técnica".[37]

3. Necessidade da medida

A vigilância das comunicações só deve ser realizada quando for o único meio para atingir um objetivo legítimo ou, quando houver vários meios, for o menos propenso a violar os direitos humanos. O ônus de estabelecer essa justificativa, tanto nos processos judiciais quanto nos legislativos, recai sobre o Estado.

O segundo passo do estudo do grau de necessidade consiste em analisar se a medida proposta é menos prejudicial. Ou seja, quando as medidas de vigilância implicam a coleta e o armazenamento maciço e indiscriminado de informações sobre as comunicações privadas de, por exemplo, milhões de usuários de telecomunicações e serviços financeiros online, a grande maioria dos quais nunca estará envolvida na prática de atos criminosos, o princípio da necessidade deve levar a avaliar se existem medidas menos prejudiciais aos direitos das pessoas que não estão ligadas à investigação em questão, a fim de alcançar o objetivo pretendido.

4. Estudo da proporcionalidade no sentido estrito da medida

Essa análise requer comparar o grau de intervenção ou limitação da privacidade que a medida em questão acarreta, avaliada em relação ao grau de realização do objetivo por ela perseguido. O grau de impacto é potencializado pelo fato de que as medidas de vigilância tendem a implicar a coleta massiva e indiscriminada de informações de milhões de pessoas, a grande maioria das quais nunca estará envolvida na investigação de qualquer crime. O uso de ferramentas de vigilância das comunicações para fins de prevenção do crime é, portanto, desproporcional.[38] Além disso, as informações retidas para esse fim costumam ser excessivas em comparação com a ameaça que se pretende combater.

De acordo com a Corte IDH, uma medida que interfere com um direito só pode ser considerada *necessária* se não existir uma medida alternativa menos lesiva do direito para alcançar o objetivo legítimo[39], e proporcional, se a afetação ao direito humano não for exagerada ou desproporcional em relação às vantagens obtidas por meio dessa limitação.[40]

---

36 SCJN. Amparo em revisão 237/ 2014. Relator: Arturo Zaldívar Lelo de Larrea. Aprovado por maioria de votos. A partir desse precedente, surge a tese isolada 1a. CCLXVIII/2016 (10a.) "SEGUNDA ETAPA DEL TEST DE PROPORCIONALIDADE. EXAME DA IDONEIDADE DA MEDIDA LEGISLATIVA". Registro: 2013152.

37 SCJN. Amparo em revisão 163/2018 Citando a [1] Bernal Pulido, Carlos, O princípio da proporcionalidade e os direitos fundamentais, 2ª ed., Madrid, CEPC, 2005, p. 727.

38 SURVEILLE. (2015). "Surveillance: Ethical Issues, Legal Limitations,and Efficiency", Disponível em: https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.10-Synthesis-report-from-WP4.pdf p. 22

39 Corte IDH. (2008). Caso Kimel vs. Argentina, Sentença de 2 de maio de 2008, Série C No. 177, parágrafo 74.

40 Ibidem, parágrafo 83.

A importância de garantias eficazes contra o abuso de medidas de vigilância eletrônica secreta também foi destacada pela Assembleia Geral da Organização das Nações Unidas,[41] Relatoria Especial da ONU para o Direito à Liberdade de Expressão e Opinião, o Gabinete do Alto Comissariado para os Direitos Humanos da ONU,[42] a RELE[43], bem como por organizações da sociedade civil e especialistas que reuniram as melhores práticas derivadas da jurisprudência e da doutrina comparada e elaboraram os Princípios Internacionais sobre a Aplicação dos Direitos Humanos à Vigilância das Comunicações.[44]

III. Garantias

Entre as opções de garantia adicionais estão (i) o controle judicial, (ii) a transparência e supervisão independente e (iii) a notificação às pessoas afetadas pelas medidas de vigilância estatal.

1. Controle judicial

Uma das garantias fundamentais para inibir os riscos de abuso das medidas de vigilância secreta é o controle judicial. A importância fundamental do controle judicial, prévio ou imediato, foi destacada pela RELE:

> As decisões de realizar tarefas de vigilância que invadam a privacidade das pessoas *devem ser autorizadas por autoridades judiciais independentes*, que devem explicar as razões pelas quais a medida é adequada para atingir os objetivos pretendidos no caso específico; se é suficientemente restrita para não afetar o direito envolvido mais do que o necessário; e se é proporcional ao interesse que se pretende promover.[45]

No mesmo sentido, a Corte Interamericana de Direitos Humanos estabeleceu que é imprescindível que sejam as autoridades judiciais as responsáveis por autorizar "medidas invasivas de coleta de informações", ou seja, os métodos de obtenção de informações como escuta e gravação eletrônica, incluindo audiovisual, bem como a pretensão dos órgãos de inteligência de requerer informações referentes a dados pessoais a empresas de telecomunicações, para o que é necessária autorização judicial.[46]

A Corte IDH também reconhece que o direito à privacidade exige garantias específicas em relação ao uso de novas tecnologias quando se trata de atividades de inteligência. Por isso, é indispensável contar com autorização judicial prévia para aplicar métodos de vigilância dirigidos a pessoas específicas, especialmente se isso implicar o acesso a bases de dados e sistemas de informação privados que contenham dados pessoais, rastrear usuários online ou localizar dispositivos eletrônicos.[47]

---

41 Nações Unidas. Assembleia Geral. (2013). Resolução A/RES/68/167 sobre o direito à privacidade na era digital. Disponível em: https://docs.un.org/es/A/RES/68/167

42 Nações Unidas. Assembleia Geral. (2014). Resolução A/HRC/27/37. O direito à privacidade na era digital, Relatório do escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos. Parágrafo 37. Disponível em: https://docs.un.org/es/A/HRC/27/37: "O artigo 17, parágrafo 2, do Pacto Internacional sobre Direitos Civis e Políticos estabelece que toda pessoa tem direito à proteção da lei contra interferências ou ataques ilegais ou arbitrários (...) Garantias internas, sem monitoramento externo independente, têm se mostrado particularmente ineficazes contra métodos de vigilância ilegais ou arbitrários. Embora essas garantias possam assumir diversas formas, o envolvimento de todos os níveis do governo na supervisão dos programas de vigilância, juntamente com a supervisão por parte de uma agência civil independente, é essencial para garantir uma proteção eficaz da lei." (tradução própria)

43 CIDH. (2013). Relatoria Especial para a Liberdade de Expressão, Liberdade de Expressão e Internet, 31 de dezembro de 2013, OEA/Ser.L/V/II.

44 Ver: Princípios Internacionales sobre a Aplicação dos Direitos Humanos à Vigilância das Comunicações. Disponível em: https://es.necessaryandproportionate.org/text

45 CIDH. Relatoria Especial para a Liberdade de Expressão, Liberdade de Expressão e Internet. (2013). OEA/Ser.L/V/II, parágrafo 165.

46 Corte IDH. (2023). Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia, Sentença de 18 de outubro de 2023, Exceções Preliminares, Fundo, Reparações e Custas, parágrafos. 542, 547 e 551.

47 Ibidem, parágrafo 553.

Da mesma forma, reforça a noção de proteção especial que requer a informação obtida e classificada como "dados sensíveis", que abrange aqueles que afetam aspectos mais íntimos das pessoas e podem revelar aspectos como saúde, orientação sexual, crenças religiosas, filosóficas, políticas ou morais, afiliações, dados genéticos, dados biométricos, financeiros ou relacionados com menores de idade e geolocalização pessoal. Esses dados permitem elaborar perfis detalhados e, devido ao seu impacto e potencial para discriminar seu titular, exigem uma proteção reforçada.[48]

Da mesma forma, foram reconhecidas outras garantias indispensáveis para inibir os riscos inerentes ao abuso das medidas de vigilância, tais como medidas de transparência e supervisão independente ou o direito de notificação à pessoa afetada.

2. Medidas de transparência e supervisão independente

A RELE destacou que "os Estados devem estabelecer mecanismos de supervisão independentes sobre as autoridades encarregadas de realizar as tarefas de vigilância"[49].

Da mesma forma, a Relatoria Especial sobre o Direito à Liberdade de Opinião e Expressão da ONU recomendou aos Estados que estabeleçam ou mantenham "mecanismos nacionais de supervisão independentes e eficazes, capazes de garantir a transparência, quando apropriado, e a prestação de contas pelas atividades de vigilância das comunicações e pela interceptação e coleta de dados pessoais realizadas pelo Estado".[50] Além disso, ele defendeu que os Estados devem tornar transparentes os pedidos de interceptação ou acesso às comunicações das pessoas, sua finalidade e a investigação a que se referem, bem como tornar transparente o quadro jurídico que legitima essa vigilância e os procedimentos aplicados para tal tarefa.[51]

Da mesma forma, a Corte Interamericana de Direitos Humanos indicou que é essencial que o marco legal contemple a existência de um órgão civil independente do Poder Executivo e dos próprios serviços de inteligência. Essa entidade, que pode ser de natureza parlamentar, administrativa ou judicial, deve contar com conhecimentos técnicos adequados e dispor das faculdades necessárias para exercer suas funções, incluindo acesso total às informações necessárias para cumprir sua função.[52]

3. Direito de notificação

Outra das garantias fundamentais para proteger o direito à privacidade é a obrigação por parte da autoridade de notificar uma pessoa de que sua privacidade ou dados pessoais foram interferidos por meio de uma medida de vigilância secreta. Embora essa notificação possa não ser feita de forma prévia ou imediata, uma vez que poderia comprometer o sucesso de uma investigação, ela deve ocorrer quando a investigação não estiver mais em risco, não houver risco de fuga, destruição de provas ou quando o conhecimento possa gerar um risco iminente à vida ou à integridade pessoal de alguém.

Este direito de notificação às pessoas afetadas por medidas de vigilância foi reconhecido, por exemplo, pelo Relator Especial sobre o direito à liberdade de opinião e expressão da ONU, que sustentou que "em qualquer caso, uma vez que a vigilância tenha sido concluída e exista a possibilidade de buscar a reparação adequada em relação ao uso de medidas de vigilância das comunicações".[53]

---

48 Ibidem, parágrafo 554.

49 CIDH. Relatoria Especial para a Liberdade de Expressão, Liberdade de Expressão e Internet. (2013). OEA/Ser.L/V/II, parágrafo 170

50 Nações Unidas. Assembleia Geral. (2014). Resolução A/RES/68/167 sobre O direito à privacidade na era digital. Disponível em: https://docs.un.org/es/A/RES/68/167

51 Nações Unidas. Assembleia Geral. (2013). Resolução A/HRC/23/40. Relatório do Relator Especial sobre a promoção e proteção do direito à Liberdade de opinião e Expressão, Frank La Rue. Disponível em: https://docs.un.org/es/A/HRC/23/40

52 Corte IDH. Caso Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia, Sentença de 18 de outubro de 2023, Exceções Preliminares, Fundo, Reparações e Custas. Parágrafo 564.

53 Idem.

O direito à notificação foi reconhecido, além disso, pelo Tribunal Europeu dos Direitos Humanos (doravante, TEDH), que determinou no caso Ekimdziev vs. Bulgária que, uma vez que a vigilância tenha cessado e tenha decorrido o tempo estritamente necessário para que o propósito legítimo da vigilância não seja colocado em risco, a notificação à pessoa afetada deve ser realizada sem demora.[54]

Resumo

O direito à privacidade e à proteção de dados pessoais são direitos fundamentais reconhecidos por tratados e instrumentos internacionais em matéria de direitos humanos. Esses direitos se estendem ao âmbito das comunicações digitais, incluindo metadados ou dados de tráfego das comunicações.

Consequentemente, para que as atividades de inteligência sejam legítimas em um Estado democrático e compatíveis com os direitos humanos, as restrições aos nossos direitos (privacidade, proteção de dados pessoais, entre outros) devem:

- Estarem previstas em uma lei que seja particularmente precisa, clara e detalhada das autoridades legitimamente habilitadas, descrevendo o procedimento e as circunstâncias em que podem ser realizadas medidas de vigilância das comunicações (princípio da legalidade). Leis vagas ou ambíguas são incompatíveis com os direitos humanos, pois podem ser utilizadas de forma discricionária, arbitrária e abusiva.;
- Prever uma finalidade legítima;
- Manter uma relação de causalidade com a finalidade legítima (princípio da adequação); ou seja, é necessário que a restrição da nossa privacidade e proteção de dados pessoais mantenha uma conexão com a garantia da segurança pública ou nacional;
- Não existirem medidas mais eficazes ou menos lesivas dos direitos (princípio da necessidade);
- Nem ser maior o grau de afetação aos nossos direitos do que o da realização da medida (princípio da proporcionalidade).

Nesse sentido, a vigilância maciça e indiscriminada das comunicações é particularmente problemática, pois afeta pessoas que não estão envolvidas na prática de crimes.

Além disso, devem ser estabelecidas garantias adequadas para prevenir, evitar e remediar abusos, tais como:

- Um controle judicial prévio, para garantir que as medidas de vigilância sejam autorizadas por juízes independentes que sirvam como contrapeso na análise sobre se as medidas cumpriram os princípios de legalidade, necessidade e proporcionalidade.
- Transparência e supervisão independente, para garantir a devida prestação de contas perante possíveis abusos na aquisição e utilização de medidas de vigilância; e,
- O direito de notificação das pessoas afetadas, para garantir o direito de acesso à justiça, ao devido processo legal e ao recurso efetivo das pessoas para contestar medidas de vigilância impostas contra elas.

54 TEDH. (2007). Caso da Associação para a Integração Europeia e os Direitos Humanos e Ekimdzhiev vs. Bulgária, Aplicação Nro. 62540/00.

CAPÍTULO DOIS: NORMAS E PROCEDIMENTOS QUE REGULAM A VIGILÂNCIA DAS COMUNICAÇÕES

Os países objeto desta investigação –Brasil,[55] México,[56] Colômbia,[57] Chile,[58] Paraguai,[59] Peru[60] e El Salvador[61]– consagram a nível constitucional a inviolabilidade das comunicações, a proteção da vida privada e dos dados pessoais.

Agora, serão abordadas as normas e procedimentos que regulam a vigilância das comunicações nos países objeto da investigação, com foco em:

- Autoridades competentes em cada país para a interceptação em comunicações privadas (com ou sem ordem judicial),
- Circunstâncias e procedimentos pelos quais as comunicações podem ser intervencionadas e,
- Garantias fundamentais para a prevenção de abusos, arbitrariedades e discricionariedade pelas medidas de vigilância.

I. Quem, em que casos e sob que procedimentos podem ser realizadas medidas de vigilância das comunicações?

As autoridades que pretendam obter autorização judicial, prévia ou posterior, para intervir em comunicações privadas deverão fundamentar e justificar devidamente os seus pedidos, especificando com precisão e clareza as circunstâncias e os procedimentos aplicados em cada medida. Como veremos, a justificação da medida deve satisfazer critérios de necessidade, proporcionalidade e, em algumas ocasiões, padrões probatórios de causa provável.

---

55 A Constituição Federal do Brasil garante esses direitos no artigo 5º, inciso XII, que protege a inviolabilidade das comunicações e da correspondência, e no inciso LXXIX, que reconhece a proteção de dados como direito fundamental.

56 O artigo 16 da Constituição Política dos Estados Unidos Mexicanos reconhece o direito à privacidade ao estabelecer que "ninguém pode ser incomodado em sua pessoa, família, domicílio, papéis ou posses, a não ser por mandado escrito da autoridade competente, que fundamente e motive a causa legal do procedimento [...]". Além disso, o segundo parágrafo do artigo 16 da Constituição reconhece o direito à proteção de dados pessoais ao reconhecer que "toda pessoa tem direito à proteção de seus dados pessoais, ao acesso, retificação e cancelamento dos mesmos, bem como a manifestar sua oposição, nos termos estabelecidos pela lei [...]". Por sua vez, os parágrafos décimo segundo e décimo terceiro do artigo 16 da Constituição reconhecem o direito à inviolabilidade das comunicações privadas.

57 O artigo 15 da Constituição Política da República da Colômbia estabelece que nenhuma interferência na vida privada das pessoas será feita sem uma lei que determine as condições para tal e sem controle judicial. Da mesma forma, o artigo 250 limita as autoridades e os prazos em que deve ocorrer o processo legal para a interceptação de comunicações.

58 O artigo 19 da Constituição Política do Chile, modificada em 2024, prevê em seu parágrafo 4º a proteção da vida privada e dos dados pessoais.

59 O artigo 36 da Constituição da República do Paraguai garante a inviolabilidade dos documentos e comunicações privadas. Nesse sentido, os registros documentais (independentemente do formato), a correspondência, os escritos e as comunicações de qualquer natureza não podem ser examinados, reproduzidos, interceptados ou apreendidos, salvo por ordem judicial nos casos especificamente previstos na lei e quando isso for indispensável para o esclarecimento de assuntos da competência das autoridades pertinentes.

60 O artigo 10 da Constituição Política do Peru garante a inviolabilidade das comunicações e documentos privados. As comunicações, telecomunicações ou seus instrumentos só podem ser abertos, apreendidos, interceptados ou intervencionados por ordem motivada do juiz, com as garantias previstas na lei.

61 O artigo 24 da Constituição da República de El Salvador reconhece que toda correspondência é inviolável. Além disso, proíbe a interferência e a intervenção nas comunicações telefônicas.

Tabela 1. Autoridades competentes por país para intervir nas comunicações (com ou sem ordem judicial) e circunstâncias e procedimentos pelos quais as comunicações podem ser interceptadas

PAÍS	AUTORIDADES COMPETENTES	CIRCUNSTÂNCIAS E PROCEDIMENTOS PELOS QUAIS SE PODE INTERVIR NAS COMUNICAÇÕES
Brasil	• A Agência Brasileira de Inteligência (doravante denominada ABIN) é a principal entidade estatal autorizada a planejar, executar, supervisionar e controlar atividades de vigilância para fins de inteligência. A ABIN não tem prerrogativa para realizar interceptações sem autorização judicial; no entanto, pode acessar informações obtidas por outros órgãos do Sistema Brasileiro de Inteligência (Sisbin)[62] por meio de mecanismos de cooperação estabelecidos na legislação vigente. • No que diz respeito aos dados de registo, apenas as autoridades policiais e o Ministério Público (doravante designado MP) podem solicitá-los sem mandado judicial.[63]	• A Lei de Interceptação Telefônica permite a violação do sigilo e a interceptação de comunicações quando houver indícios razoáveis de autoria ou participação em um crime punível com pena de prisão;[64] • Além disso, o Código de Processo Penal exige uma motivação e indicação de elementos concretos para justificar "a quebra do sigilo";[65] e, • A Lei de Interceptação Telefônica proíbe a vigilância por tempo indeterminado. A autorização judicial deve ser motivada, com um prazo máximo de 15 dias. Esse prazo pode ser renovado se for justificado.[66]
Chile	• O Ministério Público, com a autorização prévia de um tribunal de garantia que avalia a adequação, necessidade e proporcionalidade da medida.[67] • Endereços de órgãos de inteligência com autorização judicial prévia.[68]	A interceptação das comunicações,[69] que são entendidos como aquelas que "simulam sistemas de transmissão de telecomunicações"[70] e o acesso remoto a equipamentos informáticos [71] devem cumprir os seguintes requisitos de procedência: • Deve haver "suspeitas fundamentadas", baseadas em fatos concretos, de que uma pessoa cometeu/participou na preparação/prática de um crime.[72] • Devem ser descritas as circunstâncias factuais e jurídicas que se referem a crimes específicos e pessoas determinadas; e, • Deve ser considerado "estritamente indispensável" quando não houver outra medida investigativa para alcançar o objetivo perseguido pelas autoridades.[73]

62 A ABIN faz parte do Sisbin, que integra diversos órgãos da administração pública federal responsáveis pela produção de informações relevantes para as atividades de inteligência. O funcionamento do Sisbin é regulamentado pela Lei nº 9.883/99 e pelo Decreto nº 11.693/23.

63 De acordo com o previsto em normas específicas: a Lei de Organizações Criminosas (Lei n.º 12.850/2013), a Lei de Crimes de Lavagem de Dinheiro (Lei nº 9.613/1998) e o Código de Processo Penal (art. 13-A), que limita essa possibilidade a investigações de crimes como sequestro, tráfico de pessoas, extorsão e envio irregular de crianças ou adolescentes para o exterior.

64 Lei de Interceptação Telefônica, Lei nº 9.296/1996, artigo 2, 1.

65 Código Processual Penal, Artigo 13-B.

66 Lei de Interceptação Telefônica, Artigo 8-A.

67 Código Processual Penal, Artigo 222.

68 Lei 19974 sobre o sistema de inteligência do Estado e cria a agência nacional de inteligência, artigos 24 e 25.

69 Duração da ordem: Para a interceptação de comunicações, um prazo não superior a 60 dias, prorrogável por períodos iguais.

70 Duração da ordem: 30 dias, prorrogáveis por períodos de igual duração. No caso de medidas que "simulem sistemas de transmissão de telecomunicações", são incluídas medidas técnicas para preservar a integridade dos conteúdos e a segurança, para evitar o acesso não autorizado, bem como um prazo para a sua destruição.

71 Duração da ordem: prazo máximo de 30 dias, prorrogável por períodos de igual duração, com um máximo de 60 dias.

72 Código Processual Penal, Artigo 222.

73 Lei 19974 sobre o sistema de inteligência do Estado e cria a agência nacional de inteligência, artigos 24 e 25.

PAÍS	AUTORIDADES COMPETENTES	CIRCUNSTÂNCIAS E PROCEDIMENTOS PELOS QUAIS SE PODE INTERVIR NAS COMUNICAÇÕES
Colômbia	• A Corregedoria Geral da Nação;[74] • Autoridades de Polícia Judicial;[75] • Forças Militares e a Polícia Nacional;[76] y, • Departamento Nacional de Inteligência.	• Investigar crimes e acusar os supostos infratores perante os tribunais competentes; • Desenvolver atividades de inteligência e contra-inteligência, nas quais as Forças Armadas e a Polícia Nacional são as únicas autorizadas; e • O Ministério Público pode ordenar à polícia judiciária a retenção, apreensão ou recuperação de informações e que estas sejam analisadas por especialistas em informática forense, com o objetivo de que sirvam como prova.[77]
El Salvador	O Procurador-Geral da República e o Diretor do Centro de Intervenção são as autoridades competentes para solicitar a interceptação das telecomunicações, diretamente ou por meio de algum delegado designado por eles, que pertença ao Centro e que reúna os mesmos requisitos exigidos por esta lei para ser Diretor.[78]	• Para a investigação, deve existir um procedimento de investigação de um fato criminoso; e • Dentro dos elementos do julgamento, as investigações devem indicar a existência de indícios razoáveis de que foi cometido, está sendo cometido ou está prestes a ser cometido um fato criminoso estabelecido na Lei.[79]
México	• A Guarda Nacional, com poderes conferidos pela Lei da Guarda Nacional (doravante, LGN); • A Procuradoria-Geral da República, com poderes conferidos pelo Código Nacional de Processo Penal (doravante, CNPP); e • As Procuradorias das 32 entidades federativas, com poderes conferidos pelo CNPP. No entanto, uma reforma da Lei da Guarda Nacional – apresentada em junho de 2025 – propõe conferir poderes ao Ministério da Defesa Nacional (SEDENA) para processar e usar informação para atividades de inteligência por motivos de segurança nacional.	• A LGN estabelece um padrão de necessidade para medidas de vigilância das comunicações, constatando a existência de indícios suficientes que comprovem que está sendo organizada a prática de crimes.[80] • O artigo 16 da Constituição exige que as autoridades que pretendam solicitar à autoridade judicial federal a autorização para realizar uma interceptação em comunicações privadas devem fundamentar e justificar seus pedidos. • Quando o titular do Ministério Público "considerar necessária" a • interceptação em um inquérito por prática de um crime.[81] • A Lei de Segurança Nacional estabelece o padrão de necessidade, exigindo o cumprimento do requisito de iminência das ameaças à segurança nacional descritas na lei.[82]
Paraguai	O Ministério Público e a Polícia Nacional, por meio de uma ordem judicial e do devido processo legal, podem realizar a interceptação das comunicações.[83]	A interceptação de comunicações será excepcional.[84]

74 Constituição Política - Artigo 250. Lei 906 de 2004 (Modificado pelo art. 52 Lei 1453-2011) Decreto 1704-2012 Artigo 235.

75 Quanto ao artigo 235 da Lei 906 de 2004, este indica que a operação técnica da interceptação cabe às autoridades competentes, mas não determina explicitamente quais são essas autoridades competentes. No entanto, a Sentença C-594/14 da Corte Constitucional indica que o artigo 46 da Lei 938-2004 "determina que tal competência recai sobre as autoridades policiais judiciais".

76 Lei 1621-2013 - Artigo 3.

77 Lei 906 de 2004 (Modificado pelo art. 53 Lei 1453-2011) Artigo 236.

78 Lei Especial para a Intervenção das Telecomunicações, com suas reformas. Decreto N.º 552.- Artigo 7.

79 Ibidem, artigo 6.

80 Lei de Guarda Nacional, artigos 100 e 103.

81 Código Nacional de Procedimentos Penais, Artigo 291.

82 Lei de Segurança Nacional, artigos 5, 33 e 35.

83 Código Processual Penal, artigo 198, 199, 200 e 228. Duração da ordem: 6 meses, prorrogável uma vez pelo mesmo período.

84 Código Processual Penal - Artigo 200.

PAÍS	AUTORIDADES COMPETENTES	CIRCUNSTÂNCIAS E PROCEDIMENTOS PELOS QUAIS SE PODE INTERVIR NAS COMUNICAÇÕES
Peru	• A Polícia Nacional do Peru (doravante, PNP) pode intervir, sem necessidade de ordem judicial, quando se tratar apenas de acesso a metadados de geolocalização.[85] • O Ministério Público deve contar com ordem judicial e garantias legais,[86] atuando sob supervisão judicial. • Órgão Supervisor de Investimentos Privados em Telecomunicações (doravante, OSIPTEL).[87]	• A PNP pode solicitar dados de geolocalização quando se tratar de crimes em flagrante delito;[88] • O Ministério Público pode interceptar comunicações privadas e documentos em casos de crimes graves (corrupção, terrorismo, sequestro, lavagem de dinheiro, entre outros);[89] e, • A OSIPTEL pode solicitar às operadoras móveis acesso em tempo real aos dados técnicos e de geolocalização do dispositivo, para verificar a qualidade do serviço de Internet móvel.[90]

Fonte: Elaboração própria com informações fornecidas por organizações da AlSur.

II. Garantias fundamentais

A seguir, apresentamos informações sobre as garantias identificadas por país. Essas garantias são fundamentais para a prevenção de abusos, arbitrariedades e discricionariedade por parte das autoridades.

No caso do **Brasil**, é necessária uma autorização judicial para obter metadados, bem como dados de geolocalização das pessoas[91]. A lei prevê a ação de habeas data, que permite aos cidadãos acessar informações sobre si mesmos em registros oficiais ou solicitar sua correção;[92]. Além disso, é possível interpor ações civis ou penais contra abusos ou ilegalidades cometidos na execução de medidas de vigilância. Excepcionalmente, se o tribunal ao qual é apresentada a ordem de vigilância não se pronunciar no prazo de 12 horas, o Ministério Público ou um agente da polícia podem solicitar os dados de geolocalização e metadados diretamente às empresas de telecomunicações e telemática.[93]

No **Chile**, as comunicações entre advogados e réus estão isentas das medidas de interceptação, e os provedores de serviços de internet são obrigados a destruir os dados de seus assinantes após o prazo máximo de armazenamento dessas informações.[94] Além disso, prevê-se a notificação da medida de interceptação à pessoa afetada, uma vez que esta tenha sido executada.[95]

Na **Colômbia**, nenhuma interferência na vida privada das pessoas será feita sem uma lei que determine as condições para tal e sem controle judicial.[96] Limita as autoridades e os prazos em que deve ocorrer o processo legal para a interceptação de comunicações.[97] As atividades de inteligência serão limitadas pelo "respeito aos direitos humanos e [o] cumprimento estrito da Constituição, da Lei e do Direito Internacional Humanitário e do Direito Internacional dos Direitos Humanos".[98]

85 Decreto Legislativo N.º 1182 – Artigo 4.3
86 Constituição Política do Peru Artigo 2.10, Lei N.º 27697 Artigo 1 e 2, Código Processual Penal (Decreto Legislativo N.º 957) Artigo 230.
87 Resolução OSIPTEL N.º 137-2021-CD - Artigo 4.
88 Decreto Legislativo N.º 1182 – Artigo. 4.3
89 Lei N.º 27697 – Artigo 1 e 2
90 Resolução OSIPTEL N.º 137-2021-CD - Artigo 4.
91 De acordo com o artigo 10, § 1 do Marco Civil da Internet (Lei Nro. 12.965/2014) e o artigo 13-B do Código de Procedimento Penal.
92 Constituição Federal da República Federativa de Brasil, artigo 5º, inciso LXXII.
93 Artigo 13-B, §4 do CPP.
94 Código Processual Penal, artigo 222.
95 Ibidem, artigo 224.
96 Constituição Política da República de Colômbia, artigo 15.
97 Ibidem, artigo 250.
98 Lei 1621 de 2013, artigo 4.

Além disso, e de forma excepcional, as comunicações entre o arguido e o seu advogado poderão ser interceptadas mediante autorização judicial fundamentada que indique factos concretos que liguem o advogado ao crime investigado.[99]

Em **El Salvador**, as telecomunicações podem ser interceptadas temporariamente e excepcionalmente mediante autorização judicial.[100] Excepcionalmente, a decisão judicial admitirá recurso de apelação por parte do promotor, justificando o motivo da injustiça. O juiz deverá remeter os autos sem tramitação à Câmara competente. A Câmara deverá decidir sobre o recurso com base apenas na análise dos autos, no prazo mais breve possível, que não excederá 24 horas a partir do seu recebimento.[101]

No **México**[102], O artigo 16 da Constituição estabelece, em primeiro lugar, a necessidade de obter autorização judicial federal para realizar a interceptação de comunicações privadas,[103] requisito que também é reproduzido pelo CNPP para o acesso a dados de geolocalização em tempo real e o acesso a dados conservados.[104] Em segundo lugar, é proibida a interceptação de comunicações em matéria eleitoral, fiscal, comercial, civil, trabalhista ou administrativa, nem no caso das comunicações do detido com seu defensor.

Existem diversas exceções pelas quais o Ministério Público pode ordenar o acesso a dados de geolocalização ou dados conservados por empresas de telecomunicações sem autorização judicial prévia quando estiver em perigo a integridade física ou a vida de uma pessoa, ou estiver em risco o objeto do crime, bem como em fatos relacionados com a privação ilegal da liberdade, sequestro, extorsão ou crime organizado.[105] No entanto, existe a obrigação de informar o juiz de controle dentro de 48 horas após a realização da requisição, para que a autoridade judicial ratifique total ou parcialmente a medida ou a revogue.[106] E, no caso dos dados de localização geográfica conservados por instituições de crédito, as Disposições Administrativas que determinam a conservação e entrega desses dados não exigem qualquer controle judicial.[107]

No **Paraguai**, A interceptação nas comunicações requer uma decisão fundamentada do juiz;[108] e prevê-se a inviolabilidade do sigilo da correspondência realizada pelos serviços de telecomunicações e do patrimônio documental, exceto quando houver ordem judicial.[109] Excepcionalmente, tanto o juiz quanto o Ministério Público têm o poder de solicitar relatórios a pessoas ou entidades públicas ou privadas.[110] Esses relatórios podem ser solicitados verbalmente ou por escrito, incluindo detalhes sobre o procedimento, o nome do acusado, o local de entrega do relatório, o prazo para sua apresentação e as consequências do não cumprimento. Assim, facilita o acesso a dados conservados por empresas de telecomunicações sem controle judicial.

---

99 Código Processual Penal, artigo 222.

100 Constituição Política da República de El Salvador artigo 24, e Lei Especial para a Intervenção das Telecomunicações, com suas reformas. Decreto Nro. 552. - artigo 8.

101 Lei Especial para a Intervenção das Telecomunicações, com suas reformas. Decreto Nro. 552.- artigo 11.

102 Cabe ressaltar que, em junho de 2025, data final da redação do presente relatório, estão em processo de aprovação diversas leis no México que visam tanto reformar o mecanismo de exceção – para ampliar os casos em que se pode eludir a autorização judicial – como estabelecer que as autoridades de inteligência (incluindo o Exército) poderão solicitar, sem qualquer garantia, acesso irrestrito e direto a qualquer registro público ou privado, bem como a uma Plataforma Única de Identidade que conterá a identificação biométrica de todas as pessoas como obrigação para acessar qualquer tipo de serviço.

103 Constituição Política dos Estados Unidos Mexicanos, Artigo 16.

104 Lei da Guarda Nacional Artigo 9, seção XXVI, e do Código Nacional de Processo Penal.

105 Código Nacional de Procedimentos Penais, artigo 303.

106 Idem, artigo 303.

107 Secretaria da Fazenda e Crédito Público, Disposições de caráter geral a que se refere o artigo 115 da Lei de Instituições de Crédito.

108 Código Processual Penal, Artigo 200.

109 Lei N° 642/95 de Telecomunicações, artigo 89.

110 Código Processual Penal, artigo 228.

No **Peru**, somente é possível intervir nas comunicações com uma ordem judicial fundamentada. A autorização judicial deve ser fundamentada, especificar o tipo de comunicação, ser limitada no tempo e as informações não relacionadas devem ser mantidas confidenciais.[111] Além disso, a interceptação de comunicações privadas só é permitida em casos de crimes graves (corrupção, terrorismo, lavagem de dinheiro, etc.).[112] Finalizada a interceptação, deve-se notificar o afetado, que pode impugnar judicialmente.[113] Além disso, o habeas corpus é aplicável em casos de interceptações indevidas que afetem a liberdade pessoal. [114] e o habeas data em caso de tratamento indevido de dados pessoais ou violação da privacidade.[115]

Excepcionalmente, e no caso dos dados relativos à geolocalização, a polícia poderá acessar essas informações sem a necessidade de uma ordem judicial prévia para certos tipos de crimes. Esse acesso deve ser posteriormente validado judicialmente. Nesse sentido, as empresas operadoras de telecomunicações devem armazenar dados relativos à geolocalização por um período mínimo de um (1) ano, podendo essa obrigação ser prorrogada por até dois (2) anos adicionais.[116]

Resumo

SOBRE AS AUTORIDADES COMPETENTES, CIRCUNSTÂNCIAS E PROCEDIMENTOS PARA INTERVIR NAS COMUNICAÇÕES

Embora a maioria dos quadros jurídicos regionais preveja requisitos gerais de fundamentação e motivação, a clareza e a precisão das circunstâncias e dos procedimentos para a realização de medidas de vigilância variam dentro do quadro jurídico regional.

Por exemplo, no **Brasil**, a interceptação nas comunicações privadas requer *"indícios razoáveis"* da prática de um crime, com base em elementos concretos e com um prazo determinado; no **Chile**, requer *"suspeitas fundamentadas"*, com base em circunstâncias factuais e jurídicas que se refiram a crimes específicos e pessoas determinadas;

Na **Colômbia**, considera-se de forma genérica que as comunicações privadas podem ser interceptadas *"para investigar crimes e acusar os supostos infratores"*, *bem como "para desenvolver atividades de inteligência e contra-inteligência"*.

Ambas as legislações apresentam critérios muito amplos, subjetivos e ambíguos que violam o princípio da legalidade, deixando-nos em um estado de indefesa ao não limitar e restringir a atuação das autoridades com o objetivo de evitar efeitos arbitrários, caprichosos ou abusivos na esfera jurídica das pessoas. Em **El Salvador**, da existência de indícios razoáveis de que foi cometido, está sendo cometido ou está prestes a ser cometido um ato criminoso.

Países como o **Peru**, por sua vez, baseiam a motivação das medidas mais na categoria dos crimes investigados; ou seja, crimes em flagrante delito e crimes graves, como casos de corrupção, terrorismo, sequestro ou lavagem de dinheiro.

No entanto, embora das normas anteriormente descritas se possa deduzir um requisito geral de fundamentação e motivação, que inclui a comprovação de elementos objetivos que justifiquem sua necessidade e proporcionalidade, sua aplicação é duvidosa tanto no desenvolvimento de regras de procedência específica em outras leis secundárias, como na prática.

---

111 Constituição Política do Peru, artigo 2.10.
112 Até 60 dias, prorrogáveis. Artigos 1, 2.7 e 2.8 Lei N.º 27697.
113 Código Processual Penal, artigo 231.3 e 228.
114 Constituição Política do Peru, artigo 200.1.
115 Idem, artigo 200.3
116 Decreto Legislativo Nro. 1182, artigos 3 e Segunda Disposição Complementar Final.

Por outro lado, apesar de a maioria das leis estabelecer quem serão as autoridades competentes para intervir nas comunicações, detectamos uma incerteza jurídica regional devido ao estabelecimento de termos vagos ou genéricos em relação aos casos em que essas autoridades podem fazer uso de medidas de vigilância.

Por exemplo, no **México**, os Ministério Públicos podem ordenar a interceptação de comunicações quando *"considerarem necessário"* tal medida no âmbito de um inquérito criminal.

SOBRE AS GARANTIAS PARA A PREVENÇÃO, IDENTIFICAÇÃO E REPARAÇÃO DE MEDIDAS DE VIGILÂNCIA ILEGAIS

A maioria dos países objeto desta investigação estabelece a necessidade de um controle judicial prévio para a intervenção em comunicações privadas. No entanto, alguns países da região estabelecem exceções preocupantes que permitem contornar esse controle judicial.

Por exemplo, no **Brasil**, se o tribunal não se pronunciar no prazo de 12 horas, o Ministério Público ou um agente da polícia podem solicitar os dados diretamente às empresas de telecomunicações e telemática. Da mesma forma, no **México**, o mecanismo excepcional estabelecido no artigo 303 do Código Nacional de Processo Penal permite que os ministérios públicos solicitem acesso a dados conservados ou geolocalização em tempo real às empresas de telecomunicações sem obter previamente uma autorização judicial, onde a exceção se tornou a regra geral e um número significativo de solicitações feitas sob o mecanismo excepcional não são ratificadas pela autoridade judicial.

Além disso, no **Paraguai**, tanto o juiz quanto o Ministério Público têm o poder de solicitar relatórios a pessoas ou entidades públicas ou privadas sem autorização judicial; e na **Colômbia**, o uso de dados de comunicações em investigações criminais.[117] e para as funções de inteligência[118] não impõe a obrigação de controle judicial.

Nesse sentido, ressalta-se que a evasão do controle judicial das medidas de vigilância incentiva os abusos, ao nos privar dos contrapesos necessários, impede a detecção dos mesmos e permite a impunidade que incentiva sua repetição crônica. Por isso, é necessário que os quadros jurídicos detalhem claramente a necessidade do controle judicial federal prévio ou imediato de todas as medidas de vigilância reconhecidas por seus quadros legais, sem mecanismos excepcionais que permitam a evasão desse requisito.

Por outro lado, observa-se que alguns marcos legais, como o do **Brasil** e do **Peru**, contemplam medidas de garantia adicionais para o exercício do direito à proteção de dados pessoais – como o habeas data – bem como a menção do habeas corpus como recurso eficaz contra casos de abuso.

Também é motivo de comemoração o fato de os marcos legais do **Chile** e do **Peru** contemplarem o direito de notificação das pessoas afetadas, concedendo um recurso eficaz de acesso à justiça para as pessoas diante de potenciais abusos das medidas de vigilância. No entanto, seria necessário analisar – especialmente considerando a falta de transparência que prevalece no uso dessas medidas de vigilância – em quantos casos essa garantia foi efetivamente colocada em prática.

117 Decreto Nro. 1704 de 2012.

118 Lei 1621 de 2013, artigo 44.

O caso do **Chile** é um dos mais protetores em termos de quadro legal, estabelecendo expressamente a exceção das medidas de interceptação de comunicações entre advogado e acusado (assim como no **México**) e ordenando aos provedores de serviços de internet a destruição dos dados de seus assinantes quando expirar o prazo máximo de armazenamento dessas informações.

Destaca-se que **nenhum dos países da região contempla medidas de transparência estatística ou supervisão independente** em relação ao uso e alcance dos poderes e técnicas de vigilância das comunicações empregadas. Nesse sentido, um dos principais problemas na análise desse tipo de medida é que não dispomos de informações suficientes para compreender o alcance, a natureza e a aplicação das leis que permitem a vigilância das comunicações.

Por outro lado, muitas vezes a autorização recai sobre um superior hierárquico da mesma instituição solicitante. Essa situação é observada, por exemplo, no acesso à informação pela ABIN e pelas forças policiais no Brasil; pela Lei da Guarda Nacional no México; pela PNP e pela OSIPTEL no Peru; e pelas Forças Militares, Polícia Nacional e Direção Nacional de Inteligência na Colômbia, o que gera preocupações pela falta de separação entre quem investiga e quem autoriza a medida.

Portanto, os marcos legais devem prever uma instituição civil independente dos serviços de inteligência e do Poder Executivo, com conhecimentos técnicos, para poder fiscalizar as autoridades competentes, tanto em relação às suas obrigações de transparência como em termos de prestação de contas.

CAPÍTULO TRÊS: CASOS DE VIGILÂNCIA DE COMUNICAÇÕES NA REGIÃO DE ACORDO COM O TIPO DE VIGILÂNCIA EMPREGADA

O próximo capítulo apresenta um breve resumo dos casos em que foi detectado o uso de alguma medida de vigilância das comunicações, a saber: **(I)** casos de intervenção em comunicações privadas em termos gerais, contemplando: (a) a colaboração de empresas de telecomunicações; e (b) a obtenção de informações; **(II)** o uso de *spywares*; **(III)** a geolocalização baseada na exploração de vulnerabilidades na infraestrutura de telecomunicações (SS7); **(IV)** o patrulhamento cibernético; e **(V)** a vigilância de pessoas por meio de sistemas de leitura de placas de veículos.

Para cada caso, é fornecida uma breve descrição sobre a técnica de vigilância, o tipo de tecnologia empregada, as autoridades que fizeram uso dela, bem como o perfil das vítimas, com o objetivo de identificar tendências e padrões na utilização de medidas de vigilância na região latino-americana.

I. Interceptação de comunicações privadas

A seguir, apresentam-se exemplos de intervenção em comunicações privadas em termos gerais (na **Colômbia** e no **Chile**), bem como exemplos específicos de: (a) colaboração de empresas de telecomunicações no acesso a registros de dados conservados (no **Paraguai**, **Chile** e **México**); e (b) obtenção de informações.

É preciso ressaltar que o alcance do que deve ser entendido como comunicações privadas tem se ampliado com a evolução e o caráter dinâmico da tecnologia e que diversos tribunais têm interpretado que os dados de tráfego das comunicações ou metadados também estão protegidos pelo direito à inviolabilidade das comunicações. Consequentemente, a divisão realizada tem como único objetivo uma melhor visualização das diferentes maneiras de intervir nas comunicações privadas.

Nesse sentido, no que diz respeito a essa técnica de vigilância, contempla-se uma definição ampla do conceito de intervenção em comunicações privadas, que abrange todo tipo de informação e tanto o conteúdo das comunicações quanto os metadados, também denominados dados de tráfego de comunicações. Por sua vez, entende-se que o conceito abrange tanto o acesso quanto o registro, a gravação, a coleta e o armazenamento das informações, tanto em tempo real quanto após o momento em que ocorre o processo comunicativo.[119]

Também é preciso ressaltar que a interceptação de comunicações, mesmo quando baseada em poderes conferidos por lei, pode dar origem a abusos na sua aplicação, bem como ao uso de tecnologias que violam o direito à privacidade.

A seguir, apresentamos dois casos emblemáticos, em termos gerais, de interceptação de comunicações privadas na **Colômbia** e no **Chile**.

119 Foi levada em consideração a definição legal do artigo 34, parágrafo segundo, da Lei de Segurança Nacional do México.

COLÔMBIA

Por conta de uma denúncia na *Revista Semana*,[120] se teve conhecimento que, de dezembro de 2019 a fevereiro de 2020, o Exército Nacional realizou atividades de espionagem por meio de um "programa de rastreamento informático" que tinha como objetivo realizar "perfis" e "trabalhos especiais"[121] por meio da coleta de informações pessoais de mais de 130 pessoas.[122] Entre as pessoas afetadas estão jornalistas, ex-ministros, funcionários da Presidência, generais, políticos, sindicalistas e jornalistas americanos.

Essa vigilância ilegal foi realizada pelo Exército Nacional, por meio de seus batalhões de inteligência cibernética (doravante, "Bacib").[123] Um indicador importante das irregularidades foram os alertas emitidos por órgãos de inteligência dos Estados Unidos, que afirmaram ter identificado o uso para fins ilegais de equipamentos técnicos que eles próprios haviam doado ao Exército colombiano.

No ano de 2019, o Ministério da Defesa, sob o comando do Exército Nacional, adquiriu o software *Hombre Invisible*,[124] cujo fornecedor era a empresa espanhola *Mollitiam Industries*.[125] O objetivo do contrato era a "aquisição da plataforma suíte de penetração para o desenvolvimento das atividades realizadas no campo da defesa cibernética ativa do Exército Nacional". Até o momento, as informações sobre sua contratação não podem ser consultadas abertamente nas páginas de contratação do Estado.

Na sequência da publicação da *Revista Semana*, a organização Fundação para a Liberdade de Imprensa (doravante, "FLIP") documentou e identificou um total de 52 casos de jornalistas vigiados ilegalmente pelo Exército Nacional até junho de 2020.[126] A FLIP também apresentou ao Ministério Público Federal (doravante, "MPF") uma petição para saber mais informações sobre o caso. De acordo com o indicado, a FGN declarou que não se tratava de "130 alvos de ações ilegais de monitoramento, seguimento, interceptações, perfis, trabalhos especiais pelo Exército Nacional, mas sim de um número de pessoas que não ultrapassa as 20".[127]

---

120 Semana. (2020). Espionagem do Exército Nacional: As pastas secretas. Disponível em: https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/

121 De acordo com a terminologia utilizada pelos militares.

122 Por exemplo, telefones, endereços residenciais e comerciais, e-mails, amigos, familiares, filhos, colegas, contatos, infrações de trânsito e até mesmo locais de votação – de várias pessoas.

123 Eles "pertencem às brigadas de inteligência militar e ao Batalhão de Contra-Inteligência de Segurança da Informação (Bacsi). Ambos dependem do Comando de Apoio à Inteligência Militar (Caimi) e do Comando de Apoio à Contra-Inteligência Militar (Cacim)".
Durante o período de dezembro de 2019, o ministro da Defesa era Carlos Holmes Trujillo e o comandante do Exército era Nicacio Martínez. O primeiro dos dois, ministro da Defesa nos primeiros anos do governo de Iván Duque; e o segundo, ex-comandante do Exército que anunciou sua aposentadoria no mesmo período em que a Suprema Corte de Justiça invadiu essa entidade. Em maio de 2020, data em que foi publicado o artigo da revista Semana sobre as chamadas "pastas secretas", o comandante do Exército era Eduardo Zapateiro. De acordo com a revista Semana, essas mudanças no comando ocorreram em relação à descoberta de irregularidades em matéria de vigilância digital cometidas pelo Exército no final de 2019.

124 Rico, M. (2023, fevereiro 20). Mollitiam: Assim é a contratada do Exército e suas ferramentas de espionagem cibernética. Disponível em: https://www.elespectador.com/judicial/mollitiam-asi-es-la-contratista-del-ejercito-y-sus-herramientas-de-ciberespionaje/

125 Mollitiam Industries. https://www.mollitiamindustries.com/ (Contrato adjudicado mediante processo Nro. 277-CENAINTELIGENCIA 2019).

126 Fundação para a Liberdade de Imprensa (FLIP). (2020). Quatorze novos casos de jornalistas vítimas de ações de perfilamento por parte do Exército Nacional. Disponível em: https://flip.org.co/en/pronunciamientos/catorce-nuevos-casos-de-periodistas-que-fueron-victimas-de-acciones-de-perfilamiento-por-parte-del-ejercito-nacional

127 Fundação para a Liberdade de Imprensa. (2020). Quatro meses depois dos arquivos secretos. Disponível em: https://flip.org.co/en/pronunciamientos/cuatro-meses-despues-de-las-carpetas-secretas

Após a publicação da denúncia, algumas vítimas afirmaram ter sofrido violência ou represálias relacionadas ao caso. Um exemplo foram os jornalistas da *Rutas del Conflicto* (doravante, "RdC"), um projeto jornalístico que documenta fatos relacionados ao conflito armado no país. De acordo com Óscar Parra, membro da equipe da RdC, apesar de não terem provas que relacionem os fatos, eles consideram que o início de seu "perfilamento" como organização surgiu de uma solicitação de informações ao Exército Nacional no âmbito de uma investigação realizada pela RdC em 2019.[128]

De acordo com o exposto por O. Parra, após realizar tal solicitação e ter que insistir por meio de instâncias judiciais, dois militares compareceram ao escritório da organização para responder pessoalmente à mesma, evitando dar resposta por correio físico ou digital. Além disso, os oficiais permaneceram do lado de fora do prédio naquele mesmo dia.

À luz do ocorrido, Parra classificou isso como intimidação, sobre a qual informaram o juiz responsável pelo caso, que acabou ordenando ao Exército que fornecesse as informações correspondentes. Da mesma forma, o general Nicacio Martínez apresentou uma ação judicial[129] contra o mesmo jornalista, argumentando que RdC estava desacreditando o Exército. A justiça decidiu a favor de RdC e encerrou o processo.

Embora este seja um dos poucos relatos relacionados a algum tipo de represália adicional às medidas de vigilância denunciadas pela *Revista Semana*, é importante destacar que os jornalistas na Colômbia são constantemente alvo dessas ações de vigilância ilegal e têm seu direito à liberdade de expressão e privacidade violado com mais frequência do que outros setores. Desde 2019, a FLIP documentou um número elevado de agressões contra jornalistas, com uma tendência sustentada de entre 400 e 500 ataques anuais na Colômbia.[130]

Depois que as ações de vigilância ilegal vieram à tona, foram iniciadas duas investigações, uma pela Procuradoria-Geral da Nação (doravante, "PGN") e outra

pela FGN. De acordo com o meio de comunicação *El Espectador*,[131] para 2021, a investigação mais avançada era a da PGN, na qual "foi ordenada a formulação de acusações contra militares com provas dos equipamentos, das pessoas, das ordens e das informações recuperadas".[132]

No entanto, em fevereiro de 2021, o mesmo meio de comunicação indicou que as investigações de ambas as entidades não coincidiam quanto ao número de vítimas dessas ações ilegais. Além disso, foi indicado que, até essa data, *"não se conheciam os avanços no processo disciplinar e na formulação da acusação estabelecida pela Procuradoria contra treze militares, nem a audiência pública que deveria ocorrer"*.[133]

---

128 Abu Shihab, L. (2020, maio 5). Conversamos com uma das vítimas de espionagem por parte do Exército colombiano. VICE. https://www.vice.com/es/article/nuevo-escandalo-en-colômbia-por-seguimientos-ilegales-del-ejercito-a-periodistas-politicos-y-defensores-de-direitos-humanos/

129 A ação de tutela é um mecanismo estabelecido no artigo 86 da Constituição Política da República da Colômbia. A ação de tutela consiste no direito que toda pessoa tem de reclamar perante um juiz, a qualquer momento e em qualquer lugar, por meio de um procedimento preferencial e sumário, a proteção judicial imediata de seus direitos constitucionais fundamentais.

130 El Colombiano. (2024). A violência contra os jornalistas é disfarçada como o direito de debate dos governantes. Disponível em: https://www.elcolômbiano.com/colômbia/la-violencia-contra-los-periodistas-se-disfraza-como-el-direito-a-debatir-de-los-gobernantes-flip-OH23715128

131 El Espectador. (2021). "Pastas secretas": Após a denúncia, o silêncio. Disponível em: https://www.elespectador.com/judicial/carpetas-secretas-despues-de-la-denuncia-el-silencio-article/

132 Isso foi ordenado para 20 de maio de 2020 contra treze militares, entre os quais estavam os generais Eduardo Quirós e Gonzalo Ernesto García, que enfrentarão um julgamento disciplinar na Procuradoria. O último deles foi funcionário do extinto Departamento Administrativo de Segurança, dissolvido após o escândalo das "chuzadas" no governo de Álvaro Uribe. O último deles era funcionário do extinto Departamento Administrativo de Segurança, dissolvido após o escândalo das "chuzadas" no governo de Álvaro Uribe.

133 El Espectador. (2021). "Pastas secretas": Después da denúncia, o silêncio. Disponível em: https://www.elespectador.com/judicial/carpetas-secretas-despues-de-la-denuncia-el-silencio-article/

Além das medidas tomadas pelas entidades nacionais, em outubro de 2020, a CIDH convocou uma audiência pública sobre o caso.[134] "A delegação do Estado colombiano, liderada por Alejandro Ordóñez, embaixador junto à OEA, negou o caráter sistemático dessas atividades. Afirmou também que, à data da audiência, "havia nove investigações em curso sobre esses fatos, negando ainda a falta de participação das vítimas". Esta audiência não consta dos registros audiovisuais da CIDH e não é claro identificar as nove investigações a que Ordoñez se referiu. Na audiência, foi enfatizado o seguinte:

> A questão da inteligência ilegal na Colômbia [naquela época, já havia] ocupado a CIDH por dezesseis anos, durante os quais persistiu a impunidade e a falta de informação sobre o conteúdo dessas atividades ilegais, bem como a falta de esclarecimento sobre as motivações e a estrutura que opera por trás das interceptações e a repetição dos fatos.[135]

CHILE

Em outubro de 2019, foi revelada a fuga de milhares de arquivos de inteligência utilizados pela instituição policial *Carabineros* do Chile, que evidenciavam o rastreamento ilegal das comunicações de líderes sociais, movimentos de defensores dos direitos humanos e sindicatos no país.[136]

Os vazamentos, denominados *PacoLeaks*[137], foram publicadas nos dias 25, 26 e 28 de outubro de 2019.[138] O terceiro vazamento revelou dados de mais de 300 memorandos internos e 10.000 anexos dos *Carabineros*, com informações detalhadas sobre atividades de movimentos sociais e sindicatos,[139] bem como relatórios de acompanhamento e vigilância de líderes e suas organizações.[140] Nesse sentido, ficou evidente que os movimentos ambientais e os grupos feministas são o principal alvo das atividades de inteligência dos *Carabineros*.

Embora, neste caso, não tenha sido possível identificar a identidade do operador da tecnologia de vigilância, do desenvolvedor ou dos intermediários que permitiram a obtenção das informações, a partir dessa fuga de arquivos de inteligência, foram revelados diversos mecanismos de vigilância e espionagem da instituição policial em questão contra organizações sociais. De acordo com uma das fontes consultadas,[141] entre esses mecanismos destacam-se: busca de atividades e troca de comunicações em redes sociais, infiltração em eventos, acompanhamento in loco de manifestantes e líderes, registro fotográfico policial em primeira pessoa, espionagem por meio de drones e fichas de reconhecimento com dados pessoais.

---

134 Comissão Colombiana de Juristas. (2020). A CIDH reiterou que a vigilância ilegal na Colômbia é sistemática e pediu garantias para as vítimas. Disponível em: https://www.coljuristas.org/sala_de_prensa/cidh-reitero-que-la-vigilância-ilegal-en-colômbia-es-sistematica-y-pidio-garantias-para-las-victimas

135 Ibidem.

136 CIPER (2019). Hackeamento dos Caribineros em meio à crise expõe 10.515 arquivos: entre eles, há dados de inteligência. Disponível em: https://www.ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia/

137 Paco, termo amplamente utilizado no Chile para se referir aos agentes da polícia.

138 La Izquierda Diario (2019). PACOLEAKS. Vazamento de documentos da polícia revela vigilância de organizações políticas e sociais. Disponível em: https://www.laizquierdadiario.com/Filtracion-de-documentos-de-Carabineros-revela-seguimientos-a-organizaciones-politicas-y-sociales

139 Greves legais, negociações coletivas, atos de "pintatón", coletivas de imprensa ou atos públicos.

140 Interferência (2019). PacoLeaks: Estes são os nomes e organizações que foram vigiados pela polícia nos últimos meses. Disponível em: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

141 Doble Espacio (2019). Da Juventude Comunista à Universidade Católica: as organizações e instituições investigadas pela Polícia. Disponível em: https://doble-espacio.uchile.cl/2019/11/04/desde-las-juventudes-comunistas-a-la-universidad-catolica-las-organizaciones-e-instituciones-investigadas-por-carabineros/

De acordo com alguns meios de comunicação,[142] entre as organizações sociais, líderes e movimentos defensores dos direitos humanos que constavam nos documentos de acompanhamento e inteligência, encontravam-se: sindicatos e associações como o Colégio de Professores, Agrupamento Nacional de Funcionários Públicos (doravante "ANEF"), Confusam e a Central Unitaria de Trabalhadores (doravante "CUT"); organizações estudantis como a Federação de Estudantes da Universidade do Chile (doravante, FECH) e a Federação de Estudantes da Universidade Arturo Prat (doravante, "FEDEUNAP"); e coletivos de direitos humanos, como a Agrupamento de Familiares de Detidos Desaparecidos (doravante, "AFDD"), Agrupamento de Familiares Ejecutados Políticos (doravante, "AFEP") e a Coordinadora Nacional de Organizações de Direitos Humanos e Sociais. Também figuram movimentos sociais e temáticos como No+AFP, Modatima, No a Ciclo e o Movimento pela Água e os Territórios, bem como grupos feministas como a Rede Chilena Contra a Violência contra as Mulheres, a Rede de Mulheres do Norte e o Coletivo Voz en Fuga.

Além disso, foram divulgadas fichas com fotografias, dados pessoais e, em alguns casos, movimentos detalhados de líderes sociais catalogados como "alvos de interesse",[143] entre os quais Rodrigo Mundaca, líder da Modatima; Bárbara Figueroa, presidente da CUT; Mario Aguilar, do Colégio de Professores; Luis Mesina, porta-voz da Coordinadora No+AFP; e Emilia Schneider, presidente interina da FECH.

Os *Carabineros* do Chile confirmaram a veracidade dos documentos vazados, justificando suas ações com base na Lei de Inteligência e na proteção da segurança pública e da integridade física dos organizadores de atividades sociais.[144]

No caso do líder da Modatima, a informação vazada detalha a hora exata de sua chegada ao Chile em 1º de outubro de 2019, após receber o Prêmio Internacional de Direitos Humanos de Nuremberg, na Alemanha. O líder afirmou que recebeu ameaças de morte anônimas nas redes sociais após sua chegada ao país.[145] Para o líder ambientalista, as informações dos *Carabineros* sobre sua chegada ao Chile:

> (...) confirma o que há muito tempo denunciamos: existe uma ação coordenada por parte das forças de inteligência do Estado [...] para controlar todos os nossos passos, vigiando-nos permanentemente, o que viola direitos humanos fundamentais, como o direito à liberdade, à liberdade de opinião e o direito de discordar.[146]

Além disso, Emilia Schneider, presidente interina da FECH, afirmou que *"é preocupante que nos classifiquem como alvo de interesse, ainda mais quando vemos líderes que foram assassinados, como Macarena Valdés ou Camilo Catrillanca"*.[147] Após os vazamentos, várias organizações sociais divulgaram à mídia que a polícia estava monitorando atividades que não envolviam grandes aglomerações.

---

142 Interferência (2019). PacoLeaks: Estes são os nomes e organizações que foram vigiados pela polícia nos últimos meses. Disponível em: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

143 Interferencia (2019). PacoLeaks: Carabineros criaram fichas de líderes sociais para mantê-los sob vigilância. Disponível em: https://interferencia.cl/articulos/pacoleaks-carabineros-creo-fichas-de-lideres-sociales-para-mantenerlos-vigilados

144 Interferencia (2019). PacoLeaks: Estes são os nomes e organizações que foram vigiados pelos Carabineros nos últimos meses. Disponível em: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

145 Interferencia (2020). Mundaca se pronuncia sobre o indeferimento da Suprema Corte ao seu recurso por 'Pacoleaks': "é um voto de confiança a uma polícia que viola os Direitos Humanos." Disponível em: https://interferencia.cl/articulos/habla-mundaca-sobre-el-rechazo-de-la-suprema-su-amparo-por-pacoleaks-es-un-voto-de

146 Interferencia (2019). PacoLeaks: Estes são os nomes e organizações que foram vigiados pelos Carabineros nos últimos meses. Disponível em: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

147 Interferencia (2019). PacoLeaks: Carabineros criaram fichas de líderes sociais para mantê-los sob vigilância. Disponível em: https://interferencia.cl/articulos/pacoleaks-carabineros-creo-fichas-de-lideres-sociales-para-mantenerlos-vigilados

Em 2019, na sequência da divulgação de arquivos secretos, foram iniciadas várias ações judiciais contra a polícia e o Ministério do Interior.[148] Por exemplo, o Colégio de Professores apresentou um recurso de amparo contra o diretor-geral dos *Carabineros*, Mario Rozas, e o ministro do Interior, Gonzalo Blumel.[149]

O recurso de amparo foi rejeitado pelo Tribunal de Apelações de Santiago com base no seguinte argumento:

> (...) para que as informações apresentadas ao tribunal possam ser avaliadas, elas devem ter uma origem legítima e estar em conformidade com a lei; caso contrário, não podem ser levados em consideração nem validados em um processo jurisdicional [...] este recurso tem como fundamento um fato ilícito, como é o caso do hackeamento e obtenção de informações da *Carabineros* do Chile, em relação ao qual a instituição afetada formulou — conforme expressou — a consequente denúncia na esfera penal.[150]

O líder da Modatima também apresentou um recurso de amparo contra o diretor-geral da Polícia e o ministro do Interior, solicitando que se especificasse desde quando eram realizadas as práticas de vigilância e *"o propósito de analisar o que fazemos, o que pensamos, com quem nos reunimos"*.[151] O Tribunal de Apelações de Santiago também rejeitou o recurso de amparo com o mesmo argumento usado no caso do Colégio de Professores.[152]

Nesse mesmo sentido, a vice-reitora de Extensão e Comunicações da Universidade do Chile, a presidente da Agrupação de Familiares de Detenidos Desaparecidos, a presidente da FECH e outros ativistas apresentaram uma queixa contra o Ministro do Interior e o Diretor Geral da Polícia por espionagem contra eles[153]. Este recurso também foi rejeitado com o argumento dos casos anteriores sobre a origem dos antecedentes levados ao conhecimento do tribunal.[154]

148 Interferencia (2019). Líderes sociais vigiados tomam medidas legais contra Rozas e Blumel. Disponível em: https://interferencia.cl/articulos/dirigentes-sociales-vigilados-toman-acciones-legales-contra-rozas-y-blumel

149 Para mais informação, ver: https://juris.pjud.cl/busqueda/pagina_detalle_Sentença?k=eHFSeVBncXp0Z085dzhVU2M-veThnQT09

150 COLÉGIOS DE PROFESSORES DE CHILE A.G / CARABINEROS DE CHILE - MINISTÉRIO DO INTERIOR VISTA EM POS DO ING. CORTE 2460-2019: 09-12-2019 (-), Rol N° 2473-2019. Em Buscador Corte de Apelaciones (https://juris.pjud.cl/busqueda/u?7ps0). Data da consulta: março de 2025.

151 Interferencia (2020). Mundaca se pronuncia sobre o indeferimento da Suprema Corte ao seu recurso por 'Pacoleaks': "é um voto de confiança a uma polícia que viola os Direitos Humanos." Disponível em: https://interferencia.cl/articulos/habla-mundaca-sobre-el-rechazo-de-la-suprema-su-amparo-por-pacoleaks-es-un-voto-de

152 MUNDACA CABRERA RODRIGO / CARABINEROS DE CHILE VISTA COM ING. CORTE 2319, 2362, 2460, 2473, 2507, 2512 e 2682 TODAS DEL 2019.-: 09-12-2019 (-), Rol N° 2295-2019. Em Buscador Corte de Apelações (https://juris.pjud.cl/busqueda/u?7psz). Data de consulta: março de 2025.

153 Interferencia (2019). Líderes sociais vigiados tomam medidas legais contra Rozas e Blumel. Disponível em: https://interferencia.cl/articulos/dirigentes-sociales-vigilados-toman-acciones-legales-contra-rozas-y-blumel

154 OLIVARES SAAVEDRA ROSARIO-ASTUDILLO ASTUDILLO LEANDRO-BARRA ARANCIBIA GUILLERMO-SCHNEIDER VIDELA EMILIA/MINISTÉRIO DO INTERIOR e SEGURANÇA PÚBLICA-CARABINEROS DE CHILE. VISTA EM POS DEL ING. CORTE 2507-2019.-: 09-12-2019 (-), Rol N° 2512-2019. Em Buscador Corte de Apelaciones (https://juris.pjud.cl/busqueda/u?7hgt). Data de consulta: março de 2025.

II. Colaboração das empresas de telecomunicações no acesso ao registro de dados conservados

Como observou o então Alto Comissário das Nações Unidas para os Direitos Humanos em seu relatório de 2014 sobre "O direito à privacidade na era digital", tanto o conteúdo das comunicações quanto seus metadados são protegidos pelo direito à privacidade, uma vez que os metadados também podem revelar dados sobre o comportamento das pessoas e permitir tirar conclusões sobre sua vida privada.[155]

Nesse sentido, a conservação e o armazenamento de metadados das comunicações por parte das empresas de telecomunicações costumam fazer parte das medidas legislativas e de política pública em matéria de colaboração com a justiça, principalmente para que as autoridades possam solicitar seu acesso, mediante autorização judicial prévia, para fins de prevenção e investigação de crimes.

No entanto, a maioria dos marcos legais que regulam esse acesso não estabelece de forma clara e precisa quais são as autoridades que poderão ter acesso a esses dados pessoais, em que circunstâncias, sob quais procedimentos e com quais garantias. Isso é particularmente preocupante, considerando que essa prática consiste na conservação maciça e indiscriminada dos dados pessoais de milhões de usuárias de serviços de telefonia móvel, a maioria das quais não está, nem estará envolvida na prática de um crime.

Nesse sentido, foram detectadas graves irregularidades e abusos na região no que diz respeito ao acesso a esses dados. A seguir, exemplificamos sua utilização com casos documentados no **Paraguai**, **Chile** e **México**.

PARAGUAI

No Paraguai, o Ministério Público pode solicitar acesso aos metadados das comunicações mantidos pelos provedores de Internet sem autorização judicial e sem que exista uma causa formal ou acusação prévia, simplesmente por estar investigando um caso e considerar isso necessário.[156]

Atualmente, há mais de 20 casos perante a Suprema Corte do Paraguai que questionam esse procedimento. No entanto, desde 2004, a Corte mantém sua posição, considerando que os metadados não fazem parte das comunicações e, portanto, podem ser solicitados pelo Ministério Público sem ordem judicial.[157]

155 Nações Unidas. Assembleia Geral. (2014). Resolução A/HRC/27/37. O direito à privacidade na era digital, Relatório do Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos. Parágrafo 19. Disponível em: https://docs.un.org/es/A/HRC/27/37

156 Com base no artigo 228 do Código Processual Penal.

157 Para mais informações, consulte o resumo "Quem defende os seus dados" (todas as edições), onde a ISP TIGO disponibiliza o número de pedidos de relatórios que o Ministério Público realiza anualmente. Veja também: https://www.tedic.org/wp-content/uploads/2025/02/QDTD_Paraguai_2024-WEB.pdf

CHILE

No contexto da crise social e política de 2019, a Promotoria Metropolitana Ocidental do Chile[158] solicitou provedores de serviços de internet (ISPs) o fornecimento de dados das pessoas assinantes de serviços de telefonia móvel que circularam nas proximidades das estações de metrô incendiadas.[159] Nessa solicitação, era exigido o acesso a todos os números de telefone que se conectaram às antenas e células da *Entel*, *Movistar* e *WOM* entre 18 e 28 de outubro cerca de 5 estações de Metrô na zona oeste de Santiago.[160]

O Ministério Público apresentou o pedido em duas ocasiões, nos dias 4 e 12 de novembro de 2019. Na primeira, solicitou, por meio da Brigada de Investigações Policiais Especiais (doravante, "BIPE") da Polícia de Investigações do Chile (doravante, "PDI") à *Entel*, *Movistar* e *WOM* a entrega de informações sobre o tráfego das antenas telefônicas instaladas entre os municípios de Maipú e Pudahuel, onde foram registrados os ataques às estações de metrô.

De acordo com relatos publicados pelo meio de comunicação *La Tercera*[161], a *WOM* foi a única empresa que forneceu as informações na primeira solicitação, sem que houvesse uma ordem judicial necessária prevista por lei[162] tal entrega. A *Movistar* recusou-se e a *Entel* forneceu os dados de forma parcial.

Em consequência do acima exposto, ocorreu a segunda solicitação, em que o Ministério Público apresentou um pedido ao Nono Tribunal de Garantia de Santiago, solicitando ao tribunal uma ordem judicial geral para que a *Entel* e a *Movistar* entregassem as informações exigidas pelo Ministério Público[163]. Em 12 de novembro, o tribunal ordenou a entrega dos dados sobre todos os telefones celulares que se conectaram às antenas dessas empresas de telefonia nas estações atacadas.

A respeito, a *WOM* emitiu um comunicado manifestando que:

> Solicitou-se maior precisão na solicitação enviada pelo órgão e, uma vez recebida a esclarecimento, procedeu-se ao cumprimento da ordem judicial remetida pelo Ministério Público. Esta informação refere-se apenas ao tráfego nas nossas antenas, o que não implica dados específicos dos clientes.[164]

De acordo com uma consulta feita pelo CIPER Chile ao Ministério Público em 2023,[165] seis pessoas foram condenadas pelos ataques às estações de metrô na zona oeste de Santiago. Até o momento, foi estabelecida uma correlação entre a sua condenação e o pedido de informação do Ministério Público às empresas de telefonia móvel.

---

158 BioBioChile (2020). O Ministério Público solicitou dados às empresas de telefonia móvel para identificar os autores dos ataques às estações do metrô. Disponível em: https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/moviles-y-computacion/2020/01/08/afirman-que-wom-entrego-informacion-de-usuarios-durante-estallido-social-compania-se-defendio.shtml

159 As medidas de vigilância apresentadas respondem a um caso de geofence. Isso consiste na solicitação, por parte das autoridades, dos dados de localização e identificação reversa das pessoas que estavam circulando perto de certas estações do metrô de Santiago que haviam sido incendiadas.

160 La Tercera (2019). O Ministério Público solicita informações sobre as antenas de celular dos dias em que ocorreram os ataques ao metrô. Disponível em: https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

161 La Tercera (2020). WOM sobre a entrega de informações ao Ministério Público por ataque ao metrô: "Não envolve dados específicos dos clientes". Disponível em: https://www.latercera.com/nacional/noticia/wom-entrega-informacion-fiscalia-ataque-metro-no-implica-datos-especificos-los-clientes/966760/

162 Consagrado no artigo 19 da Lei 21732.

163 La Tercera (2019). O Ministério Público solicita informações sobre as antenas de celular dos dias em que ocorreram os ataques ao metrô. Disponível em: https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

164 La Tercera (2020). WOM sobre a entrega de informações ao Ministério Público por ataque ao metrô: "Não envolve dados específicos dos clientes". Disponível em: https://www.latercera.com/nacional/noticia/wom-entrega-informacion-fiscalia-ataque-metro-no-implica-datos-especificos-los-clientes/966760/

165 CIPER (2023). O Ministério Público encerrou os processos relativos aos ataques ao metrô: condenou 14 pessoas e não detectou grupos organizados para incendiar estações. Disponível em: https://www.ciperchile.cl/2023/10/17/fiscalia-cerro-las-causas-por-ataques-al-metro-condeno-a-14-personas-y-no-detecto-grupos-organizados-para-quemar-estaciones/

MÉXICO

No México, o artigo 190, seção II, da Lei Federal de Telecomunicações e Radiodifusão (doravante, "LFTR")[166] estabelece a obrigação dos concessionários de telecomunicações de conservar, por dois anos, um registro dos metadados das comunicações de todos os seus usuários de forma indiscriminada. Esse registro inclui metadados como: origem e destino das comunicações; data, hora e duração; dados de identificação dos comunicantes e dos dispositivos; e até mesmo a localização geográfica aproximada dos usuários.

O artigo 190, seção III da LFTR estabelece, por sua vez, a obrigação de entrega dos dados conservados às autoridades habilitadas a acessar tal registro. Nesse sentido, por meio de solicitações de acesso à informação, a R3D: Rede em Defesa dos Direitos Digitais detectou que existem sérias discrepâncias entre o número de acessos relatados pelas autoridades competentes, o poder judiciário federal e as empresas de telecomunicações, sugerindo uma prática generalizada de acesso ilegal aos dados conservados pelas empresas de telecomunicações.

Além disso, há evidências de que o mecanismo excepcional previsto no artigo 303 do CNPP, pelo qual as autoridades podem solicitar diretamente o acesso aos dados, sem controle judicial prévio, tem sido sistematicamente abusado para obter tais informações sem qualquer controle judicial.

Entre os abusos documentados, há evidências reveladas pelo *The New York Times* em novembro de 2023 sobre como a Procuradoria Geral da Justiça da Cidade do México acessou registros telefônicos, mensagens de texto e dados de localização de várias figuras políticas, tanto do partido governista quanto da oposição.[167]

O Ministério Público solicitou essas informações à empresa de telecomunicações *Telcel*, argumentando que esses dados seriam utilizados em investigações sobre sequestros e desaparecimentos forçados e invocando as causas de exceção à autorização judicial prévia a que se refere o artigo 303 do CNPP.

De acordo com o *The New York Times*, entre as pessoas vigiadas desde 2021 até o momento estão Dolores Igareda, alta funcionária da Suprema Corte de Justiça da Nação; Ricardo Amezcua, membro do judiciário da Cidade do México; Santiago Taboada, prefeito e candidato à chefia do governo da capital; Higinio Martínez, senador do Morena pelo Estado do México; Horacio Duarte, então titular da Agência Nacional de Alfândegas; a senadora Lilly Tellez e a ex-legisladora Alessandra Rojo de la Vega. De acordo com o jornal, nenhuma dessas pessoas estava envolvida em casos de sequestro.

Esse *modus operandi* das autoridades também foi denunciado em 2019 pela jornalista Marcela Turati, pela cofundadora da Equipe Argentina de Antropologia Forense (EAAF), Mercedes Doretti, e pela defensora dos direitos humanos Ana Lorena Delgadillo. Elas apontaram que a Subprocuradoria Especializada em Investigação de Crime Organizado (doravante, "SEIDO") do México acessou seus registros telefônicos ao incluí-las na mesma pasta em que eram investigados membros de uma organização criminosa.[168]

---

166 Lei Federal de Telecomunicações e Radiodifusão, Disponível em: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf – próxima a ser reformada, pelo que os artigos 189 e 190 passarão a ser os artigos 160 e 161 da nova lei.

167 Maria Abi-Habib, Natalie Kitroeff e Emiliano Rodríguez Mega (2023). Políticos e funcionários, alvos de vigilância no México. https://www.nytimes.com/es/2023/11/09/espanol/mexico-vigilância-fiscalia-telcel.html

168 R3D. (2021). SEIDO acessou registros telefônicos para espionar jornalista e defensoras por investigarem massacre de San Fernando. Disponível em: https://r3d.mx/2021/11/26/seido-accedio-a-registros-telefonicos-para-espiar-a-periodista-y-defensoras-por-investigar-masacre-de-san-fernando/

A SEIDO investigou Turati, Delgadillo e Doretti pelos crimes de desaparecimento forçado e sequestro. Dessa forma, as autoridades tiveram acesso às suas informações pessoais, aos telefones que usavam e à sua localização geográfica. No caso de Turati, também obtiveram os dados pessoais que ela forneceu ao Ministério das Relações Exteriores para solicitar seu passaporte.

Cabe ressaltar que o acesso aos dados conservados foi feito sem autorização judicial e que, sob nenhuma circunstância, o acesso a tais informações pode ser considerado justificado, uma vez que não há qualquer indício de que a jornalista, a defensora e o perito, respectivamente, tenham participado da prática de qualquer crime, mas que sua participação no caso consistiu exclusivamente no acompanhamento das famílias das vítimas denunciantes.

A partir desses casos, observou-se um *modus operandi* no México em que os ministérios públicos abrem uma investigação ou utilizam uma já existente e, com base em "informações anônimas", solicitam às empresas de telecomunicações que lhes forneçam informações sobre números que não têm relação com nenhum crime. Dessa forma, são utilizados processos sobre sequestro ou outros crimes graves com a intenção de eludir a obrigação de obter autorização judicial federal prévia.

Além disso, em nenhum caso submetem à ratificação judicial os pedidos de acesso a dados conservados, contrariando o disposto no artigo 303 do CNPP. Para isso, argumentam que não encontraram utilidade na informação e, por isso, não fazia sentido solicitar a ratificação judicial, pelo que, de forma impossível de verificar, procederam à sua destruição.

O esquema documentado sugere que poderia haver muitos outros casos em que as autoridades obtiveram das empresas de telecomunicações, metadados de comunicações e geolocalização em tempo real de forma fraudulenta, sem que fossem realizadas investigações que permitissem identificar outras vítimas e punir os responsáveis.

III. Obtenção de informação

Dentro do gênero de intervenção em comunicações privadas, outras tecnologias de intervenção em comunicações detectadas na região são as ferramentas de obtenção forense.

Essas ferramentas permitem extrair de um dispositivo físico todas as informações armazenadas, incluindo comunicações privadas, dados de identificação das comunicações, bem como informações, documentos, arquivos de texto, áudio, imagem ou vídeo contidos em qualquer dispositivo, acessório, aparelho eletrônico, equipamento informático, aparelho de armazenamento e tudo o que possa conter informações, incluindo as armazenadas em plataformas ou centros de dados remotos vinculados a eles.[169]

Eles também permitem a clonagem de cartões SIM, obtenção de senhas, recuperação de informações apagadas e, em alguns casos, permitem conhecer o conteúdo de aplicativos de mensagens como WhatsApp, iMessage, entre outros.

A empresa israelense *Cellebrite* é a desenvolvedora da ferramenta de obtenção forense mais popular do mundo. Há anos, a comercialização desses produtos para dezenas de governos, incluindo regimes autocráticos ou opressivos de países como China, Turquia, Venezuela, Bielorrússia, Rússia e Bangladesh, vem sendo documentada. Esses governos têm usado esses equipamentos para vigiar injustificadamente dissidentes, jornalistas, ativistas, pessoas da comunidade LGBTIQ+ e pessoas pertencentes a minorias étnicas.[170]

---

169 Foi levada em consideração a definição legal do artigo 291 do CNPP, parágrafo 4, reformado em 17 de junho de 2016.

170 Access Now. (2021). O que a empresa de espionagem Cellebrite não consegue esconder dos investidores. Disponível em: https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/

A partir da polêmica em torno do abuso dos equipamentos vendidos pela *Cellebrite* e de seu interesse em abrir o capital na bolsa de valores, a empresa declarou que formaria um comitê de ética e deixaria de vender seus produtos a governos autoritários ou opressores. No entanto, ex-funcionários da empresa declararam que ela não fez nada para prevenir abusos.[171] Os casos em que agiu contra abusos foram aqueles que chegaram aos meios de comunicação ou aqueles em que foi obrigada a agir por meio de processos legais.[172]

MÉXICO

No México, dezenas de autoridades federais e estaduais adquiriram ferramentas de obtenção forense desenvolvidas pela *Cellebrite* e outras empresas semelhantes. Em muitos casos, a legalidade de sua utilização é questionável e, na maioria dos casos, existe uma opacidade generalizada em relação ao seu uso.[173]

PARAGUAI

No Paraguai, há evidências de que o Ministério Público e a Polícia Nacional utilizaram o *Septier*, de acordo com dados de contratos públicos, pelo menos em 2018, durante o governo do presidente Mario Abdo Benitez, por meio da empresa *Winner*.[174]

IV. Spyware

Uma das tecnologias de vigilância mais invasivas que foram detectadas é o uso de sistemas de vigilância conhecidos como *spyware*. Embora as características possam variar, normalmente a infecção de um dispositivo através da operação de um *spyware* permite a interceptação e coleta indiscriminada de todos os tipos de comunicações e dados, criptografados ou não, bem como o acesso remoto e secreto a dispositivos pessoais e aos dados armazenados neles, o que facilita a vigilância em tempo real e a manipulação dos dados contidos nesses dispositivos.[175] Ou seja, a tecnologia empregada por um *spyware* dá aos seus usuários não apenas a capacidade de monitorar a pessoa, mas também de manipular o dispositivo infectado, incluindo a alteração, exclusão ou até mesmo a implantação de informações incriminatórias.

Uma vez infectado um dispositivo, normalmente os operadores do *spyware* podem gravar comunicações de vídeo e áudio; coletar mensagens, textos e e-mails (mesmo de plataformas supostamente seguras); bem como acessar calendários, contatos e dados de geolocalização. Eles também podem acessar outros dispositivos conectados, como dispositivos tecnológicos vestíveis ou veículos, que podem conter mais dados relativos à saúde e à localização da pessoa.[176]

---

171 Haaretz. (2021). Trabalhei na empresa israelense de hacking telefônico Cellebrite. Eles mentiram para nós. Disponível em: https://www.haaretz.com/israel-news/2021-07-27/ty-article/i-worked-at-israeli-phone-hacking-firm-cellebrite-they-lied-to-us/0000017f-f652-d460-afff-ff764fae0000

172 Dhaka Tribune. (2021). Empresa israelense de hacking telefônico Cellebrite vai interromper vendas para Bangladesh. Disponível em: https://www.dhakatribune.com/world/middle-east/255655/israeli-phone-hacking-firm-cellebrite-to-stop

173 Rede em Defesa dos Direitos Digitais (R3D). (2025). O Estado da Vigilância. Disponível em: https://r3d.mx/wp-content/uploads/EDLV_2025.pdf https://r3d.mx/wp-content/uploads/EDLV_2025.pdf

174 Vinner SRL. Ver: https://winner.com.py/

175 Nações Unidas. Assembleia Geral. (2018). Resolução A/HRC/39/29. O direito à privacidade na era digital. Parágrafo 19. Disponível em: https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high: Os governos parecem recorrer cada vez mais a programas informáticos de interceptação maliciosa que se infiltram nos dispositivos digitais das pessoas. Esse tipo de pirataria informática permite a interceptação e a coleta indiscriminada de todos os tipos de comunicações e dados, criptografados ou não, bem como o acesso remoto e secreto a dispositivos pessoais e aos dados armazenados neles, o que facilita a vigilância em tempo real e a manipulação dos dados contidos nesses dispositivos."

176 Nações Unidas. Assembleia Geral. (2022). Resolução A/HRC/51/17. O direito à privacidade na era digital. Disponível em: https://docs.un.org/es/A/HRC/51/17

A seguir, exemplificamos sua utilização com casos documentados no **Paraguai**, **México** e **El Salvador**.

PARAGUAI

Em 2012, o governo paraguaio adquiriu o software espião *FinFisher*[177], conforme revelado por investigações do Citizen Lab da Universidade de Toronto e do jornal ABC Color. Essas investigações incluem documentação oficial, como faturas de compra, bem como atas de entrega e recebimento assinadas pela Secretaria Nacional Antidrogas (SENAD), o que confirma o uso estatal desse malware para atividades de vigilância.

Outro caso relevante é o do software *Galileo* – Sistema de Controle Remote (RCS), desenvolvido pela empresa *Hacking Team*. Os vazamentos de *Wikileaks*[178] apresentaram comunicações entre esta empresa e o Ministério Público do Paraguai, que evidenciam uma intenção de compra do sistema. Posteriormente, em outubro de 2014, o parceiro local da *Hacking Team* solicitou um equipamento adicional, o que sugere um interesse sustentado por parte das autoridades paraguaias nesta tecnologia de espionagem.

Além disso, os vazamentos de *Wikileaks*[179] revelaram conversas diplomáticas sobre a aquisição de equipamentos de escuta telefônica pelo Ministério do Interior em 2010. Essa prática se concretizou em 2012, durante o governo de Federico Franco, quando foi adquirido um equipamento no valor de US$ 2,5 milhões. No entanto, esse equipamento desapareceu misteriosamente dos escritórios do Ministério do Interior, conforme denunciado em um relatório da Auditoria Geral do Poder Executivo em novembro de 2013.[180]

Embora não existam casos concretos e plenamente identificados de vigilância dos cidadãos no Paraguai, não se descarta que tais práticas estejam sendo realizadas. Esses antecedentes sugerem que o país poderia estar seguindo as tendências regionais em matéria de vigilância estatal, muitas vezes marcadas pela opacidade e pela falta de controles públicos.

177 Citizen Lab (2015). Não preste atenção ao servidor por trás do proxy. Disponível em https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

178 Wikileaks. (2014). Nota sobre o Paraguai. Disponível em: https://wikileaks.org/hackingteam/emails/emailid/249367

179 Wikileaks. (2010). Nota sobre o Paraguai Disponível em: https://wikileaks.org/plusd/cables/10ASUNCION97_a.html

180 Sequera, M., Samaniego, M. Crime cibernético: Desafios da harmonização da Convenção de Budapeste no sistema penal paraguaio. Pág. 48. Disponível em: https://www.direitosDigitais.org/wp-content/uploads/minuta_TEDIC.pdf

MÉXICO

No México, a aquisição e o abuso de tecnologias de *spyware* foram amplamente documentados, tanto em relação ao *spyware FinFisher* da empresa Gamma International;[181] *Galileo* de *Hacking Team*;[182] quanto ao *Pegasus* da empresa israelense *NSO Group*. A seguir, sintetizamos as principais descobertas sobre o *spyware Pegasus*.[183]

A *NSO Group Technologies* é uma das empresas cujo nome tem sido amplamente associado a ações de vigilância em vários países, incluindo o México.[184] A empresa afirma que sua tecnologia é utilizada exclusivamente por clientes governamentais aprovados pelo Ministério da Defesa de Israel.[185] Apesar de afirmar respeitar uma política de direitos humanos, o número de casos documentados em que sua tecnologia é utilizada de forma abusiva contra a sociedade civil em todo o mundo continua a crescer.

O primeiro antecedente do *Pegasus* no México foi registrado em 2012, quando investigações jornalísticas publicaram que a Secretaria de Defesa Nacional (doravante, "SEDENA") se tornou o primeiro cliente internacional do *NSO Group* ao adquirir o sistema *Pegasus* como parte de uma série de contratos celebrados com a empresa *Security Tracking Devices S.A. de C.V.*, que totalizaram 5,6 bilhões de pesos.[186] Esses contratos foram celebrados após uma demonstração do funcionamento do sistema *Pegasus* em maio de 2011 ao então presidente Felipe Calderón, bem como ao Secretário de Defesa Nacional, Guillermo Galván Galván.[187]

Em junho de 2017, o Citizen Lab, assim como a ARTICLE 19, a Rede em Defesa dos Direitos Digitais (R3D) e a SocialTIC publicaram o relatório *"Governo Espião: Vigilância sistemática a jornalistas e defensores dos direitos humanos no México"*,[188] no qual são relatados vários casos de tentativas de infecção contra defensores dos direitos humanos e jornalistas com o malware *Pegasus* durante o governo do presidente Peña Nieto.[189]

---

181 Em 2013 e 2015, uma investigação do Citizen Lab – laboratório multidisciplinar da Universidade de Toronto – revelou evidências da presença de servidores de comando e controle da FinFisher em 32 países, incluindo o México#. O então Instituto Federal de Acesso à Informação e Proteção de Dados (IFAI) anunciou o início de uma investigação#, mas nenhum resultado relevante foi divulgado.

182 Uma grande quantidade de e-mails e documentos internos da empresa italiana Hacking Team foram divulgados ao público em 5 de julho de 2015. Neles, ficou evidente que a empresa de software de espionagem havia vendido seus produtos a governos de países em grave crise de direitos humanos, como Bahrein, Sudão e Uzbequistão. De um total de 35 nações, o México acabou sendo o principal cliente da empresa, com transações feitas por diferentes governos locais, órgãos e agências federais por meio de empresas intermediárias e, em praticamente todos os casos, sem poderes legais para fazê-lo. O gráfico a seguir mostra os gastos do México em relação a outros países clientes da Hacking Team.

183 Na região, surgiram informações sobre outros países onde o uso do Pegasus poderia ter sido implantado, incluindo possivelmente a Colômbia. No entanto, o caso mais bem documentado e sobre o qual existe mais evidência sobre o uso do Pegasus na região é, sem dúvida, o do México.
Sobre o caso da Colômbia. Disponível em: https://es.wired.com/articulos/estados-unidos-confirma-que-financio-el-uso-del-software-espia-pegasus-en-colômbia
Sobre El Salvador. Disponível em: https://elfaro.net/es/202503/el_salvador/27785/embajador-johnson-no-dudo-que-pudo-haberse-usado-pegasus-en-el-salvador

184 Sobre Panamá. Disponível em: www.univision.com/noticias/especiales/exclusiva-martinelli-tambien-espio-a-estadounidenses-dice-testigo
Cox, J. & L. Franceschi Bicchierai, (2016). "Conheça o NSO Group, o novo grande player no setor de spyware governamental", Motherboard. Disponível em: https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware

185 Ibidem.

186 Aristegui Noticias. (2012). O governo federal, por meio da Sedena, comprou 5 bilhões de pesos em equipamentos de espionagem. Disponível em: https://aristeguinoticias.com/1607/mexico/gobierno-federal-via-sedena-compro-5-mil-mdp-en-equipo-para-espionaje/

187 Rede em Defesa dos Direitos Digitais (R3D). (2021). O NSO Group mostrou o Pegasus a Felipe Calderón e ao seu Secretário de Defesa.. Disponível em: https://r3d.mx/2021/08/11/nso-group-mostro-pegasus-a-felipe-calderon-y-su-secretario-de-defensa

188 Rede em Defesa dos Direitos Digitais (R3D). (2017). Governo espião: Vigilância sistemática a jornalistas e defensores dos direitos humanos no México. Disponível em: https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

189 Ahmed, A., & Perlroth, N. (2017). Usando mensagens de texto como isca, spyware do governo tem como alvo jornalistas mexicanos e suas famílias. The New York Times. Disponível em: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

Apesar da mudança de governo e das repetidas declarações do então presidente da República, Andrés Manuel López Obrador, no sentido de que jornalistas e defensores dos direitos humanos não seriam mais vigiados e que o *Pegasus* e nenhum outro sistema semelhante de interceptação de comunicações privadas não seriam mais utilizados, a vigilância prevaleceu em seu governo. Em 2022 e 2023, a investigação *"Ejército Espía"* revelou novos casos de vigilância com o *Pegasus* atribuíveis com alto grau de certeza ao Exército Mexicano.[190]

Até agora, as vítimas documentadas da espionagem por parte da SEDENA incluem o subsecretário de Direitos Humanos, Alejandro Encinas,[191] o coordenador da Comissão da Verdade para a "Guerra Suja" – o período de desaparecimentos forçados, torturas e execuções cometidas pelas forças de segurança mexicanas, incluindo o exército, entre os anos 1960 e 1980 –, Camilo Vicente Ovalle,[192] uma organização de direitos humanos, o Centro de Direitos Humanos Miguel Agustín Pro Juárez (Centro Prodh), o defensor dos direitos humanos Raymundo Ramos e dois jornalistas, Ricardo Raphael e um jornalista do meio digital Animal Político.[193] **De fato, as infecções com o Pegasus ocorreram em momentos em que as vítimas realizavam trabalhos relacionados a violações dos direitos humanos cometidas pelas Forças Armadas.**

Em 2017, 2022 e 2023, os defensores dos direitos humanos e jornalistas vigiados pelo *spyware Pegasus* apresentaram denúncias criminais ao Ministério Público Especial para Crimes contra a Liberdade de Expressão (doravante "FEADLE") por, entre outros, crimes de interceptação ilegal de comunicações privadas e acesso ilegal a sistemas informáticos. No entanto, até o momento, a impunidade prevaleceu.

O fato de uma das vítimas, o Centro Prodh, ter sido alvo de vigilância com o *Pegasus* em dois governos diferentes e ter apresentado duas denúncias criminais diferentes mostra como a impunidade e a falta de medidas adequadas levaram à repetição da vigilância ilegal.

EL SALVADOR

Entre julho de 2020 e novembro de 2021, o mesmo software *Pegasus* foi usado para infectar 35 dispositivos pertencentes a jornalistas e membros da sociedade civil, de acordo com o relatório do *Projeto Torogoz* desenvolvido pelo Citizen Lab e Access Now.[194]

O relatório apontou que, das 35 pessoas que foram infectadas e vigiadas com o software, 22 são membros do meio de investigação jornalística *El Faro*.[195] O relatório concluiu ainda que o acesso aos dispositivos móveis dos jornalistas coincide com momentos anteriores à publicação de reportagens do *El Faro* com informações de interesse público.

190 Rede em Defesa dos Direitos Digitais (R3D). Exército Espião. Disponível em: https://ejercitoespia.r3d.mx/

191 Kitroeff, Natalie & R. Bergman, "Presidente mexicano disse que pediu a aliado para não se preocupar com espionagem", The New York Times, 23 de maio de 2023, Disponível em: https://www.nytimes.com/2023/05/23/world/americas/mexico-president-spying-pegasus.html

192 Lopez, Oscar & M. Sheridan, "Ele está liderando a investigação do México sobre a Guerra Suja. Quem o está espionando?", The Washington Post, 23 de junio de 2023, Disponível em: https://www.washingtonpost.com/world/2023/06/03/mexico-pegasus-dirty-war-lopez-obrador/

193 Rede em Defesa dos Direitos Digitais (R3D), Artigo 19, Social Tic, et. al., Exército Espião, Disponível em: https://ejercitoespia.r3d.mx/

194 The Citizen Lab & Access Now. (2022). Projeto Torogoz: Hackeamento extensivo da mídia e da sociedade civil em El Salvador com o spyware Pegasus. Universidade de Toronto. Disponível em: https://utoronto.scholaris.ca/items/025fd761-7d3f-4356-b6f8-f43eeab65128

195 Ver: https://elfaro.net/es?ref=inicio

Este caso ocorreu durante o primeiro mandato do presidente Nayib Bukele em El Salvador. O governo negou qualquer ligação com esses fatos e afirmou não ser cliente do *NSO Group*.[196] No entanto, o relatório do *Projeto Torogoz* afirma que, embora não haja provas que liguem a infecção específica a um cliente específico da *Pegasus*, foi possível identificar um cliente da *Pegasus* que opera em El Salvador desde novembro de 2019, ao qual deram o nome de "*Torogoz*".[197] Além disso, como mencionado anteriormente, o *NSO Group* declarou que este software é vendido apenas a governos.[198]

A CIDH e sua RELE, bem como o Escritório Regional do Alto Comissariado das Nações Unidas para os Direitos Humanos (doravante, OACNUDH) manifestaram preocupação com as informações sobre o uso do *Pegasus* contra jornalistas e organizações da sociedade civil em El Salvador. Por sua vez, exortaram o Estado a investigar o caso de forma eficaz e imparcial e a garantir a proteção das vítimas.[199]

Em nível nacional, a organização *Cristosal*, dedicada à defesa dos direitos humanos, apresentou uma ação perante a Câmara de Contencioso Administrativo da Suprema Corte de Justiça contra a Corte de Contas de El Salvador por se recusar a investigar o possível uso de fundos estatais para a compra do *Pegasus*. No entanto, a ação foi indeferida.[200] A *Cristosal* declarou que apresentaria um recurso por falta de investigação sobre o uso de fundos estatais para a compra do software.[201]

Em nível internacional, em dezembro de 2022, jornalistas do *El Faro* apresentaram uma denúncia contra o *NSO Group* perante um tribunal federal nos Estados Unidos. A ação foi movida com o objetivo de que a empresa revelasse quem é o cliente que comprou o *Pegasus*, esclarecesse quais informações foram coletadas dos jornalistas, o que foi feito com essas informações e que elas fossem eliminadas de seus servidores.[202] O caso foi indeferido com base no argumento de que nem os réus nem os autores estavam nos Estados Unidos.[203]

Em julho de 2024, empresas de tecnologia e organizações de imprensa dos Estados Unidos apresentaram um *amicus curiae* ao Nono Tribunal de Apelações para apoiar a ação movida pelos membros do *El Faro* contra o *NSO Group*. A ação está em fase de apelação devido à rejeição inicial do caso.[204]

---

196 Abi-Habib, M. (2022). O software espião Pegasus foi usado para hackear jornalistas em El Salvador. The New York Times. Disponível em: https://www.nytimes.com/es/2022/01/12/espanol/el-faro-pegasus.html

197 The Citizen Lab & Access Now. (2022). Projeto Torogoz: Hackeamento extensivo da mídia e da sociedade civil em El Salvador com o spyware Pegasus. Universidade de Toronto. Disponível em: https://utoronto.scholaris.ca/items/025fd761-7d3f-4356-b6f8-f43eeab65128

198 NDTV. (2021). Empresas como a NSO não podem vender o Pegasus a entidades não governamentais, afirma o embaixador de Israel na Índia. Disponível em: https://www.ndtv.com/india-news/firms-like-nso-cant-sell-pegasus-to-non-government-actors-israels-ambassador-to-india-2590792

199 Comissão Interamericana de Direitos Humanos (CIDH). (2022). A CIDH, sua Relatoria Especial para a Liberdade de Expressão e a OACNUDH expressam preocupação com as descobertas sobre o uso do software Pegasus em El Salvador. https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

200 Swissinfo.ch. (2023). O Supremo Tribunal de El Salvador não admite ação contra órgão que não investigou o Pegasus. Disponível em: https://www.swissinfo.ch/spa/el-supremo-salvadore%C3%B1o-no-admite-demanda-contra-ente-que-no-investig%C3%B3-pegasus/48445076

201 DW. (2023, mayo 1). ONG presentará demanda de amparo ante Corte Suprema de El Salvador por espionaje con Pegasus a periodistas. LatAm Journalism Review. https://latamjournalismreview.org/es/news/ong-presentara-demanda-de-amparo-ante-corte-suprema-de-el-salvador-por-espionaje-con-pegasus-a-periodistas/

202 De Assis, C. (2022). Depois de terem sido espionados, alguns jornalistas do El Faro processam nos Estados Unidos o fabricante do spyware Pegasus. LatAm Journalism Review. Disponível em: https://latamjournalismreview.org/es/articles/tras-haber-sido-espiados-periodistas-de-el-faro-demandan-en-estados-unidos-al-fabricante-del-spyware-pegasus/

203 Electronic Privacy Information Center. (2024). Dada et al. v. NSO Group. Disponível em: https://epic.org/documents/dada-et-al-v-nso-group/

204 Gressier, R. (2024). Gigantes de tecnologia e imprensa reconhecem o recurso do El Faro no caso Pegasus. El Faro. Disponível em: https://elfaro.net/es/202407/el_salvador/27511/Gigantes-de-tecnolog%C3%ADa-y-prensa-dan-espaldarazo-a-la-apelaci%C3%B3n-de-El-Faro-en-caso-Pegasus.htm

V. Geolocalização baseada na exploração de vulnerabilidades na infraestrutura de telecomunicações (SS7)

Além de antenas, a rede de telefonia móvel é formada por comutadores, interfaces e bancos de dados que permitem localizar os dispositivos e obter as informações necessárias para fornecer o serviço de telecomunicações.

A forma como nossos dispositivos e antenas se comunicam é ditada por um protocolo. O sistema de sinalização por canal comum Nro. 7 (SS7) é um conjunto de protocolos utilizados pelos operadores de redes móveis para trocar informações, estabelecer e encaminhar chamadas telefônicas, mensagens de texto e outras comunicações dentro das redes 2G e 3G.[205]

O protocolo foi adotado há quase quarenta anos, numa época em que o campo das telecomunicações móveis era composto por poucas empresas, conhecidas entre si, pelo que não foi concebido com medidas de autenticação. A falta de medidas contra acessos ilegítimos fez com que o protocolo fosse abusado por diversas entidades para fins de vigilância. Dois casos representativos de geolocalização com base na exploração dessas vulnerabilidades encontram-se no **Brasil** e no **Peru**.

BRASIL

No início de 2023, a imprensa revelou que a Agência Brasileira de Inteligência (Abin) utilizou ilegalmente ferramentas de geolocalização de dispositivos eletrônicos durante o governo Bolsonaro (2019-2022), sendo a principal delas o *spyware FirstMile*.[206]

O *FirstMile*, desenvolvido pela empresa israelense Cognyte (ex-Verint), é um software espião que explora vulnerabilidades nas redes de telecomunicações (SS7) para rastrear a localização de dispositivos móveis. A tecnologia permitia monitorar até 10.000 celulares por ano, bastando inserir o número de telefone do alvo, independentemente da rede utilizada (3G, 4G ou 5G). A partir de um número de telefone inserido, o *FirstMile* pode fornecer a localização de um dispositivo – e, portanto, da pessoa a quem ele pertence – com base em sua posição ao se conectar a uma rede móvel.

No Brasil, a empresa *Suntech* atuou como representante e desenvolvedora do *FirstMile*, segundo informações da Associação Catarinense de Empresas de Tecnologia (Acate).[207] contrato para a aquisição desse software foi assinado diretamente pela Abin em dezembro de 2018, durante o final do governo de Michel Temer. A aquisição ocorreu por meio do contrato 567/2018[208], que é confidencial.

Não se sabe ao certo quantas vezes o programa de espionagem foi utilizado, mas há registros[209] de que ele foi empregado para espionar cidadãos brasileiros entre 26 de dezembro de 2018 e 8 de maio de 2021, período do contrato em que a ferramenta foi adquirida, conforme confirmado pela Agência Brasileira de Inteligência. Investigadores indicam[210] que, embora o contrato tenha terminado em 2021, há sinais de que o sistema foi usado com maior frequência nos últimos anos do governo Bolsonaro (2019-2022) para vigiar ilegalmente funcionários públicos, políticos, policiais, advogados, jornalistas e até mesmo juízes e membros do Supremo Tribunal Federal (doravante, STF).

---

205 Electronic Frontier Foundation. (2024). EFF para a FCC: O SS7 é vulnerável, e as empresas de telecomunicações devem reconhecer isso. Disponível em: https://www.eff.org/deeplinks/2024/07/eff-fcc-ss7-vulnerable-and-telecoms-must-acknowledge

206 Dantas, D.; Camporez, P.; Bronzatto, T.. Abin de Bolsonaro usou programa secreto para monitorar localização de pessoas por meio do celular. O Globo, 14 mar. 2023. Disponível em: https://oglobo.globo.com/politica/noticia/2023/03/abin-de-bolsonaro-usou-programa-secreto-para-monitorar-localizacao-de-pessoas-por-meio-do-celular.ghtml.

207 G1. First Mile: o que se sabe sobre o software espião usado pela Abin. G1, 25 jan. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml.

208 Ibidem.

209 Ibidem.

210 G1. PF prende dois servidores e apura se Abin rastreou celulares de forma ilegal na gestão Bolsonaro. G1, 20 oct. 2023. Disponível em: https://g1.globo.com/politica/noticia/2023/10/20/policia-federal-abin-geolocalizacao.ghtml.

Por exemplo, relatórios indicam que o software foi amplamente utilizado entre maio de 2020 e abril de 2022, durante o mandato de Alexandre Ramagem como chefe da Abin, para monitorar ilegalmente agentes públicos - incluindo jornalistas, juízes do STF e opositores políticos - e outros cidadãos, sugerindo um possível uso para intimidação ou controle de dissidência.[211] Na época, a agência operava sob a supervisão do Gabinete de Segurança Institucional (GSI) da Presidência da República, comandado pelo general Augusto Heleno.

Investigações da Polícia Federal iniciadas em 2023 sugerem que um grupo dentro da Abin, especialmente durante o mandato de Ramagem, instrumentalizou a agência para o monitoramento ilegal de autoridades, funcionários públicos e outros cidadãos sem qualquer controle judicial ou legislativo, o que permitiu que essa vigilância em massa ocorresse sem que as vítimas fossem notificadas ou tivessem qualquer possibilidade de defesa.[212] Sua forma de utilização levanta questões de abuso de poder e violação de direitos constitucionais.

As investigações estão em andamento, e os documentos obtidos até o momento indicam que a Abin realizou operações de monitoramento ilegal com a ferramenta por pelo menos três anos, sem transparência sobre seu uso ou mecanismos de prestação de contas.[213] A falta

de transparência na aquisição e uso da ferramenta continua sendo um dos principais pontos de investigação da Polícia Federal e do STF em 2024.

Em janeiro de 2023, a Polícia Federal lançou a *"Operação Última Milha"* para investigar a instrumentalização da Abin para fins políticos, a chamada "Abin paralela". De acordo com a decisão do Ministro Alexandre de Moraes, a investigação indica a existência de um núcleo político na Abin, especialmente sob a gestão de Alexandre Ramagem, que usou ilegalmente a tecnologia para monitorar autoridades, funcionários públicos e cidadãos.

Em janeiro de 2024, a Polícia Federal deflagrou a *Operação Vigilância Aproximada* - um desdobramento da Última Milha - para investigar uma organização criminosa dentro da Abin que monitorava ilegalmente pessoas e autoridades, invadindo aparelhos eletrônicos e infraestruturas de telecomunicações. Um dos investigados é o deputado Alexandre Ramagem (PL-RJ), ex-diretor da Abin. Foram cumpridos 21 mandados de busca e apreensão e pelo menos sete agentes da Polícia Federal estão sendo investigados. Em 2025, os desdobramentos do caso levaram à suspensão do policial federal Carlos Afonso Gonçalves Gomes Coelho, coordenador do Comando de Aviação Operacional da Polícia Federal, acusado de fazer parte do "núcleo da alta administração" da "Abin paralela" junto com Ramagem na época dos fatos.

Em janeiro de 2024, a Agência Nacional de Telecomunicações (Anatel) abriu três processos administrativos sigilosos para investigar o possível envolvimento de empresas de telefonia móvel no monitoramento ilegal de telefones celulares usando o software *FirstMile*. Está sendo investigado se as operadoras identificaram tentativas de acesso indevido às informações na época ou se só tomaram conhecimento posteriormente, por meio da imprensa. Seu dever de comunicação com a agência também está sendo examinado. As empresas negaram ter tido contato com a Abin ou conhecimento da vigilância ilegal, afirmando que implementaram bloqueios contra o acesso indevido por meio de protocolos de interconexão internacional. Há relatos de que a Abin operou sem interação prévia com as operadoras, mas não está claro quando detectaram os ataques.[214]

---

211 G1. First Mile: o que se sabe sobre o software espião usado pela Abin. G1, 25 jan. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml.

212 Pontes. F.. Abin espionou autoridades do Judiciário, do Legislativo e jornalistas. Agência Brasil, 11 jul. 2024, Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/abin-espionou-autoridades-do-judiciario-do-legislativo-e-jornalistas.

213 Ibidem.

214 STF: Controle de constitucionalidade sobre spyware: [Não investiga o caso concreto, mas busca a regulação desta tecnologia.]

Em dezembro de 2023, a Procuradoria Geral da República (doravante "PGR") ajuizou uma Ação Direta de Inconstitucionalidade por Omissão (ADO 84), convertida na Ação de Descumprimento de Preceito Fundamental (ADPF) 1143 perante o STF. A ação questiona a falta de regulamentação sobre o uso de *spyware* por órgãos públicos. A PGR argumentou que a aquisição e o uso de *spyware*s sem regras claras comprometem direitos fundamentais como a privacidade, a intimidade e o sigilo das comunicações. Ela solicitou que o Congresso Nacional estabelecesse um prazo para aprovar legislação sobre o assunto. O caso ainda está em julgamento, mas, em junho de 2024, o ministro Cristiano Zanin convocou uma audiência pública sobre a ADPF 1143, com a participação de 33 entidades.

PERU

O *Projeto Pisco* foi uma medida de vigilância em massa implementada pelo governo de Ollanta Humala durante os anos de 2011 a 2016, por meio da Direção Nacional de Inteligência (doravante denominada "DINI"). Consistiu na aquisição, sem licitação pública, de um sistema de interceptação legal de comunicações da empresa israelense-americana *Verint Systems*, por um valor de US$ 22 milhões, com financiamento do Ministério da Economia e Finanças.[215]

O sistema permitia a interceptação de chamadas telefônicas, mensagens de texto, e-mails, chats e navegação na web, bem como a geolocalização em tempo real de até 5.000 pessoas e a gravação simultânea de 300 conversas.[216]

Além disso, incluía o módulo *SkyLock*, uma ferramenta capaz de localizar dispositivos móveis dentro e fora do país.[217] Embora tenha sido inicialmente gerenciado pela DINI, o sistema foi posteriormente transferido para o Ministério do Interior, ficando sob a responsabilidade da Direção Geral de Inteligência do Ministério do Interior (doravante denominada "DIGIMIN"). Também se soube que as empresas operadoras *Movistar*, Claro, *Entel* e Bitel assinaram acordos de colaboração para permitir o acesso do Estado a suas redes.[218]

215 Morachimo, M. (2016). O sistema de espionagem das comunicações deixado por Humala. Disponível em: https://hiperdireito.org/2016/08/proyecto-pisco-skylock-peru-verint/

216 Associated Press (2016). Adquirindo ferramentas de espionagem baratas, os países estão "monitorando todo mundo". Disponível em: https://apnews.com/736dd5c3aa644cd499d6f6da8b9e5974

217 Esta ferramenta aproveita vulnerabilidades na infraestrutura de telecomunicações. (como SS7).

218 Direitos Digitais (2016). O Peru pagou US$ 22 milhões para espionar as comunicações de seus cidadãos. Disponível em: https://www.direitosDigitais.org/10389/peru-pago-usd-22-millones-para-espiar-las-comunicaciones-de-sus-ciudadanos/.

Durante o governo do ex-presidente Humala, houve relatos de vigilância e monitoramento de políticos de alto nível, como o ex-presidente Alan García e a candidata da oposição Keiko Fujimori.[219] Consequentemente, embora não haja vítimas identificadas publicamente nem números oficiais sobre as pessoas afetadas, o projeto e o escopo do sistema nos permitem inferir que, se ele tivesse sido usado, qualquer pessoa com acesso a mídia digital ou telefonia móvel poderia ter sido submetida à vigilância, independentemente da profissão ou atividade.

O *Projeto Pisco* foi objeto de investigações legais, políticas e administrativas por vários órgãos do Estado peruano. Por exemplo, na esfera criminal, em 2023, o Ministério Público, por meio da Promotoria Anticorrupção, iniciou uma investigação preliminar contra o ex-presidente Humala e ex-funcionários de alto escalão de seu governo pelo suposto crime de conluio agravado.

A esse respeito, o Ministério Público sustenta que a compra do sistema da empresa israelense-americana *Verint Systems*, avaliada em US$ 22 milhões e realizada sem licitação pública, foi dirigida de forma irregular, causando um prejuízo

econômico ao Estado. Em outubro do mesmo ano, a promotoria apresentou uma acusação solicitando 10 anos e quatro meses de prisão efetiva.[220] Até o momento, nenhuma sentença foi proferida.

Em nível parlamentar, em agosto de 2015, a Comissão de Inteligência do Congresso da República anunciou que analisaria a compra do sistema, descrevendo-a como uma questão prioritária. Foram marcadas sessões para avaliar o caso e o então Controlador Geral Fuad Khoury foi convocado para prestar contas das conclusões da Controladoria Geral.

O Gabinete da Controladoria Geral também teria iniciado investigações sobre a compra do sistema, embora os resultados desses processos não tenham sido totalmente disseminados ou divulgados publicamente.

Da mesma forma, há outros países, como o **Paraguai**, onde, desde 2014, o Ministério do Interior do governo de Horacio Cartes tem usado a tecnologia Septler.[221] No entanto, por motivos de "segurança", não há detalhes no portal de compras públicas e apenas informações sobre a licitação para a empresa GALCORP, S.A. estão disponíveis.[222]

No **México**, o uso de geolocalização ilegal por meio da ferramenta *Geomatrix* do *Rayzone Group* também foi documentado, com evidências de que o Gabinete do Procurador-Geral adquiriu e operou ilegalmente o sistema de geolocalização para espionar as campanhas dos candidatos presidenciais em 2018.[223]

---

219 América TV (2015). DINI: novos documentos confirmariam seguimentos a Alan García e Keiko Fujimori. Disponível em: https://www.americatv.com.pe/cuarto-poder/dini-nuevos-documentos-confirmarian-seguimientos-alan-garcia-y-keiko-fujimori-noticia-22831

220 Infobae (2023). Ministério Público pede dez anos de prisão para Ollanta Humala pelo caso Projeto Pisco. Disponível em: https://www.infobae.com/peru/2023/10/12/ollanta-humala-fiscalia-pide-diez-anos-de-carcel-por-caso-proyecto-pisco/

221 Septier. Ver: https://www.septier.com/products/

222 Contrato de licitação, disponível aqui: https://www.contrataciones.gov.py/licitaciones/adjudicacion/contrato/284615-galcorp-sociedad-anonima-1.html

223 Rede em Defesa dos Direitos Digitais (R3D). (2021). #FiscalíaEspía: A FGR adquiriu equipamentos capazes de espionar ilegalmente todos os usuários da Internet no México. https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/

VI. Patrulhamento cibernético

Outra técnica de vigilância identificada na região é o monitoramento maciço e indiscriminado da Internet - também conhecido como "patrulhamento cibernético" - realizado principalmente por forças de segurança e inteligência. Essa técnica consiste no monitoramento sistemático do conteúdo que circula na Internet que, por ser considerado pelas autoridades como "dados públicos" - dada a sua publicação e circulação on-line - permite seu uso para qualquer finalidade, inclusive vigilância e subsequente processo criminal.[224]

O "Patrulhamento cibernético" pode ser utilizado tanto pela polícia quanto pelas forças militares e deve ser justificado na prevenção, detecção ou investigação de condutas ilegais.

No entanto, quando realizado de forma massiva e indiscriminada, pode levar à violação de direitos fundamentais, como privacidade, proteção de dados pessoais, liberdade de expressão e associação e presunção de inocência.

Na região, a Direitos Digitais compilou em um relatório de 2024[225], a implantação de casos de patrulhamento cibernético em países como Argentina, Brasil, Bolívia, Colômbia, México e Uruguai, bem como a aquisição de tecnologias para esse fim. Também documentou a criação de perfis de agentes secretos falsos que aumentam o alcance do Patrulhamento cibernético na região.

Nesta seção, concentramo-nos na experiência colombiana, embora reconheçamos que, por ser uma prática de vigilância bastante nova, a documentação de informações sobre sua implementação está sendo constantemente atualizada.

COLÔMBIA

Em 2021, várias manifestações públicas foram realizadas contra a administração do Presidente Iván Duque[226], que acabou ficando conhecida como a Greve Nacional de 2021. Nesse contexto, a mídia social se tornou a ferramenta para denunciar abusos e violações de direitos humanos contra cidadãos pelas forças de segurança.

Durante esse período, o Comando Unificado Pós-Cibernético (PMU-Cyber) realizou o monitoramento de fontes abertas.[227] De acordo com as autoridades, o objetivo era identificar notícias falsas nas redes sociais que agiam contra a imagem das instituições públicas e identificar os responsáveis por "atos de vandalismo".

No âmbito das mobilizações, a PMU-Ciber dedicou mais de 20.000 horas para monitorar a atividade dos cidadãos na Internet, ao mesmo tempo em que avançava em uma estratégia para simular um ataque cibernético ao Ministério da Defesa e promover a campanha #ColômbiaEsMiVerdad (#ColômbiaÉMinhaVerdade).[228]

---

224 Camacho, L.; Ospina, D.; Upegui, J.C.(2022). Inteligência estatal na internet e nas redes sociais: o caso colombiano. Dejusticia. Disponível em: https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ; ver também: Zara, N. (2023). Inteligência baseada em fontes abertas (OSINT) e direitos humanos na América Latina: um estudo comparativo na Argentina, Brasil, Colômbia, México e Uruguay. CELE. Disponível em: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf

225 Direitos Digitais (2024). Perfilamento nas redes sociais e patrulhamento cibernético como novas modalidades de vigilância em massa implantadas pelos Estados: casos relevantes na América Latina. Disponível em: https://www.direitosDigitais.org/wp-content/uploads/Informe-RELE-vigilância-masiva_cerrado.pdf

226 Ivan Duque foi eleito candidato do partido Centro Democrático, uma organização política que define como princípios orientadores de sua motivação política "a segurança democrática, a confiança dos investidores, a coesão social, a austeridade estatal e o diálogo popular" e que, de acordo com a Fundação Karisma, é simpatizante das facções mais conservadoras do campo político colombiano.

227 O PMU-Ciber consistiu na cooperação de diferentes autoridades que se coordenaram para realizar atividades de "patrulhamento cibernético". As entidades membros do PMU-Ciber foram, a saber, o Centro Cibernético Policial; o Ministério das Tecnologias da Informação e das Comunicações (MinTIC); o Grupo de resposta a emergências cibernéticas do MinTIC; a Direção Nacional de Inteligência (DNI); a Equipe de Resposta a Incidentes de Segurança Informática da Polícia Nacional; o Comando Conjunto Cibernético das Forças Militares; e a Procuradoria Geral da Nação (FGN), liderada por Francisco Barbosa.

228 Fundação para a Liberdade de Prensa (FLIP). (2021). Os juízes da verdade, o mar de mentiras por trás do patrulhamento cibernético do Estado. https://flip.org.co/pronunciamientos/los-jueces-de-la-verdad-el-mar-de-mentiras-detras-del-ciber-patrullaje-del-estado

Por meio dessa campanha, publicações consideradas falsas na opinião das autoridades de monitoramento foram compartilhadas, sem explicar sob quais critérios uma notícia foi classificada como tal e sem qualquer tipo de contrapeso ou controle. Como parte do monitoramento das mídias sociais, as autoridades começaram a rotular as publicações identificadas como notícias falsas como "terrorismo digital". O rótulo de "terrorismo digital" estigmatizava as opiniões contra as autoridades e censurava as pessoas por meio da exclusão de publicações e contas de mídia social, em total violação dos direitos de acesso à informação e à liberdade de expressão.

Na época, o Ministro da Defesa, Diego Molano, declarou que as notícias foram identificadas como falsas graças a ferramentas como o *Colombiacheck* e o Detector de Mentiras de La Silla Vacía, ambos verificadores de notícias de âmbito nacional.[229] Esses dois verificadores afirmaram que suas classificações de conteúdo falso seguem determinados critérios e metodologias de verificação, que envolvem uma explicação do motivo pelo qual o conteúdo é classificado dessa forma e os insumos informativos.

De acordo com investigação conduzida pela *Fundação Karisma*, dentro das atividades de patrulhamento cibernético na Greve Nacional de 2021, também foi implementada a prática de "agente infiltrado em ambientes virtuais", de acordo com o disposto no art. 16 da Lei 1908 de 2018. Isso envolveu o monitoramento de perfis públicos em redes sociais e grupos de WhatsApp pelo Ministério Público, a fim de coletar informações que serviriam como evidência digital em processos de investigação subsequentes para a acusação de atos relacionados a protestos sociais em 2019 e 2021.[230]

De acordo com o relatório do Estado à CIDH, por ocasião de sua visita de trabalho à Colômbia em junho de 2021, houve 21.675 horas de "patrulhamento cibernético" desde o início das manifestações em 28 de abril até 8 de junho de 2021, sendo esta última a data de início da visita.[231] Nesse período, as autoridades colombianas identificaram pelo menos 154 notícias falsas e mais de 2.300 publicações contendo ameaças à vida ou à integridade física.[232]

Assim, de acordo com o relatório de junho da CIDH, o patrulhamento cibernético constitui um risco para as liberdades individuais, uma vez que: (a) "criminaliza expressões sobre funcionários públicos ou assuntos de interesse público", enquanto (b) tem um *"forte efeito inibidor sobre a disseminação de ideias, críticas e informações".*[233] *La CIDH também identificou o vínculo entre o Ministério da Defesa e a empresa Alotrópico S.A.S, relacionada à campanha #ColômbiaEsMiVerdad, por meio de um "serviço de posicionamento da 'marca' do Ministério da Defesa utilizando ferramentas de OSINT para atividades de marketing como análise de percepção, detecção de crises de imagem em redes sociais, identificação de atores importantes ou aliados nessa estratégia de comunicação".*[234]

---

229 Saavedra, A. M. (2021, 8 de noviembre). Colombiacheck e a campanha "Colômbia é a minha verdade". Colombiacheck. https://colômbiacheck.com/investigaciones/colômbiacheck-y-la-campana-colômbia-es-mi-verdad

230 A Fundação Karisma está prestes a publicar o relatório mencionado nesta seção.

231 CIDH. (2021). CIDH conclui visita de trabalho à Colômbia e apresenta suas observações e recomendações. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

232 Os relatórios sobre as ações monitoradas pelo PMU-Ciber foram compartilhados entre 22 de maio de 2021 e 2 de julho de 2021, por meio da conta X do Ministério da Defesa (@mindefensa). Eles foram precedidos por outras publicações sobre as atividades do PMU-Ciber em janeiro de 2020 e nos primeiros dias de maio de 2021. Da mesma forma, o Centro Cibernético Policial (CCP) publicou em junho de 2021 um balanço geral sobre a manifestação pública entre 28 de abril e 3 de junho de 2021. De acordo com essa instituição, durante esse período foram identificadas "93 notícias falsas (...) que iam contra [a] imagem institucional, [por meio de atividades de patrulhamento cibernético nas redes sociais]". Este reporte também foi compartilhado por meio de sua conta no X (@CaiVirtual).
Em 2 de julho de 2021, o Ministério da Defesa publicou o último relatório em sua conta no X, onde indicou ter identificado 157 notícias falsas; ou seja, três a mais do que as relatadas à CIDH.

233 Comissão Interamericana de Direitos Humanos (CIDH). (2021, 10 de junho). CIDH conclui visita de trabalho à Colômbia e apresenta suas observações e recomendações. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

234 Antes da greve nacional de 2021, quatro entidades estatais contrataram serviços de tecnologia com empresas fornecedoras de ferramentas para vigilância digital. A saber, DIJIN; o Comando Conjunto Cibernético da Polícia; o Exército Nacional, a Polícia Nacional; e FGN. Esses contratos foram assinados com três empresas privadas: a. Gamma Ingenieros SAS: GAMMA Ingenieros era distribuidora da 4IQ, uma empresa espanhola, agora chamada Constella Intelligence, que fornece ferramentas de inteligência baseadas em pesquisa em fontes abertas.
A contratação realizada em 2016 foi direta entre o Exército Nacional e a empresa, e o objeto do contrato foi a aquisição de equipamento de inteligência com ampliação de licença e arquitetura de hardware para o sistema de fontes abertas. O número do processo de contratação é 325-DIADQ-CADCO-CENACINTELIGENCIA-2016. https://gammaingenieros.com/ b. Deinteko SAS: Representante na Colômbia da empresa israelense Cibersixgill (anteriormente Sixgill). Esta empresa foi contratada por três das entidades acima mencionadas: (a) a DIJIN em 2019; (b) o Comando Conjunto Cibernético em 2020; e (c) a Procuradoria-Geral da Nação em 2022.

No contexto das mobilizações, a Procuradoria Geral da República (FGN) estabeleceu a Diretiva 002 de 2021, que permitiu à FGN realizar investigações sobre atos cometidos em protestos e processar por meio da aplicação do crime de terrorismo.[235] Isso é bastante alarmante, porque a Diretiva 002 de 2021 implicou uma mudança na "política criminal (...) que permitiu macroimputações, entendidas como acusações de crimes graves sobre atos de menor lesividade".

Ao estabelecer a possibilidade de aplicar o crime de terrorismo em investigações relacionadas ao National Strike, as investigações poderiam ser alinhadas com a narrativa do "ciberterrorismo" e as implicações que isso trouxe para os processos subsequentes. Além disso, o Estado utilizou alguns poderes estabelecidos na Lei 1908 de 2018 para coletar informações obtidas de grupos do WhatsApp ou páginas públicas de mídia social como evidência digital para futuras investigações relacionadas ao crime de terrorismo, que em anos anteriores não podia ser considerado aplicável em contextos de protestos (Diretiva 0008 de 2016).

De acordo com a investigação da Fundación Karisma, após as manifestações de 2021, com base nas informações fornecidas pelo FGN, pelo menos 538 pessoas foram identificadas como vinculadas a eventos ocorridos durante os protestos entre abril e julho de 2021. 259 delas são acusadas em diferentes cidades da Colômbia (Bogotá, Cali, Medellín, Pasto e Bucaramanga). De acordo com as informações coletadas, a FGN coletou informações durante o período de análise e as utilizou como prova digital para realizar condenações pelos crimes de conspiração para cometer um crime, terrorismo, violência contra funcionários públicos, dano agravado à propriedade de terceiros e obstrução de vias públicas que afetam a ordem pública.

Até o momento, não foi iniciada nenhuma investigação sobre possíveis abusos no uso dos recursos do PMU-Cyber. A única ação relacionada foi tomada pela nova Procuradora-Geral, Adriana Camargo, que emitiu uma nova Diretriz 0001 de 2024,[236] que revoga as diretrizes estabelecidas na Diretriz 0002 de 2021 e estabelece que o protesto social pacífico goza de proteção constitucional[237], e, portanto, não estará sujeito a processo ou sanção criminal. Além disso, estabelece novos critérios para a interpretação de atos criminosos ocorridos em protestos. Diferentemente da Diretiva 0002 de 2021, os parâmetros de interpretação para avaliação de casos de investigação por terrorismo seguem uma lógica de não criminalização do protesto.

235 Ver: https://cr00.epimg.net/descargables/2021/06/06/8e14ef349816167a499eadd80bbfe740.pdf

236 Ver: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=166137

237 A diretiva determina que esse tipo de ato "deve ser interpretado de acordo com o âmbito de proteção dos direitos fundamentais de liberdade de expressão, liberdade de reunião e manifestação pacífica, e somente aqueles que excedam o exercício legítimo desses direitos serão investigados e julgados de acordo com as regras substantivas e processuais penais".

V. Vigilância de pessoas por meio de sistemas de leitura de placas

Os leitores automáticos de placas são sistemas de câmeras de alta velocidade controlados por computador, instalados em postes, viaturas policiais, postes de iluminação ou outras estruturas, para registrar automaticamente as placas dos veículos, a localização, a data e a hora da captura.[238]

Essa medida de vigilância permite o registro, o armazenamento e a análise sistemática das placas dos carros que circulam em espaços públicos de forma massiva e indiscriminada. Supostamente, ela se destina a fins de segurança ou gerenciamento de tráfego. Entretanto, sua aplicação pode afetar direitos fundamentais, como o direito à privacidade, à circulação e à proteção de dados.

BRASIL

A Plataforma Integrada de Operações e Monitoramento de Segurança Pública *(Córtex)* é uma iniciativa do Ministério da Justiça e Segurança Pública (doravante denominado "MJSP") do Brasil, instituída oficialmente pela Portaria Nro. 218, de 29 de setembro de 2021. Essa plataforma é operada e gerenciada diretamente pela Secretaria de Operações Integradas (doravante denominada "SEOPI") do referido Ministério.

O *Cortex* está vinculado ao programa *Smart Sampa*, uma iniciativa da Prefeitura de São Paulo que integra câmeras de vigilância na cidade para *supostamente* melhorar a segurança pública. Não foram encontrados detalhes públicos sobre o envolvimento de desenvolvedores ou intermediários privados específicos na implementação ou gerenciamento da plataforma *Cortex* ou do programa *Smart Sampa*.

Sua implantação ocorreu principalmente durante o governo de Jair Bolsonaro (2019-2022), embora seu uso continue sob a administração de Luiz Inácio Lula da Silva (2023-atual). Durante o governo de Bolsonaro, o MJSP, por meio da SEOPI, foi responsável pela gestão e operação do *Córtex*.[239]

Relatórios indicam que, durante o governo de Jair Bolsonaro, o Ministério da Justiça optou por não auditar o sistema *Cortex*, o que levou a debates sobre o possível uso indevido da plataforma para monitorar alvos sem justificativa adequada.[240]

Em um artigo de 2020,[241] o The Intercept definia *Cortex* como uma:

> tecnologia de inteligência artificial que usa leituras de placas de milhares de câmeras de beira de estrada em rodovias, pontes, túneis, ruas e avenidas em todo o país para rastrear alvos em movimento em tempo real.

238 EFF. (s.f.). Leitores automáticos de matrículas (ALPR). Disponível em: https://sls.eff.org/es/technologies/lectores-automatizados-de-matriculas-alpr

239 A Seopi é um setor do MJSP que ganhou notoriedade em julho de 2020, quando veio à tona a existência de um dossiê de inteligência produzido pela secretaria contra policiais e professores ligados a movimentos antifascistas, que foi suspenso pelo STF após um julgamento. Em São Paulo, a iniciativa Smart Sampa, promovida pela Prefeitura Municipal, busca melhorar a segurança urbana por meio de tecnologias avançadas.

240 Freitas, C.; Valente, R.. Ministério da Justiça não quis auditar o uso do Córtex pelo governo Bolsonaro. Agência Pública, 12 oct. 2024. Disponível em: https://apublica.org/2024/10/cortex-mj-nao-quis-auditar-sistema-espiao-pelo-governo-bolsonaro/.

241 Rebello, A.. Da placa de carro ao CPF. The Intercept Brasil, 21 sep. 2021. Disponível em: https://www.intercept.com.br/2020/09/21/governo-vigilância-cortex/.

O *Cortex* é um sistema de monitoramento em massa que integra bancos de dados nacionais e municipais com tecnologias de reconhecimento de placas e, em alguns casos, reconhecimento facial. Ele não apenas monitora os veículos em tempo real por meio de câmeras instaladas nas estradas, identificando as placas e acompanhando seus trajetos, mas também é capaz de coletar e cruzar dados pessoais de mais de 160 bancos de dados, incluindo os da administração pública federal, como o Relatório Anual de Informações Sociais do Ministério da Economia, retendo os dados por um período de dez anos.

O sistema permite que cerca de 55 mil agentes, civis e militares, monitorem "alvos" sem a necessidade de justificativas específicas. De acordo com a Agência Pública,[242] em 2024 a plataforma recebeu imagens de 35,9 mil câmeras instaladas em rodovias, áreas urbanas, estádios de futebol e estradas federais. Operando 24 horas por dia, o sistema permite a vigilância contínua de pessoas e veículos.

Cortex foi objeto de um pedido de acesso à informação em 2024,[243] buscando saber quantas pessoas e veículos haviam sido monitorados. O MJSP negou a resposta, argumentando que a divulgação das informações poderia comprometer as investigações em andamento, mas confirmou que os "alvos" do *Córtex* podem ser monitorados indefinidamente, até que surjam indícios de acusação, devido à sua função de "ferramenta auxiliar de investigação". Em 2022, em resposta a uma solicitação semelhante, revelou que o sistema havia identificado até o momento aproximadamente 360.000 alvos e possibilitado a recaptura de mais de 20.000 pessoas.

Há também indicações de que municípios, governos estaduais e outros órgãos têm acesso irrestrito ao CORTEX, desde que ofereçam uma "contrapartida", ou seja, o compartilhamento de seus bancos de dados. Até março de 2023, o MJSP havia assinado 184 Acordos de Cooperação Técnica (ACTs) sob esse modelo.

Em 10 de janeiro de 2025, o governo federal assinou um acordo de cooperação com São Paulo, a cidade mais populosa do Brasil, para integrar as câmeras do *Smart Sampa* – que atualmente conta com mais de 20 mil câmeras inteligentes – à Plataforma *Cortex*.[244] Isso permite que as câmeras municipais equipadas com reconhecimento de placas de veículos acessem o banco de dados nacional sobre veículos roubados, emitindo alertas às autoridades competentes para que intervenham.

Um artigo da revista Crusoe sobre o assunto indicava que os policiais podem até mesmo identificar, em tempo real, se um veículo estava em uma determinada praia.[245] Em uma notícia mais recente, o mesmo meio de comunicação também revelou que o MJSP tem alimentado o *Córtex* com acesso aos registros dos alunos das redes municipais de ensino.[246]

Desde sua oficialização, a sociedade civil se mobilizou contra a plataforma *Córtex*. Em 2020, depois que o The Intercept publicou um artigo sobre o *Córtex*, a Coalizão pelos Direitos na Internet emitiu um comunicado acusando a plataforma de ser incompatível com os princípios que regem a proteção de dados pessoais e um instrumento para o exercício do autoritarismo, algo inaceitável em um Estado democrático de direitos.[247]

---

242 Valente, R.; Freitas, C.. Programa de vigilância do MJ permite a 55 mil agentes seguir "alvos" sem justificativa. Agência Pública, 9 oct. 2024. Disponível em: https://apublica.org/2024/10/vigilância-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/#_.

243 Através da Agência Pública, por meio da Lei de Acesso à Informação (LAI).

244 Cidade de São Paulo. Câmeras do Smart Sampa começam a ler placas para identificar veículos roubados. Notícias, 10 jan. 2025. Disponível em: https://capital.sp.gov.br/w/c%C3%A2meras-do-smart-sampa-come%C3%A7am-a-ler-placas-para-identificar-ve%C3%ADculos-roubados-%C2%A0%C2%A0.

245 BIG brother federal. Crusoe. 21 jan. 2022. Disponível em: https://crusoe.com.br/edicoes/195/big-brother-federal/.

246 Valente, R.; Freitas, C.. Inteligência do Ministério da Justiça tem acesso a cadastros de alunos, revelam documentos. Agência Pública, 3 feb. 2025. Disponível em: https://apublica.org/2025/02/cortex-ministerio-da-justica-monitora-ate-dados-de-alunos-e-pais/.

247 Coalizão pelos Direitos na Internet. Sistema Córtex, do governo federal, ameaça direitos dos cidadãos. Coalizão pelos Direitos na Internet, 1 out. 2020. Disponível em: https://direitosnarede.org.br/2020/10/01/sistema-cortex-do-governo-federal-ameaca-direitos-dos-cidadaos/.

Em 2022, as ONGs Data Privacy Brasil, Conectas, Transparência Internacional e Artigo 19 apresentaram uma denúncia ao Ministério Público Federal argumentando que o *Córtex* permitia o acesso e o compartilhamento de dados pessoais e sensíveis sem uma governança eficaz, o que abriria margem para abusos e monitoramento ilegal sem prestação de contas.[248]

A denúncia apontava que se trata de um "panóptico virtual" e da insuficiência do marco normativo que regula o *Cortex*, indicando que a Portaria 218/2021 não ajuda a compreender o alcance do sistema e, menos ainda, a entender as garantias relacionadas ao seu uso - indicando que, por exemplo, a Portaria permite tomar decisões ad hoc sobre quem deve ser incluído no cerco eletrônico e não estipula critérios básicos de devido processo e investigação contínua, baseada em provas e razões legítimas de tal violação dos direitos fundamentais, para que uma pessoa seja constantemente vigiada pelo *Cortex*. Na denúncia, as ONGs exigem informações sobre o sistema, bem como a abertura de uma investigação civil e a realização das diligências necessárias para esclarecer o exposto. Em janeiro de 2025, no entanto, o MPF decidiu arquivar a investigação, argumentando que não foram encontradas evidências de irregularidades que justificassem a a continuidade do processo - a plataforma funcionava dentro de um marco normativo e contava com mecanismos internos de auditoria e controle de acesos.

Artigos jornalísticos alertando sobre os riscos e a opacidade do sistema também foram publicados pela Agência Pública e pela revista Crusoé.[249] Em 2024, uma nova carta aberta da Coalizão afirmou que "o sistema *Córtex* e sua gestão atual representam uma violação sistemática da proteção de dados pessoais".[250]

248 Ver: https://www.telesintese.com.br/wp-content/uploads/2022/02/representacao-controle-externo-da-atividade-policial.pdf.

249 Valente, R.; Freitas, C.. Programa de vigilância do MJ permite a 55 mil agentes seguir "alvos" sem justificativa. Agência Pública, 9 oct. 2024. Disponível em: https://apublica.org/2024/10/vigilância-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/#_.; e Crusoé. Big Brother Federal. Crusoé, 21 jan. 2022. Disponível em: https://crusoe.com.br/edicoes/195/big-brother-federal/.

250 Coalizão pelos Direitos na Internet. Posicionamento da Coalizão Direitos na Rede e entidades parceiras sobre o sistema CÓRTEX do Ministério da Justiça e Segurança Pública. Coalizão pelos Direitos na Internet, 8 nov. 2024. Disponível em: https://direitosnarede.org.br/2024/11/08/posicionamento-cdr-entidades-parceiras-sistema-cortex-do-mj/.

Resumo

Os casos documentados neste capítulo ilustram a preocupante tendência crescente no uso de tecnologias para impedir a defesa dos direitos humanos e o jornalismo investigativo; para atacar, censurar, reprimir e perseguir pessoas que revelam informações de interesse público (particularmente aquelas historicamente excluídas); e para preservar a falta de prestação de contas em contextos latino-americanos com um legado de repressão, impunidade e constantes violações dos direitos humanos.

Por exemplo, no **Chile**, foi revelado o monitoramento ilegal de líderes sociais, defensores dos direitos humanos e sindicatos pela polícia. Da mesma forma, a Promotoria Metropolitana Ocidental do Chile solicitou aos provedores de serviços de internet acesso a dados pessoais sensíveis no contexto de uma explosão social e política. Na **Colômbia**, no que diz respeito à patrulha cibernética e em decorrência das diversas manifestações públicas contra o governo do presidente Duque, a PMU-Ciber realizou um monitoramento das redes sociais, violando assim os direitos de acesso à informação e liberdade de expressão de milhões de pessoas. Da mesma forma, a FLIP documentou e identificou um total de 52 casos de jornalistas vigiados ilegalmente pelo Exército Nacional até junho de 2020 por meio de um software de rastreamento informático, realizando perfis ilegais de mais de 130 pessoas.

No **México**, foram documentados tanto o acesso ilegal a dados mantidos por empresas de telecomunicações para vigiar jornalistas, especialistas e ativistas sociais, quanto o uso de *spywares* contra jornalistas e defensores dos direitos humanos que denunciam atos de corrupção e violações dos direitos humanos cometidos pelo Estado, principalmente pelo Exército mexicano. Na mesma linha, em **El Salvador** também foi documentado o uso do *Pegasus* contra jornalistas e membros da sociedade civil. No **Paraguai**, foi documentada a aquisição do software espião *FinFisher* e os vazamentos do *Wikileaks* revelaram a aquisição de equipamentos de escuta telefônica pelo Ministério do Interior.

Além disso, a maioria dessas medidas de vigilância foi realizada de forma **ilegal**, pois foram implementadas sem cumprir os princípios de legalidade, adequação, necessidade e proporcionalidade, bem como sem as garantias adequadas, refletindo abusos, falta de transparência e impunidade. Em todos os casos, foram identificadas violações de direitos humanos fundamentais, como privacidade, proteção de dados pessoais, liberdade de expressão e associação, em contextos em que as pessoas mais afetadas têm perfis relacionados ao exercício do jornalismo, ativismo, movimentos sociais e oposição política.

Por outro lado, os casos documentados também refletem uma tendência estadual e regional de fortalecimento da vigilância maciça e indiscriminada, como foram os casos identificados de intervenção em comunicações privadas na **Colômbia**, **Chile** e **Peru**, bem como o acesso aos registros de dados conservados de todos os usuários de telefonia móvel no **Paraguai**, **Chile** e **México**, afetando assim diferentes liberdades da maioria da população, incluindo nosso direito à presunção de inocência, princípio de não discriminação e autodeterminação.

Nessa linha, foram identificados padrões preocupantes não apenas de colaboração entre empresas de telecomunicações e órgãos estatais em atividades de vigilância de comunicações privadas, mas também de geolocalização baseada na exploração de vulnerabilidades na infraestrutura de telecomunicações (SS7) e de monitoramento de redes públicas.

O caso do **Brasil** exemplifica como a ABIN utilizou ilegalmente ferramentas de geolocalização de dispositivos eletrônicos durante o governo Bolsonaro, sendo o principal *spyware* o *FirstMile*. No **Peru**, o governo de Ollanta Humala implementou um sistema de vigilância em massa que permitia a interceptação de comunicações e a geolocalização de milhares de pessoas, mesmo fora do país.

O caso brasileiro também ilustra a vigilância de pessoas por meio de sistemas de leitura de placas de veículos, que permitem o registro, armazenamento e análise sistemática de placas de veículos que circulam em espaços públicos de forma massiva e indiscriminada. Esses casos evidenciam o uso ilegal de medidas de vigilância por parte dos Estados em colaboração com atores privados, violando, por sua vez, direitos humanos fundamentais.

Por fim, os casos de obtenção de informações detectados na região com ferramentas forenses de obtenção, como o caso do México com a aquisição de ferramentas desenvolvidas pela **Cellebrite** e as evidências do uso do **Septier** no Paraguai, demonstram a falta de transparência no uso dessas ferramentas pelas autoridades estatais.

CAPÍTULO QUATRO: DIAGNÓSTICO

A evolução tecnológica permitiu o uso de um amplo espectro de medidas de vigilância na região, cada vez mais avançadas e invasivas, sem uma regulamentação adequada.

A tais avanços para que cumpram as normas internacionais em matéria de direitos humanos previstas no Capítulo Dois.

Nesse sentido, a partir de uma análise comparativa da regulamentação relativa à vigilância das comunicações, identificamos uma deficiência normativa recorrente no que diz respeito às leis que estabelecem de forma precisa, detalhada e clara as autoridades, os procedimentos e as circunstâncias em que se pode recorrer a medidas de vigilância.

I. Requisitos de procedência material

As circunstâncias ou procedimentos para poder fazer uso de medidas de vigilância das comunicações variam significativamente entre os países da região, mas coincidem no fato de que, na maioria dos casos, são previstos de forma ampla, ambígua e/ou vaga, deixando os cidadãos em um estado de indefesa que fomenta a discricionariedade e os abusos na prática. Isso é exemplificado pelas deficiências legais no Brasil, na Colômbia, no México e no Peru.

No caso do **Brasil**, a Lei Nro. 9.883/1999 cria a ABIN e tem por objetivo estabelecer "o Sistema Brasileiro de Inteligência, que integra as ações de planejamento e execução das atividades de inteligência do país, com o objetivo de prestar apoio ao Presidente da República em assuntos de interesse nacional".[251]

As preocupações relacionadas à vigilância estatal estão, em grande parte, dentro do âmbito da Inteligência Brasileira.[252] A lei que regula a ABIN define competências excessivamente amplas, o que gera preocupações sobre seus limites. Por exemplo, o artigo 4º estabelece atribuições genéricas, como a coleta e análise de dados confidenciais para assessorar o presidente da República; a proteção de informações sensíveis relacionadas à segurança do Estado e da sociedade; e a avaliação de ameaças internas e externas à ordem constitucional. Essa amplitude deixa margem para interpretações extensivas, criando um cenário semelhante ao da antiga Lei de Segurança Nacional,[253] que, durante a ditadura militar, foi usada para justificar abusos.

Na **Colômbia**, a Corte Interamericana de Direitos Humanos, no caso *Membros da Corporação Coletivo de Advogados "José Alvear Restrepo" vs. Colômbia*, reconheceu a responsabilidade do Estado em abusos da função de inteligência e ordenou a reforma da Lei 1621 de 2013 – que regula as atividades de inteligência e contra-inteligência–[254] para incluir garantias como os princípios da legalidade e do devido processo legal, bem como a necessidade de controle judicial. Atualmente, foi apresentado ao Congresso um projeto de lei de reforma que propõe mudanças substanciais à lei para cumprir a decisão da Corte Interamericana de Direitos Humanos.

---

251 Ver: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm#art21

252 Escola de Ativismo. (2024). Tecno-autoritarismo: o que a "Abin paralela" nos diz sobre mecanismos de vigilância e democracia? https://escoladeativismo.org.br/tecnoautoritarismo-o-que-a-abin-paralela-nos-diz-sobre-mecanismos-de-vigilância-e-democracia/) Nota: A ABIN carrega uma herança estrutural e operacional (do Serviço Nacional de Informações (SNI), órgão da ditadura responsável pela vigilância e repressão de militantes, ativistas, partidos políticos, sindicatos, meios de comunicação e outros setores da sociedade. (https://oglobo.globo.com/politica/noticia/2024/02/04/quais-sao-os-limites-maior-escandalo-da-abin-reabre-discussao-sobre-as-atividades-de-inteligencia.ghtml).

253 Ibidem.

254 Incluindo o monitoramento do espectro eletromagnético e as interceptações de comunicações privadas.

No que diz respeito ao **México**, a clareza e a precisão dos requisitos de procedência material para realizar medidas de vigilância são variáveis no âmbito jurídico mexicano. Por exemplo, o CNPP[255] estabelece que a procedência do pedido de autorização para a intervenção em comunicações privadas, o acesso a dados conservados ou a geolocalização em tempo real requer apenas que o titular do Ministério Público "considere necessária" a intervenção no âmbito de um inquérito em que se investiga a prática de um delito.

A constatação da necessidade das medidas deve ser avaliada pelo juiz federal competente com base em indícios objetivos apresentados pela autoridade que solicita a autorização. No entanto, a redação difere excessivamente da própria autoridade para justificar a pertinência de uma medida de vigilância.

Quanto ao **Peru**, o Decreto Legislativo Nro. 1141 – que regula o funcionamento da Direção Nacional de Inteligência (DINI) e do Sistema Nacional de Inteligência (SINA) – embora estabeleça que as atividades de inteligência devem ser desenvolvidas com respeito aos direitos humanos, contempla limites muito vagos e carece de mecanismos eficazes de controle e supervisão externa, o que permite amplas margens para abusos.

Da mesma forma, o Decreto Legislativo Nro. 1182 (conhecido como Lei *Stalker*) obriga as operadoras a conservar dados massivos de tráfego e localização de todos os usuários por três anos, sem critérios razoáveis de proporcionalidade ou necessidade. Além disso, reformas recentes ampliaram os casos em que a polícia pode solicitar esses dados, enfraquecendo ainda mais as garantias judiciais e o controle cidadão.[256]

Em muitos casos, a autorização para acessar as informações é concedida por um funcionário hierarquicamente superior dentro da mesma entidade que faz a solicitação. Essa dinâmica ocorre em países como Brasil (com a ABIN e a polícia), México (por meio da LGN), Peru (por meio da PNP e da OSIPTEL) e Colômbia (com as Forças Armadas, a Polícia Nacional e a Direção Nacional de Inteligência). Essa concentração de funções tem gerado preocupações, uma vez que não existe independência entre aqueles que investigam e aqueles que devem autorizar tais medidas, o que pode resultar em abusos ou falta de controle externo.

Consequentemente, os marcos legais devem prever uma instituição civil independente dos serviços de inteligência e do Poder Executivo, com conhecimentos técnicos, para poder fiscalizar e responsabilizar as autoridades competentes, tanto em relação às suas obrigações de transparência como em termos de prestação de contas.

II. Controle Judicial

Como mencionado no primeiro e no segundo capítulo, a autorização judicial de medidas de vigilância é uma garantia fundamental para a prevenção de abusos, arbitrariedades e discricionariedade por parte das autoridades. Por isso, são particularmente preocupantes as legislações do **Paraguai** e do **Peru**, que não estabelecem o requisito de controle judicial prévio.

Com base no Decreto Legislativo Nro. 1182, conhecido como "Lei *Stalker*", o **Peru** autoriza, em casos de suspeita de flagrante delito, a Polícia Nacional a acessar dados de geolocalização em tempo real sem ordem judicial prévia.

---

255 Artigo 291.

256 É conhecido pelo menos um litígio relevante relacionado com esta norma: uma ação judicial para obter acesso ao protocolo interno da PNP sobre como se solicita e processa a geolocalização sem mandado judicial. Resultado: o pedido foi negado e o protocolo permanece confidencial, o que reflete a falta de transparência, a opacidade institucional e a ausência de controle democrático sobre esta forma de vigilância.

Por outro lado, mesmo que a legislação dos países da região estabeleça a necessidade de um controle judicial prévio, foram levantados desafios importantes com a previsão de mecanismos excepcionais, como é o caso do **Brasil**, **México** e **Paraguai**.

Assim, apesar de o **Brasil** exigir autorização judicial tanto para a obtenção de metadados quanto de informações de geolocalização,[257] também prevê que, se o tribunal não se pronunciar em um prazo de 12 horas, o Ministério Público ou um agente da polícia podem solicitar os dados diretamente às empresas de telecomunicações e telemática.

Da mesma forma, a ABIN – principal entidade estatal autorizada a realizar atividades de vigilância para fins de inteligência – não tem prerrogativa para realizar intervenção nas comunicações sem autorização judicial. No entanto, ela pode acessar informações obtidas por outros órgãos do Sisbin[258] por meio de mecanismos de cooperação estabelecidos na legislação vigente.

No **México**, embora o artigo 16 da Constituição estabeleça a necessidade de obter uma autorização judicial federal para realizar a interceptação de comunicações privadas, o mecanismo excepcional estabelecido no artigo 303 do CNPP autoriza os ministérios públicos a solicitar o acesso a dados conservados ou a geolocalização em tempo real a empresas de telecomunicações sem obter previamente uma autorização judicial, mas com a obrigação de solicitar a ratificação da medida dentro de 48 horas após a solicitação original.

Isso fez com que a exceção se tornasse a regra geral e que um número significativo de solicitações feitas sob o mecanismo excepcional não fossem ratificadas pela autoridade judicial federal — ou nem mesmo fossem submetidas a tal ratificação —, permitindo assim que as autoridades invadissem a privacidade dos usuários de telecomunicações ilegalmente e com impunidade, sem que a pessoa afetada ou um juiz tivessem conhecimento disso.

No **Paraguai**, embora o artigo 200 do Código de Processo Penal estabeleça que a interceptação de comunicações requer uma decisão fundamentada do juiz, o artigo 228 outorga tanto ao juiz quanto ao Ministério Público a faculdade de solicitar relatórios a pessoas ou entidades públicas ou privadas. Esses relatórios podem ser solicitados verbalmente ou por escrito, especificando o procedimento correspondente, o nome do imputado, o local de entrega, o prazo para sua apresentação e as consequências em caso de descumprimento. Dessa forma, é permitido o acesso a dados mantidos por empresas de telecomunicações sem a necessidade de autorização judicial.

III: Proliferação de tecnologias de vigilância em massa

Com base nos princípios da necessidade e da proporcionalidade, as medidas de vigilância só podem ser consideradas legítimas se constituírem a alternativa menos prejudicial disponível para alcançar um objetivo legítimo e se, após uma ponderação, os efeitos sobre a privacidade e a segurança não forem exagerados ou desproporcionais em relação às vantagens obtidas com a vigilância proposta.

A crescente proliferação de equipamentos e sistemas de vigilância, como antenas falsas ou *spyware*, que além de serem operados de forma autônoma, sem necessidade de colaboração de qualquer entidade e possuem amplas capacidades intrusivas, contêm medidas para dificultar sua detecção, é indicativa da pouca clareza e precisão sobre os métodos de vigilância que podem ser considerados compatíveis com as normas de direitos humanos reconhecidas nas constituições dos países da região.

---

257 De acordo com o artigo 10, § 1 do Marco Civil da Internet (Lei nº 12.965/2014) e o artigo 13-B do Código de Processo Penal.

258 A ABIN faz parte do Sistema Brasileiro de Inteligência (Sisbin), que integra diversos órgãos da administração pública federal responsáveis pela produção de informações relevantes para as atividades de inteligência. O funcionamento do SISBIN é regulamentado pela Lei nº 9.883/99 e pelo Decreto nº 11.693/23.

O problema se agrava quando não só existe uma ausência de regulamentação dessas novas tecnologias, mas também uma tendência por parte de alguns países da região de legitimar medidas de vigilância massiva e indiscriminada que são incompatíveis com os padrões internacionais em matéria de direitos humanos.

Por exemplo, no **Chile**, gera preocupações a recente aprovação da Lei Antiterrorismo N.º 21.732, de fevereiro de 2025, que habilita o uso de tecnologias como os *IMSI Catchers* e tem como objetivo "determinar, registrar e monitorar" dados que permitam "singularizar ou identificar um ou mais dispositivos" ou facilitar sua geolocalização.[259]

Entre os riscos identificados no uso desse tipo de tecnologia de vigilância em massa, destaca-se que se trata não apenas de uma tecnologia de vigilância indiscriminada, mas também extremamente desproporcional, na medida em que captura o sinal de todos os dispositivos próximos à antena falsa, impactando assim a privacidade de terceiros que não estão de forma alguma relacionados com a investigação criminal em curso e que, em contrapartida, legitima na prática a chamada *"pesca milagrosa"*.

Por sua vez, na **Colômbia**, o artigo 15 da Resolução 5839 de 2015 da Polícia Nacional estabelece as funções do Centro Cibernético Policial, entre as quais se inclui, no ponto 12, a "realiza[ção] de patrulhamento cibernético 24 horas por dia, 7 dias por semana, na web, com o objetivo de identificar ameaças de e para a detecção de fatores comuns em incidentes de seu conhecimento, bem como a violação da disponibilidade, integridade e confidencialidade das informações que circulam no ciberespaço".

Na mesma toada, no **México**, o artigo 9, seção XXXVII, da Lei da Guarda Nacional autoriza essa instituição militarizada a realizar *"ações de vigilância, identificação, monitoramento e rastreamento na rede pública da Internet em sites, com o objetivo de prevenir condutas criminosas"*. A imprecisão com que essa faculdade é descrita não permite determinar claramente seu alcance. No entanto, pode-se entender que tal faculdade visa fundamentar a investigação de fontes abertas e a formulação de perfis sobre usuários da Internet.

IV. Falta de transparência e corrupção na aquisição de tecnologias de vigilância

Em nível global e na região, os processos de contratação de equipamentos e sistemas para a vigilância das comunicações têm se destacado pela opacidade, discricionariedade e pela ausência de regulamentação e controles adequados para inibir a corrupção, a vigilância ilegal e a impunidade.

Por exemplo, no **Paraguai**, a Fundação Parque Tecnológico de Itaipu (PTI) continua com uma licitação controversa realizada em abril de 2015 para equipamentos de espionagem avaliados em 12 milhões de dólares, denunciada por irregularidades pelo deputado Mauricio Espínola.[260] Entre as empresas licitantes estão a ITTI Saeca e a Technoma, ambas ligadas ao Grupo Vázquez e ao presidente Santiago Peña, bem como a TSV SRL, empresa com histórico de conluio e favorecida em vários contratos estatais[261].

259 Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1211036

260 Última Hora (2025) Duas empresas ligadas a Peña, uma delas com antecedentes, concorrem na PTI Disponível em: https://www.ultimahora.com/dos-firmas-ligadas-a-pena-y-una-con-antecedentes-compiten-en-pti

261 ABC Color (2025) Abertura dos envelopes com as propostas da licitação de aparelhos de escuta no PTI. Disponível: https://www.abc.com.py/este/2025/04/11/postergan-apertura-de-sobres-de-ofertas-en-licitacion-de-aparatos-de-escucha-en-el-pti-en-la-que-compiten-firmas-ligadas-al-presidente-santiago-pena/

A licitação contempla uma plataforma de espionagem integral que inclui tecnologias como sistemas de interceptação legal de comunicações *(Lawful Interception)*, captadores *IMSI Catcher* para rastreamento de dispositivos móveis, kits de análise forense digital (como *Cellebrite* ou similares), software de reconhecimento facial, ferramentas OSINT para monitoramento de redes sociais e fontes abertas, equipamentos de geolocalização por satélite *(GPS Trackers)* e tecnologia de vigilância acústica. De acordo com mais de 130 protestos, as especificações técnicas dos equipamentos teriam sido projetadas para favorecer exclusivamente a empresa ITTI Saeca.

No **Brasil**, diante do vazio regulatório, a Procuradoria-Geral da República (PGR) apresentou, em dezembro de 2023, a Ação Direta de Inconstitucionalidade por Omissão Nro. 84 perante o Supremo Tribunal Federal (STF), convertida na Arguição de Incumprimento de Preceito Fundamental Nro. 1.143.[262]

A ação questiona a possível falta de legislação sobre a compra e o uso de tecnologias de espionagem e solicita ao STF que: *(i)* reconheça a omissão do Congresso na regulamentação do uso de *spyware*; *(ii)* estabeleça um prazo para sua regulamentação; e *(iii)* implementem-se medidas provisórias para garantir a proteção da privacidade e o sigilo dos dados. O caso ainda está em andamento.

Na mesma linha, em 2024, o ministro relator Cristiano Zanin, do Supremo Tribunal Federal, convocou uma audiência pública sobre a ADPF 1.143, com a participação de 33 entidades da sociedade civil para contribuir para o debate sobre a compra e o uso dessas tecnologias de vigilância. O InternetLab, juntamente com a Data Privacy Brasil, participou da audiência pública como *amicus curiae* e apresentou seus argumentos.[263] Da mesma forma, destacaram que a ausência de regulamentação sobre essas ferramentas compromete a confiança pública nas instituições democráticas, pois abre espaço para abusos de poder.

No **México**, por meio de solicitações de acesso à informação, jornalismo investigativo e vazamentos de informação, foram identificadas as principais irregularidades em relação aos processos de contratação de equipamentos e sistemas para vigilância: *(a)* a discricionariedade e a adjudicação a empresas com irregularidades (em processos de adjudicação direta com empresas sem antecedentes ou experiência na matéria); *(b)* sobrepreços na aquisição (valores exorbitantes e condições irracionais); *(c)* contratações que pretendem ser ocultadas ou ofuscadas a partir de descrições vagas do objeto das contratações; *(d)* ausência de controles para evitar a aquisição ilegal de tecnologias de vigilância; e *(e)* ausência de documentação sobre a aquisição e uso de equipamentos e sistemas de vigilância.

Portanto, é essencial que sejam exigidos na região procedimentos ou autorizações especiais que não envolvam apenas a autoridade e as empresas contratantes.

262 Ver: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814

263 InternetLab. (2024). Uso de tecnologias espiãs: InternetLab e DataPrivacy Brasil contribuem como amicus curiae e participam de audiência pública em caso no STF. InternetLab. https://internetlab.org.br/pt/noticias/uso-de-tecnologias-espias-internetlab-e-dataprivacy-brasil-contribuem-como-amicus-curiae-e-participam-de-audiencia-publica-em-caso-no-stf/

CONCLUSÕES

Os casos mencionados no Capítulo Três representam apenas uma pequena amostra de um histórico de abusos de vigilância por parte dos países latino-americanos, seja na forma de coleta massiva e indiscriminada de nossos dados pessoais sensíveis, patrulhamento cibernético, uso de *spywares* contra a sociedade civil, bem como muitos outros abusos denunciados.

Essa prática gera um **desmantelamento do espaço cívico**, especialmente o digital, impactando nossas liberdades e autonomia. Por exemplo, o caso da Colômbia é representativo da maneira como as agências de segurança pública e inteligência contratam serviços privados para o perfilamento e monitoramento de milhões de pessoas em plataformas digitais, sob a desculpa de prevenção e investigação de crimes, mas com o objetivo de coletar informações para fins de controle e repressão de expressões críticas ao governo, bem como a disseminação de desinformação. Esses contextos geram um clima de desconfiança digital que restringe a expressão, uma vez que as pessoas se autocensuram ou limitam sua participação digital.

Da mesma forma, tornou-se normal **utilizar medidas intrusivas de vigilância estatal** (em teoria excepcionais) com retórica populista de que "não temos nada a esconder" para controlar, censurar e reprimir os cidadãos. O caso do Brasil é emblemático no que diz respeito ao uso de sistemas de geolocalização, tanto através da exploração do SS7 como através de sistemas de identificação de matrículas, visualizando a intensidade com que se pode afetar a privacidade e a liberdade de movimento de milhões de pessoas, traçando perfis exaustivos com base nos deslocamentos e rotinas em termos de movimentos das mesmas, incluindo jornalistas, ativistas, funcionários públicos e pessoas associadas a investigações criminais contra familiares do então presidente Bolsonaro.

Ao prejudicar atividades como o jornalismo, a defesa dos direitos humanos ou a integridade das instituições democráticas, **a vigilância ilegal frequentemente afeta a sociedade e suas aspirações democráticas,** permitindo que quem vigia com impunidade exerça um controle e influência indevida sobre a sociedade e suas instituições. O caso de El Salvador é um exemplo claro de como a vigilância de jornalistas compromete suas fontes, colocando em risco a revelação de sua identidade e até mesmo sua segurança física. No México, por sua vez, há evidências abundantes do uso ilegal reiterado de ferramentas de vigilância de comunicações contra jornalistas, defensores dos direitos humanos, ativistas e oposicionistas políticos.

Além disso, é crucial perceber que a vigilância ilegal costuma estar associada a outras formas de intimidação, desde ataques à reputação, extorsão, invasões, infiltração ou operações psicológicas até potencializar ou facilitar agressões físicas, incluindo homicídio.

RECOMENDAÇÕES AOS ESTADOS

Para evitar insegurança jurídica e discricionariedade na implantação de medidas de vigilância, as estruturas jurídicas precisam estabelecer com mais precisão aspectos fundamentais, como a identificação das autoridades competentes. Além disso, os parâmetros e limites materiais que devem informar os pedidos de autorização de medidas de vigilância e as decisões judiciais que resolvem esses pedidos devem ser delimitados com mais precisão, a fim de garantir maior previsibilidade sobre o escopo dessas medidas.

As regras que regulamentam a vigilância nas estruturas jurídicas regionais foram projetadas tendo em mente tecnologias de escuta telefônica e outras formas de vigilância direcionada, exigindo a colaboração de partes privadas, especialmente empresas de telecomunicações. Dessa forma, os métodos tradicionais de vigilância de comunicações forneciam consideravelmente menos informações sobre as pessoas sob vigilância e inevitavelmente produziam testemunhas, como as empresas de telecomunicações.

No entanto, a proliferação e o uso diário de tecnologias de vigilância em massa cada vez mais sofisticadas e invasivas indicam que as estruturas jurídicas regionais atuais não foram capazes de garantir seu uso racional ou mesmo a possibilidade de que tais tecnologias possam ser compatíveis com os princípios de necessidade e proporcionalidade previstos no Capítulo Um.

Consequentemente, exigimos vontade política do Estado para cumprir os princípios de legalidade, necessidade e proporcionalidade, de acordo com os padrões internacionais de direitos humanos para vigilância de comunicações, exigindo que todas as estruturas jurídicas nacionais contemplem:

- **Leis com definições claras, precisas e detalhadas** das autoridades com poderes, do procedimento e das circunstâncias sob as quais as medidas de vigilância podem ser executadas, bem como um registro e controle da implementação das medidas de vigilância do Estado.

De acordo com os princípios de legalidade, propósito legítimo, necessidade e proporcionalidade mencionados no Capítulo Um, é necessário que haja clareza suficiente para inibir abusos na aquisição e no uso de tais tecnologias de vigilância, quando elas são direcionadas a indivíduos específicos e circunscritas a circunstâncias em que há indícios ou causas prováveis do cometimento de um crime ou de uma ameaça à segurança nacional.

- **Regulamentação eficaz dos processos de aquisição** de equipamentos e sistemas de vigilância de comunicações, com registro e controle dos mesmos.
- Medidas de **transparência**, uma vez que, embora a vigilância de comunicações esteja frequentemente relacionada à investigação de crimes e ameaças à segurança nacional, para os quais algum sigilo é necessário para sua eficácia, a transparência é essencial para prevenir e detectar abusos, bem como avaliar, com base em evidências, se os objetivos de interesse público que são frequentemente citados para justificar a vigilância das comunicações são alcançados ou se, na implantação de tais medidas, há atos de corrupção ou controles inadequados contra possíveis abusos.

O fato de muitas dessas tecnologias serem usadas de forma autônoma pela autoridade agressora, somado às suas características anti-forenses e anti-detecção, implica um enorme desafio para impedir seu uso ilegal. Portanto, o estabelecimento de obrigações de publicação de relatórios estatísticos, com informações desagregadas sobre seu uso, é particularmente relevante para prevenir, detectar e corrigir abusos cometidos pela vigilância ilegal de comunicações.

- Previsão de **garantias**, como revisão judicial, supervisão independente e direito de notificação.

Nesse contexto, ações como a do Brasil, em que organizações da sociedade civil solicitaram, durante a audiência pública da ADPF 1.143, que, caso o STF não declare a inconstitucionalidade total do uso de *spyware* por órgãos públicos, sejam estabelecidas regras rígidas para evitar seu abuso. Defenderam também a exigência de autorização judicial prévia para qualquer monitoramento; a restrição do uso de *spyware* apenas quando não houver outros meios de investigação disponíveis; a proteção do sigilo das comunicações; e a implementação de mecanismos que garantam a rastreabilidade da cadeia de custódia dos dados interceptados.

Nos países latino-americanos, com um legado de autoritarismo e repressão à dissidência, devemos mudar as narrativas e a percepção pública para um entendimento compartilhado em que equiparamos nossa privacidade à nossa segurança, pois a vigilância descontrolada por parte das autoridades latino-americanas, atormentadas por contextos de impunidade e corrupção, implica apenas maior controle para inibir críticas ao governo e gerar medo, em vez de proporcionar maior segurança à população.

AlSur

www.alsur.lat