Excelentíssimo Senhor Ministro Cristiano Zanin do Egrégio Supremo Tribunal Federal

Arguição de Descumprimento de Preceito Fundamental n. 1143

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA ("InternetLab"), e ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA ("Data Privacy Brasil"), já qualificadas nos autos em epígrafe, vêm, respeitosamente, à presença de Vossa Excelência, por seus advogados devidamente constituídos, com fundamento no artigo 138 do Código de Processo Civil, apresentar a sua contribuição como *amici curiae*, pelos argumentos a seguir expostos.

Sumário

I. DO OBJETO DA AÇÃO

1. Trata-se de Arguição de Descumprimento de Preceito Fundamental proposta pela D. Procuradoria-Geral da República, com o escopo de evitar e reparar violações de preceitos fundamentais pelo Poder Público. Tais violações são representadas pela omissão parcial na regulação do uso, assim como pelas aquisições e usos indiscriminados, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal.

2. Com efeito, a presente ação— inicialmente proposta como Ação Direta de Inconstitucionalidade por Omissão n. 84 e convertida para a Arguição de Descumprimento de Preceito Fundamental n. 1143 —, visa a dar efetividade plena e conferir proteção eficaz aos mandamentos contidos no art. 5º, X, XII e LXXIX, da Constituição Federal[1], tendo em vista os recentes avanços tecnológicos, que culminaram na proliferação global de ferramentas de intrusão virtual. Tais ferramentas têm sido utilizadas no âmbito de serviços de inteligência, de órgãos de repressão estatais e de defesa nacional, para a vigilância remota, secreta e invasiva de dispositivos móveis de comunicação digital, sob o pretexto do combate ao terrorismo e ao crime organizado.

3. Em suma, a inicial da D. PGR almeja corrigir a insuficiência do ordenamento jurídico pátrio em conferir proteção adequada à garantia da inviolabilidade da vida privada, da intimidade e do sigilo de comunicações e dados pessoais em aparelhos digitais de comunicação pessoal, diante das novas ferramentas e sistemas de infiltração e de intrusão virtual remota, utilizados por órgãos e agentes públicos no curso de investigações e em atividades de inteligência.

4. Para tanto, postulava que esta E. Corte (i) declare a inconstitucionalidade da omissão parcial do Congresso Nacional em tornar plenamente efetivos os

[1] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

mandamentos de proteção da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da CF, por meio da regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares; (ii) fixe prazo razoável para que o Congresso Nacional supra a mora legislativa; e (iii) estabeleça balizas provisórias à salvaguarda dos direitos fundamentais à intimidade e à privacidade, e à inviolabilidade do sigilo das comunicações pessoais e de dados, até que seja sanada a lacuna normativa inconstitucional.

5. Nesse cenário, o InternetLab e a Data Privacy Brasil requereram o seu ingresso como *amici curiae* na presente ADPF n. 1143, então ADO n. 84, a fim de que possam contribuir com o debate constitucional em voga, trazendo elementos jurídicos, teóricos e técnicos capazes de oferecer subsídios para a decisão a ser tomada por esta Suprema Corte.

6. Em 16.04.2024, o Exmo. Ministro Relator Cristiano Zanin admitiu o InternetLab e a Data Privacy Brasil como *amici curiae*, considerado a pertinência entre as finalidades institucionais das entidades e o objeto da ação. Além disso, o Exmo. Ministro convocou audiência pública a ser realizada nos dias 10 e 11 de junho de 2024, a fim de ouvir os especialistas no tema. Ambas as entidades participaram do feito e deram as suas contribuições para o debate na E. Corte. No mais, decidiu-se pela conversão da então ADO n. 84 em Arguição de Descumprimento de Preceito Fundamental, pois a ação tem natureza plúrima e heterogênea, envolvendo um conjunto de aquisições e o uso indiscriminado de ferramentas de intrusão virtual.

7. Nesse momento, portanto, o InternetLab e a Data Privacy Brasil vêm, na presente petição, apresentar a sua contribuição como *amici curiae*, que reúne dados e conclusões de pesquisas para apresentar a este E. STF:

(i) a classificação e organização dos *spywares*, programas de intrusão em dispositivos e comunicações digitais;

(ii) argumentação sobre a inconstitucionalidade do uso indiscriminado destas tecnologias tratadas pelo Estado; e

(iii) subsídios para a apreciação do caso à luz da interpretação constitucional sobre a proteção da privacidade e intimidade, do sigilo de dados e das comunicações, e do direito à proteção de dados pessoais constante no art. 5º, incisos X, XII e LXXIX da Constituição Federal.

II. A INDÚSTRIA INTERNACIONAL DE EXPLORAÇÃO DE VULNERABILIDADES: CLASSIFICAÇÃO E USOS FREQUENTES DOS *SPYWARES*

8. Para que possamos adentrar às consequências jurídicas do uso e obtenção de *spywares*, primeiro é preciso examinar o que são essas ferramentas e como elas se inserem em uma indústria global de exploração de vulnerabilidades nos sistemas e protocolos de informação. É o que faremos nos parágrafos a seguir.

9. *Spywares* são, em linhas gerais, ferramentas (*softwares*) com capacidades intrusivas de extração de informações e invasão em dispositivos ou sistemas eletrônicos e de comunicações, construídos a partir da exploração de falhas de segurança que eventualmente existam nesses dispositivos ou em redes e protocolos de informação por meio dos quais transitam os fluxos de comunicação. O usuário, titular ou operador do sistema dificilmente é capaz de ter conhecimento a respeito da instalação de um *spyware*, uma vez que essas ferramentas são intencionalmente construídas com o objetivo de serem silenciosas.

10. Como observado por Fionnuala Ní Aoláin, professora de direito público da Universidade de Minnesota Law School e Relatora Especial da ONU sobre Contraterrorismo, os *spywares* exigem hoje cooperação internacional para uma moldura jurídica que possa evitar falhas na malha existente em termos de supervisão e *accountability*. As poucas iniciativas jurídicas são insuficientes para uma proteção adequada de direitos. Segundo Ní Aoláin, "*a tecnologia de spyware está atualmente a ser produzida e implementada sem um quadro regulamentar rigoroso capaz de responder às suas características únicas e à ameaça substancial aos direitos humanos*"[2]. Os *spywares* são tecnologias intrusivas para vigilância do conteúdo das comunicações digitais dos indivíduos e outras informações, incluindo metadados (localização,

[2] NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 8. Disponível em: https://repository.graduateinstitute.ch/record/301602?v=pdf

duração, fonte e contatos). Nesse sentido, a "extração de informações" se refere a uma ampla gama de tipos de dados.

11. Uma vulnerabilidade, por sua vez, pode ser definida como "*um conjunto de condições ou comportamentos que permite a violação de uma política de segurança explícita ou implícita*"[3]. Vulnerabilidades podem surgir em qualquer estágio, desde o *design* até a implantação do *software*, e podem ter diversas causas técnicas. Essas incluem falhas no *software*, decisões de *design* ou de configuração mal orientadas, além de interações imprevistas entre os sistemas e as condições do ambiente.[4] É indiscutível, no campo da engenharia de *software*, que vulnerabilidades sempre irão existir, assim como o fato de que essas falhas expõem sistemas e usuários desses produtos a riscos significativos[5].

12. Uma vez que tais vulnerabilidades não sejam comunicadas, quer aos fabricantes de dispositivos e *softwares*, quer à população, a sua descoberta e exploração é a porta de entrada para a vigilância direcionada[6]. Ou seja, cria-se, a partir do desenvolvimento, compra e venda dessas tecnologias, um verdadeiro mercado de exploração de vulnerabilidades de segurança nas comunicações. Conforme a autora Ní Aoláin, as principais empresas do setor privado que desenvolvem *spywares* são os grupos NSO (Israel), Quadream (Israel), Candiru/Saito (Israel), Gamma International Ltd (Reino Unido), Vilicius Holding GmbH (Alemanha), Trovicor GmbH (Alemanha), Qosmos (França), Amesys (França), Area SpA (Itália), Hacking Team (Itália), Cytrox (Macedônia), Cyberpoins (EUA), BlueCoat Systems (EUA), Cisco Systems (EUA), entre outros.[7]

[3]HOUSEHOLDER, Allen D. *et al*. The cert guide to coordinated vulnerability disclosure. *Software Engineering Institute: Cert Coordination Center (Carnegie Mellon University)*. Disponível em: https://vuls.cert.org/confluence/display/CVD/The+CERT+Guide+to+Coordinated+Vulnerability+Disclosure, p. 3.
[4]*Ibidem*, p. 7.
[5]*Ibidem*, p. 2.
[6]SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. *Surveillance and Human Rights*. United Nations Human Rights. 28 mai. 2019. Disponível em: https://digitallibrary.un.org/record/3814512?v=pdf.
[7] NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 20. Disponível em: https://repository.graduateinstitute.ch/record/301602?v=pdf

13. Em termos gerais, há duas maneiras principais pelas quais os governos podem acessar essas ferramentas. A primeira é por meio do desenvolvimento de *softwares* de monitoramento em suas próprias agências e departamentos de inteligência, ou pela reinvenção de expedientes investigativos já existentes. A segunda, e a mais comum, é por meio da encomenda e aquisição de *softwares* espiões avançados oferecidos por empresas que fazem parte da indústria internacional de vigilância.

14. Nesse sentido, o relatório "*Surveillance and Human Rights*"[8], desenvolvido pela Relatoria Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão da Organização das Nações Unidas, mobilizou uma série de análises em todo o mundo sobre a vigilância estatal direcionada. As submissões evidenciaram que a maioria das tecnologias de vigilância direcionada usadas pelos governos vêm do setor privado. Em geral, essas empresas firmam acordos sigilosos com autoridades interessadas nessas ferramentas.

15. A falta de transparência de governos e empresas que exploram as vulnerabilidades de segurança resulta em uma consequência notável: dificulta a compreensão pública do problema. Nessa perspectiva, a maior parte das informações que possuímos sobre as vulnerabilidades de segurança resulta do trabalho investigativo de organizações civis e pesquisadores independentes[9].

16. A operação da indústria de vulnerabilidades é consideravelmente mais obscura se comparada, por exemplo, aos processos de compras ordinários do governo. A ausência de transparência é crucial para que esse tipo de negócio atinja seu objetivo principal, que consiste na vigilância silenciosa de alvos específicos possibilitada pelo aproveitamento de falhas de segurança de tecnologias usadas pela maioria dos cidadãos. Assim, ao não se dar transparência a tais produtos/serviços e sobre a negociação sobre eles, Estados evitam que tais vulnerabilidades sejam descobertas e corrigidas, gerando um ciclo vicioso.

17. Este ciclo vicioso produz tecnologias mais suscetíveis à vigilância e menos seguras no geral, pois não há garantia que vulnerabilidades serão apenas exploradas

[8]SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. *Surveillance and Human Rights*. United Nations Human Rights. 28 mai. 2019.
[9]*Ibidem*, p. 2-3.

com finalidades legítimas. Assim, a ausência ou fragilidade de controles na exportação e transferência de tecnologias que exploram as vulnerabilidades explicitadas acima é um catalisador para expedientes de vigilantismo, o que se reforça em governos com tendências autocráticas[10]. David Kaye[11]e Marietje Schaake[12] falam sobre a dinâmica desse mercado:

> Elas vendem e fazem a manutenção de seus produtos para clientes governamentais sem levar em conta os padrões de repressão desses governos e sem a transparência e diligência adequadas. Estamos no precipício de uma catástrofe tecnológica de vigilância global, uma avalanche de ferramentas compartilhadas entre fronteiras, com governos que não conseguem restringir sua exportação ou uso.[13]

18. Desta maneira, a indústria global de vulnerabilidades de segurança está apoiada em práticas opacas de Estados, e ambos implicam em um ambiente informacional menos seguro e confiável a todos os cidadãos. Tais serviços e produtos vêm impactando significativamente o ambiente democrático, bem como as liberdades de imprensa e de expressão.

19. Este impacto precisa ser ilustrado. Como exemplo de caso que ganhou repercussão internacional nesse sentido, abordaremos abaixo o caso da ferramenta Pegasus, desenvolvido pela empresa israelense *NSO Group Technologies*[14].

II.1. O CASO PEGASUS

20. O *software* Pegasus ficou globalmente conhecido por sua instalação furtiva e pela potencialidade em extrair uma grande quantidade de dados, em fluxo e armazenados, de celulares. Dentre as suas características e funcionalidades, destaca-

[10]SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. *Surveillance and Human Rights*. United Nations Human Rights. 28 mai. 2019, p. 1.

[11]Ex-relator da ONU na relatoria especial de promoção e proteção do direito à liberdade de opinião e expressão.

[12]Ex-membra do Parlamento Europeu e ex-diretora do Centro de Cyber Política da Universidade de Stanford.

[13]KAYE, D; SCHAAKE, M. Global spyware such as Pegasus is a threat to democracy. Here's how to stop it. *Washington Post*, 19 jul. 2021. Disponível em: https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/

[14] Vide, para mais informações, o *site* da empresa: https://www.nsogroup.com.

se a capacidade de acessar remotamente os dispositivos, permitindo ao invasor o monitoramento e, inclusive, o controle do aparelho.

21. Assim, o Pegasus permite o acesso e o envio de mensagens, a interceptação e a efetuação de chamadas e videochamadas, a transformação do celular em escuta ou em câmera remota, e até o acesso à geolocalização, isto é, o registro da mobilidade e o rastreio do aparelho a partir de dados do GPS[15].

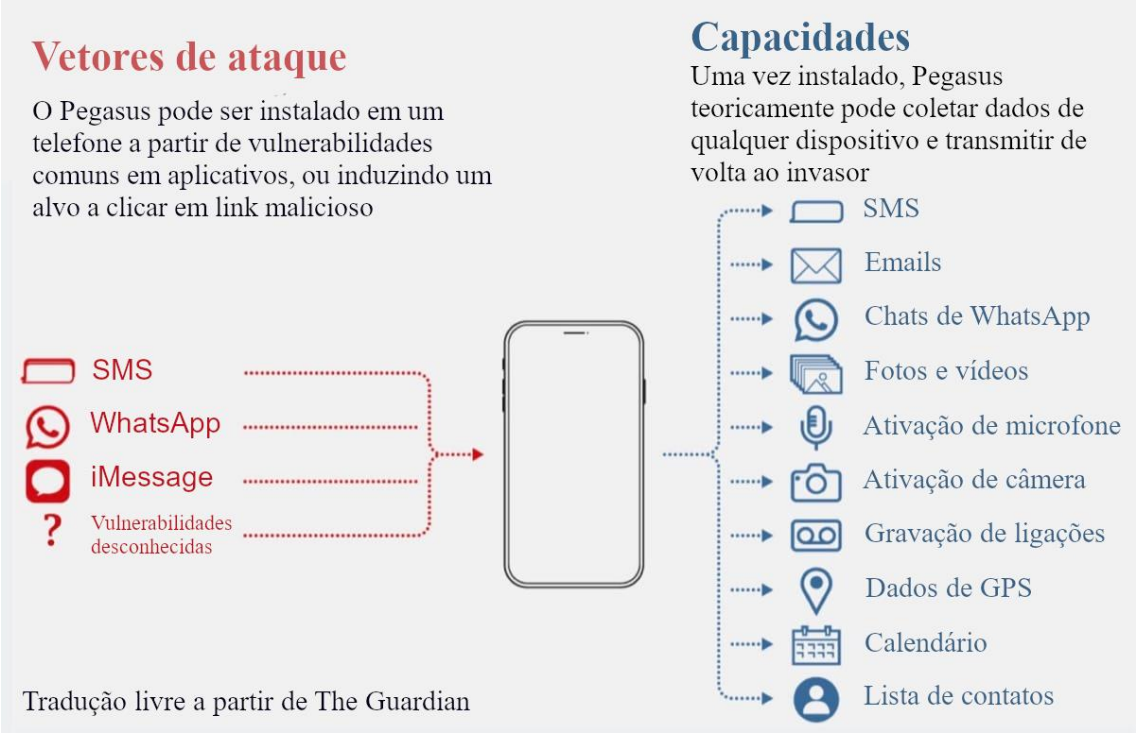

Figura 1: Funcionamento do *spyware* Pegasus (Tradução livre a partir de The Guardian)[16].

22. Em 2020, a *Forbidden Stories* e a Anistia Internacional publicaram o vazamento de uma lista da NSO Group com mais de 50.000 números de celulares de mais de 50 países possivelmente alvos dos clientes da NSO Group[17]. Na época, a empresa israelense alegou que a lista divulgada não era de sua autoria e que vendia apenas para que governos monitorassem dispositivos móveis de indivíduos

[15] PEGG, David, CUTLER, Sam. What is Pegasus spyware and how does it hack phones?. *The Guardian*, 18 jul. 2021. Disponível em: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

[16] *Ibidem.*

[17] FORBIDDEN STORIES. *About the Pegasus Project*, 18 jul. 2021. Disponível em: https://forbiddenstories.org/about-the-pegasus-project/

específicos, suspeitos de estarem envolvidos em crimes graves, como "*terrorismo, pedofilia, tráfico de pessoas e de drogas, sequestros, dentre outros*"[18]. No entanto, a investigação comprovou que "*pelo menos 180 jornalistas foram selecionados como alvos em países como a Índia, o México, a Hungria, Marrocos e França*"[19]. Além de jornalistas, "*potenciais alvos incluem também defensores de direitos humanos, acadêmicos, líderes sindicais, diplomatas, políticos que, em geral, são críticos ao governo no poder*."[20]

23. Nos meses que se seguiram à publicação da lista, 17 organizações de mídia e comunicação científica e mais de 80 jornalistas se juntaram à *Forbidden Stories* e à Anistia Internacional, com o objetivo de revelar os usos ilegítimos do Pegasus por governos.

24. Em 2021, o Laboratório de Segurança da Anistia Internacional[21] publicou o relatório da metodologia e dos resultados de uma "*análise forense aprofundada de inúmeros dispositivos móveis de defensores dos direitos humanos e jornalistas de todo o mundo*."[22] O relatório apontou um uso ou intenção de uso generalizada do Pegasus e identificou perfis de alvos de monitoramento, que incluem acadêmicos, jornalistas, ativistas de direitos humanos, representantes políticos e funcionários públicos[23].

25. Nos anos que se seguiram ao lançamento da investigação, ocorreram denúncias e protestos contra o uso do Pegasus. Entidades não governamentais e especialistas independentes produziram uma Carta aberta solicitando aos Estados a implementação de suspensão imediata sobre a venda, transferência e uso desse tipo

[18] NSO GROUP. *Enough is enough!* Disponível em: https://www.nsogroup.com/Newses/enough-is-enough/

[19]FORBIDDEN STORIES. *About the Pegasus Project*, 18. jul. 2021. Disponível em: https://forbiddenstories.org/about-the-pegasus-project/

[20]*Ibidem*. No original: "Potential targets also include human rights defenders, academics, businesspeople, lawyers, doctors, diplomats, union leaders, politicians and several heads of states"

[21]O *Amnesty International Security Lab* é uma equipe multidisciplinar de pesquisadores, hackers, programadores, ativistas e defensores que trabalham para proteger a sociedade civil contra vigilância digital ilegal, *spyware* e outras violações dos direitos humanos possibilitadas pela tecnologia. Mais informações: AMNESTY INTERNATIONAL. Security Lab – Homepage, 2024. Disponível em:https://securitylab.amnesty.org/.

[22]AMNESTY INTERNATIONAL. *Forensic Methodology Report*: How to catch NSO Group's Pegasus. 18 jul. 2021. Disponível em: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/#_ftn1.

[23]FORBIDDEN STORIES. *Pegasus: the new global weapon for silencing journalists*. 18 jul. 2021. Disponível em: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

de tecnologia. A Carta Internacional[24] traz alertas sobre a necessidade de imposição de uma suspensão imediata sobre a venda, transferência e uso de tecnologias de vigilância, ante os riscos para os direitos e liberdades individuais.

26. O Parlamento Europeu também investigou o episódio e produziu relatório[25], em que argumenta que a falta de regulamentações locais para o uso de *spywares*, que proíbam usos generalizados dessas ferramentas, têm representado ameaças a direitos humanos. Assim, defende que "*o uso de* spywares *deve ser permitido apenas* em casos excepcionais *e por um período limitado de tempo*", e que:

> *spywares* só devem ser utilizados nos Estados-Membros em que as alegações de abuso tenham sido exaustivamente investigadas e que a legislação nacional esteja em conformidade com as recomendações da Comissão de Veneza e com a jurisprudência do Tribunal de Justiça da UE, e que regulamentações de controle das exportações tenham sido aplicadas.[26]

27. No entanto, a *NSO Group*, empresa responsável pela fabricação do *spyware* Pegasus, é apenas uma das muitas companhias que conformam o amplo mercado internacional privado de tecnologias de vigilância e intrusão remota.

28. Como referido por Edward Snowden, em entrevista concedida ao Jornal *The Guardian*[27], tais *softwares* não produzem qualquer tipo de proteção aos cidadãos, mas somente formas de infiltração, isto é, violações ao direito à privacidade[28].

---

[24] A Carta Internacional, em sua versão original na língua inglesa, pode ser encontrada no site da Transparência Internacional: <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>.

[25]EUROPEAN PARLIAMENT. *Investigation of the use of Pegasus and equivalent surveillance spyware*. Jun. 2013. Disponível em: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf.

[26]EUROPEAN PARLIAMENT. *Spyware:* MEPs call for full investigations and safeguards to prevent abuse. 15 jun. 2023.

[27] Trechos da entrevista podem ser acessados aqui no jornal britânico independente: PEGG, David; LEWIS, Paul. Edward Snowden calls for spyware trade ban amid Pegasus revelations. *The Guardian*, 19 jul. 2015. Disponível em: https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations?_twitter_impression=true.

[28] Da entrevista, em tradução livre: "*É como uma indústria onde a única coisa que eles fazem é criar variantes personalizadas da Covid para escapar das vacinas*", disse ele. "*Seus únicos produtos são vetores de infecção. Eles não são produtos de segurança. Eles não fornecem nenhum tipo de proteção, nenhum tipo de profilaxia. Eles não fazem vacinas – a única coisa que vendem é o vírus*", cf. PEGG, David; LEWIS, Paul. Edward Snowden calls for spyware trade ban amid Pegasus revelations. *The*

29. O caso Pegasus é um exemplo de muitos existentes, o que deve gerar um alerta ainda maior. Se a indústria de exploração de vulnerabilidades opera propositalmente de forma opaca, a consequência é que temos um ambiente de ausência de conhecimento e confiança em relação às funcionalidades, capacidades e níveis de proteção a direitos humanos praticados no oferecimento de serviços por diferentes empresas.

30. Entretanto, um juízo sobre os direitos fundamentais tangenciados pelas diferentes tecnologias oferecidas por esta indústria precisa recorrer a uma tipologia de tais ferramentas e de suas capacidades.

31. Em meio a expressões técnicas e diferentes nomes, **o efeito concreto que cada funcionalidade possui sobre o usuário e sobre a integridade do sistema informacional deve ser o parâmetro de entendimento de como essas ferramentas operam.** Entender essas diferenças é crucial para que entendamos o risco colocado por elas.

32. Por esse motivo, apresentamos no próximo tópico uma **tipologia sobre os diferentes tipos de ferramentas de vigilância direcionada *(spywares)* identificados em contratos da administração pública brasileira**, relacionando-os aos graus de risco que tais ferramentas apresentam a direitos fundamentais. Buscamos demonstrar, a partir da análise de tecnologias hoje utilizadas, como o mercado de vulnerabilidades nas comunicações pode afetar a integridade do sistema informacional, a segurança nas comunicações e a confiança num ambiente democrático.

II.2. DAS DIFERENTES DEFINIÇÕES E CAPACIDADES DOS *SPYWARES*

33. *Spywares* são programas de computador com capacidades intrusivas de extração de informações e invasão em dispositivos ou sistemas eletrônicos e de comunicações, construídos a partir da exploração de falhas de segurança que eventualmente existam nesses dispositivos ou em redes e protocolos de informação por meio dos quais transitam os fluxos de comunicação. Do ponto de vista analítico, os *spywares* podem ser diferenciados a partir de suas *affordances* e suas possibilidades de ação.

Guardian, 19 jul. 2015. Disponível em: https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations?__twitter_impression=true

34. Apesar de pouco utilizado no direito constitucional brasileiro, o conceito de *affordance* é muito utilizado no direito computacional contemporâneo.[29] O conceito de *affordance* foi construído inicialmente na psicologia e nos estudos sobre ambiente e percepção visual,[30] sendo posteriormente recepcionado nas áreas de design e interação homem-máquina.[31] As *affordances* concernem às possibilidades de ação proporcionadas por um determinado objeto ou arquitetura.

35. Partindo da discussão sobre *affordances* e possibilidades de ação, analisou-se como diferentes arquiteturas e construções de códigos produzem certos tipos de possibilidades de ação, em razão das características dos próprios programas de computador e suas intencionalidades. Essa diferenciação nos permitiu enxergar mais claramente diferentes *tipos de spywares*, que podem ser diferenciados funcionalmente, produzindo categorias descritivas mais precisas.

36. O problema de se considerar todos os tipos de *spywares* como um bloco monolítico, homogêneo, é a redução da complexidade deste gênero de programas de computador, do qual surgem especificidades. Por isso, partimos de elementos caracterizadores comuns, porém apresentamos tipologias específicas.

37. Analiticamente, de acordo com a literatura especializada,[32] os diferentes tipos de *spywares* precisam passar por quatro elementos comuns, que os tornam identificáveis como tal:

(i) os dados são obtidos de um dispositivo a partir de uma extração que não ocorreria se não fosse em razão da introdução de um programa de computador, código ou ataque;

[29] HILDEBRANDT, Mireille. Law as Information in the Era of Data-Driven Agency. *The Modern Law Review*, v. 79, n. 1, p. 1-30, 2016. HILDEBRANDT, Mireille. Smart technologies. *Internet Policy Review*, v. 9, n. 4, p. 1-16, 2020.

[30] GIBSON, James J. *The ecological approach to visual perception.* Boston: Houghton Mifflin, 1979.

[31] MCGRENERE, Joanna; HO, Wayne. Affordances: Clarifying and evolving a concept. *Graphics interface*, 2000, p. 179-186.

[32] HARKIN, Diarmaid; MOLNAR, Adam; VOWLES, Erica. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, media, culture*, v. 16, n. 1, p. 33-60, 2020, p. 36-37.

(ii) os dados são extraídos dos dispositivos partindo da premissa de que o usuário do dispositivo tido como alvo não está ciente da situação de extração de informações;

(iii) o código ou programa de computador é utilizado no contexto de criar um alvo, seja um indivíduo ou um grupo de indivíduos, com a intenção de monitoramento, rastreio e vigilância; e

(iv) os dados que são extraídos dos dispositivos possuem um contexto específico legítimo e podem ser considerados como informações privadas, como localização, fotos, senhas, mensagens, metadados de aplicativos, entre outros.

38. Para a melhor compreensão e análise dos *softwares* que são construídos para extração de informação de um usuário ou sistema sem conhecimento do titular ou operador do sistema, apresentamos de forma sistematizada as diferentes capacidades dessas ferramentas.

39. Identificamos, assim, seis (6) categorias que podem auxiliar a Corte no julgamento adequado sobre os como as ferramentas afetam preceitos fundamentais:

1) Extração em dispositivo;
2) Extração em infraestrutura;
3) Derrubada de chaves criptográficas;
4) Extração de informações deletadas;
5) Extração de sistemas de comunicação em nuvem;
6) Extração de informações para inferência.

40. A classificação não é única e excludente, podendo, portanto, mais de um *software* cumprir mais de um método de extração. Inclusive, com base em nossa análise, identificamos que a grande maioria dos *spywares* tem a capacidade de ação por mais de uma via, assim aumentando o seu poder de sucesso na invasão do alvo selecionado.

41. A tipologia proposta é aplicável na prática. A partir da categorização, classificamos as tecnologias elencadas em um relatório de pesquisa que traz as tecnologias adquiridas pelo Poder Público no país. Abaixo, indicamos um mapa

baseado no relatório "Mercadores da Insegurança"[33], apontando a disseminação dos *spywares* no Brasil. No Doc. 01, indicamos uma tabela contendo suas características e classificação a partir da tipologia proposta.

Figura 2: Tipologias por estados (Data Privacy Brasil)

42. A intenção da construção da tipologia não é somente prover um ganho analítico do ponto de vista descritivo. Entendemos que, com uma compreensão mais apurada das diferentes *affordances* desses tipos de *spywares*, fica mais evidente a relação existente entre certos tipos de riscos a direitos fundamentais que são intensificados e que exigem, por sua vez, uma contrapartida institucional mais robusta no sentido de criação de instrumentos de controle, contrapesos e procedimentos institucionais aptos a diminuir os riscos produzidos aos direitos fundamentais dos cidadãos.

[33] AMARAL, P.; CANTO, M.; PEREIRA, M. C. M.; André Ramiro (coord.). *Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil.* Recife: IP.REC, 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf.

43. Esses riscos aos direitos de privacidade são especialmente sensíveis, considerando que o direito à privacidade e à proteção de dados pessoais são direitos fundacionais em sociedades democráticas e habilitam a realização de outros direitos fundamentais, como o direito de liberdade de expressão, direito de liberdade religiosa, direito de liberdade de associação, direito de devido processo, direito de liberdade de movimento, direito à vida e à liberdade. Como reconhecido por Fionnuala Ní Aoláin, os *spywares* afetam os direitos fundamentais de forma interconectada.[34]

44. Os *spywares* afetam os direitos fundamentais de forma molecular (ou de forma interconectada), pois estes são violados em conjunto e não de forma isolada, o que representa um problema de alta importância para o sistema de justiça no Brasil e para a devida tutela dos direitos fundamentais. A tipologia construída ajuda a pensar os tipos de violações a partir das possibilidades de ação (*affordances*), oferecendo maior clareza analítica para uma análise do ponto de vista dos direitos constitucionais e efetiva tutela dos direitos fundamentais no Brasil.

II.2.1. Extração em dispositivo

45. *Softwares* de extração em dispositivos são **ferramentas capazes de extração lógica e física nos dispositivos eletrônicos**, o que inclui celulares, drones, cartões SIM e SD, dispositivos GPS, dentre outros. Isso significa que podem extrair todos os arquivos ou arquivos selecionados de um dispositivo (como arquivos de redes sociais, aplicações de mensageria ou navegadores), de acordo com a aplicação utilizada.

46. **Esta é a categoria mais recorrente entre as ferramentas de intrusão cibernética no governo brasileiro, sendo mais da metade dos *softwares* contratados**. Algumas dessas ferramentas são: da empresa Cellebrite, os modelos UFED, Physical Analyzer, Premium, Advanced Services e CHINEX; da empresa Exterro/AccessData, o Forensic Toolkit; e da empresa Micro Systemation AB, XRY Logical, Physical, Pinpoint (expansão), CRY Cloud e MSAB Office.

[34] NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 34.

47. Esta categoria é a mais utilizada pelas forças de segurança pública, órgãos investigativos e forenses, no âmbito de uma investigação em curso. As ferramentas de extração em dispositivos não necessariamente são utilizadas de forma remota, de forma que o dispositivo atingido deve estar sob posse da autoridade investigativa.

48. Por demandarem a presença física do dispositivo eletrônico, seus alvos, ao menos em tese, sabem que foram submetidos a procedimentos de busca e apreensão. No entanto, a necessidade física do dispositivo eletrônico não diminui a gravidade do acesso às comunicações privadas. Trata-se, de qualquer maneira, de possibilidade de quebra de sigilo de comunicação privada que exige cumprimento dos ritos formais do devido processo legal, bem como observância às garantias processuais fundamentais dos indivíduos sob suspeita.

49. O expediente investigativo diretamente no aparelho pode, ainda, trazer riscos de busca especulativa (*fishing expedition*)[35] que não têm finalidade definida e extrapolam limites razoáveis, ou o risco de acesso a arquivos pessoais que não tenham qualquer relação com a investigação em curso.

50. Embora não possam ser diretamente tratados como "ferramentas de intrusão remota", a regulação da utilização desta categoria traria, minimamente, segurança jurídica para o processo de cadeia de custódia e ordenamento das investigações em território nacional.

II.2.2. Extração em infraestrutura

51. *Softwares* de extração em infraestrutura são **ferramentas capazes de extração a partir da invasão de infraestruturas de redes públicas ou privadas.**

52. Essa invasão pode ocorrer por meio de falhas em protocolos de sistemas que deveriam ser compartilhados apenas entre operadoras de telecomunicações, ou de vulnerabilidades de segurança no sistema. As falhas e brechas podem demorar meses até que os desenvolvedores consigam corrigir o erro. Também há situações de

[35]SILVA. Viviani Ghizoni da; MELO E SILVA, Philipe Benoni; ROSA, Alexandre Morais da. *Fishing Expedition e Encontro Fortuito na Busca e na Apreensão*. Florianópolis: Emais Editora & Livraria Jurídica, 2ª Edição, 2022.

descaso de operadoras de telefonia, como o da falha explorada pelo FirstMile, que é conhecida há anos[3637].

53. Exemplo dessa categoria são as ferramentas FirstMile, GI2 e PI2, operadas pela empresa Cognyte[38]. O FirstMile, cuja utilização pela Agência Brasileira de Inteligência (Abin) tem sido investigada pela Polícia Federal, teria sido utilizado para monitorar autoridades, jornalistas, ativistas e ministros do Supremo Tribunal Federal (STF)[39].

54. A ferramenta é capaz de identificar, com precisão, a localização de dispositivos eletrônicos que utilizem as redes 2G, 3G e 4G. Isso ocorre por meio de falhas no protocolo Sistema de Sinalização Nº 7 (SS7), um fenômeno já identificado pela comunidade de ciência da computação há mais de dez anos. O SS7 é um protocolo que deixa diferentes operadoras se comunicarem e compartilharem informações, como o monitoramento da posição de aparelhos, para garantir a entrega de mensagens SMS.

55. O FirstMile, com base em uma técnica de *spoofing* que emula comunicações que deveriam ser verdadeiras entre dispositivos que operam com base neste protocolo de comunicação, pode monitorar até 10 mil donos de celulares a cada 12 meses, apenas a partir do número de contato telefônico desejado.

---

[36] KURTZ, João. Falha em rede de celulares deixa brecha para ataques bancários. *Techtudo*. 10 mai. 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/05/falha-em-rede-de-celulares-deixa-brecha-para-ataques-bancarios-entenda.ghtml.

[37] Em 2017, a organização CodingRights demonstrou como pesquisadores de segurança da informação vinham alertando sobre as vulnerabilidades, cf. TEIXEIRA, Lucas. Consultando o espião de bolso: vulnerabilidades SS7 e rastreamento global. Medium, 28 jul. 2917. Disponível em: https://medium.com/codingrights/consultando-o-espi%C3%A3o-de-bolso-vulnerabilidades-ss7-e-rastreamento-global-bc9920008c3c.

[38] Em 2021, a Verint criou uma empresa denominada "Cognyte", derivada do setor de Cyber Inteligência focada em soluções de negócios. Mais informações em: https://www.verint.com/press-room/2021-press-releases/verint-celebrates-day-one-as-a-company-focused-on-enabling-brands-to-achieve-boundless-customer-engagement-following-completion-of-cognyte-software-spin-off/ e https://www.businesswire.com/news/home/20210622005107/en/Cognyte-Starts-as-a-Separate-Public-Company-with-Strong-First-Quarter-Results

[39] O QUE é o FirstMile, software que teria sido usado pela Abin para monitorar jornalistas e ministros do STF. *Correio Brasiliense*, 25 jan. 2024. Disponível em: https://www.correiobraziliense.com.br/mundo/2024/01/6792403-o-que-e-o-firstmile-software-que-teria-sido-usado-pela-abin-para-monitorar-jornalistas-e-ministros-do-stf.html

56. Além disso, o sistema é capaz de gerar alertas sobre a rotina de movimentação dos alvos de interesse. Apesar de não ser uma informação tão precisa quanto o GPS, a agregação de informação sobre localização em uma estação rádio-base (ERB) permite a identificação de padrões de localização e intensifica ameaças a liberdades individuais.

57. O GI2 é capaz de localizar o dispositivo alvo com precisão, usando um dispositivo *homing* dedicado, sem desabilitar o alvo de se comunicar; extrair as coordenadas GPS do celular do alvo em redes GSM e UMTS (3G); ouvir, ler, editar, e redirecionar chamadas recebidas e realizadas, bem como mensagens de textos (criptografia A5/1 e A5/3); ativar remotamente o microfone de um aparelho celular; Identificar a presença do aparelho telefone do alvo; bloquear comunicações celular para neutralizar IEDs e interceptar SMS recebidos e enviados.

58. O PI2, por sua vez, tem capacidade de coletar tráfego GSM em "área ampla", além de interceptar ligações e mensagens de texto, quebra de criptografia, análise de "padrões suspeitos de comunicação" e possibilidade de múltiplos usuários analisarem chamadas ao mesmo tempo.

II.2.3. Derrubada de chaves criptográficas

59. *Softwares* de derrubada de chaves criptografadas são ferramentas capazes de romper com os mecanismos de defesa do dispositivo, quebrando as senhas criptografadas para o acesso ao aparelho. Isso ocorre, por exemplo, por meio do desbloqueio de dispositivos protegidos por padrão, senha ou código PIN, além de *bypass* de criptografia em dispositivos Android e iOS.

60. A criptografia é, em linhas gerais, um recurso que protege a segurança das informações, fazendo uso de técnicas matemáticas para cifrá-las e decifrá-las, o que é fundamental para a garantia da disponibilidade, integridade e confidencialidade de quaisquer trocas de dados e comunicações na internet. Como veremos no tópico III.2, os ministros desta E. Corte já sinalizaram no sentido de que a criptografia é um mecanismo de segurança que promove direitos fundamentais[40].

[40] Na ADI nº 5.527 e ADPF nº 403, o Supremo Tribunal Federal reconheceu a importância da privacidade em meios digitais, afirmando que a criação de *backdoors* (a criação de meios excepcionais para acessar os dados dos usuários criptografados) cria violações de segurança em massa, julgando

61. No caso da criptografia forte, ninguém além das partes envolvidas consegue acessar os dados enviados ou recebidos, nem mesmo o fornecedor do dispositivo ou do canal de comunicação. Todavia, falhas de segurança nos protocolos desenvolvidos podem ser encontradas e exploradas pelas empresas desenvolvedoras dessas ferramentas, o que torna o conteúdo das comunicações acessível, violando-se o sigilo.

62. **Em geral, esses *softwares* são adquiridos com outras ferramentas que somam características intrusivas.** Dentre os *softwares* analisados, o Encase Forensic[41], da empresa OpenText, é a ferramenta especialista desta categoria com acesso a dados encriptados com Bitlocker (Windows 10), Data Protection 8.17 (Dell) e PGP v10.3 (Symantec), acesso a dados encriptados com APFS (Apple File System) e *bypass* da segurança para o Apple T2 Security.

II.2.4. Extração de informações deletadas

63. **Esta categoria inclui ferramentas capazes de recuperar arquivos apagados de um dispositivo eletrônico.** Elas possibilitam a recuperação de documentos do próprio dispositivo ou até mesmo dados de outras aplicações como Whatsapp, Facebook e Telegram, além de permitir o acesso a *e-mails* e arquivos anexados.

64. Essa funcionalidade pode ser encontrada nos *softwares* UFED e Physical Analyzer da Cellebrite, no Forensic Toolkit da Exterro/AccessData e nos XRY Physical e MSAB Office da Micro Systemation AB.

II.2.5. Extração de sistemas de comunicação em nuvem

65. ***Spywares* de extração de sistemas de comunicação em nuvem são ferramentas capazes de extração de dados de aplicações com armazenamento em nuvem, como Facebook, Google, iCloud, Twitter e Snapchat**. Inclui modalidade de extração automática, a partir de *tokens* de acesso a aplicações previamente extraídos com aparelho em mãos, e de extração manual, sem necessidade de o aparelho estar presente, a partir de *login* e senha previamente acessados por outros meios.

constitucional a adoção de criptografia de ponta-a-ponta em aplicações na internet. Esse ponto será desenvolvido nesta petição.

[41] Detalhes do produto em: https://www.opentext.com/pt-br/produtos/encase-forensic.

Encontrado nas ferramentas UFED Cloud (Cellebrite), Magnet AXIOM (OpenText) e CRY Cloud (Micro Systemation AB).

II.2.6. Extração de informações por inferência

66. *Spywares* de extração de informações por inferência são ferramentas com um alto grau invasivo, capazes de processar dados, gerando informações "novas" em análises complexas dos dispositivos.

67. Esse tipo de funcionalidade inclui a análise, filtragem, visualização e sistematização de dados extraídos de dispositivos móveis, drones, tecnologias vestíveis, GPS, veículos, cartões SIM e o reconhecimento de conteúdos em imagens, cartões de memória e outras fontes. Além da unificação de banco de dados para armazenamento de provas com indexação, filtragem e ferramentas de pesquisa de resultados de dados armazenados.

68. Pode-se citar, como exemplos, os *softwares* UFED Cloud, Pathfinder e Commander, da empresa Cellebrite; no Magnet AXIOM, da empresa OpenText; no Forensic Toolkit, da empresa Exterro/AccessData; e nos XAMN Horizon e XAMN Spotlight, da empresa Micro Systemation AB.

69. Esta categoria representa *softwares* mais sofisticados, que são ferramentas mais complexas, utilizando-se de mecanismos de Inteligência de Fontes Abertas (OSINT) e/ou inteligência artificial para a exploração e análise dos dados. Esta característica demonstra um potencial de crescimento, acompanhando o aprimoramento e expansão da inteligência artificial.

70. Estes *spywares* introduzem uma camada adicional de inteligência, capaz de ligar associações e localizações de indivíduos e fazer correlações e inferências de uma forma não transparente. Esta falta de transparência pode levar a interpretações erradas na análise de informações, por exemplo, pela reprodução de preconceitos já vistos em diversas novas ferramentas que utilizam tecnologias de reconhecimento facial e inteligência artificial[42]. Além disso, pelo seu caráter extremamente opaco, seus

[42]O artigo *Insuficiência dos princípios éticos para normatização da Inteligência Artificial: o antirracismo e a anti-discriminação como vetores da regulação de IA no Brasil* demonstra a problemática do uso da IA sem uma regulação pautada nos direitos humanos. Disponível em https://www.dataprivacybr.org/documentos/insuficiencia-dos-principios-eticos-para-normatizacao-

vieses podem ser reproduzidos em atividades de investigação e inteligência, criando riscos generalizados a indivíduos e grupos sociais que sejam submetidos aos *spywares*.

II.3. DA NECESSÁRIA DIFERENCIAÇÃO ENTRE *SPYWARES* E INTELIGÊNCIA EM FONTES ABERTAS (OSINT)

71. Visto as características e gêneros dos *spywares*, cumpre explicar o que seriam OSINT e, assim, diferenciar essa tecnologia das ferramentas de *spywares*. A Inteligência de Fontes Abertas (IFA), em inglês *Open Source Intelligence (OSINT)*, é um serviço de inteligência, que opera por meio de dados públicos e de fontes abertas como redes sociais, mídias, blogs, tuítes e notícias.

72. Segundo Koops, Heopman e Leenes (2013)[43], a inteligência de fontes abertas (OSINT) é um processo de coleta, análise e uso de dados de fontes abertas para propósitos inteligentes. Já para Howells e Ertugan (2017)[44], a OSINT é uma forma de gerenciamento de coleta de inteligência que localiza, seleciona e extrai informações de fontes abertas, como Twitter e Facebook, e por fim, analisa as informações para produzir inteligência. Na área de segurança da informação, este processo de coleta de dados tem o objetivo de produzir informações atuais e relevantes que sejam valiosas para um invasor ou um concorrente.

73. Assim, **a principal diferença entre *spywares* e OSINTs é a forma como eles obtêm dados**: os primeiros exploram vulnerabilidades nos códigos e programas computacionais para, sem o consentimento de usuários, ter acesso a seus dados. **As OSINTs, por outro lado, utilizam fontes de dados públicos, disponíveis na rede mundial de computadores, de modo a criar inteligência a partir da compilação, sistematização e interpretação de fontes abertas**.

---

da-inteligencia-artificial-o-antirracismo-e-a-anti-discriminacao-como-vetores-da-regulacao-de-ia-no-brasil/?idProject=2331.

[43] KOOPS, Bert-Jaap; HOEPMAN, Jaap; LEENES, Ronald. Open-source intelligence and privacy by design. Computer Law & Security Review. *Computer Lay and Security Review*, v. 29, n. 6, p. 676-688, 2013.Disponível em: https://www.cs.ru.nl/J.H.Hoepman/publications/osint-pbd.pdf

[44] HOWELLS, Karen; ERTUGAN, Ahmet. Applying fuzzy logic for sentiment analysis of social media network data in marketing. *Procedia Computer Science*, v. 120, p. 664-670. 2017. Disponível em: https://www.sciencedirect.com/science/article/pii/S187705091732505X

74. Assim, as duas tecnologias são formas distintas de realizar inferências e coletar evidências sobre pessoas e instituições. Ainda que ambos operem sem o consentimento de usuários, os *spywares* realizam a invasão de sistemas, coletando dados muitas vezes sigilosos e restritos.

75. A diferenciação dessas tecnologias é essencial ao debate, uma vez que as OSINTs, apesar de possíveis usos arbitrários, também podem ser utilizadas em contextos de promoção a direitos fundamentais. Destaca-se, ainda, que o jornalismo investigativo faz uso lícito das OSINTs, criando mecanismos eficazes para a apuração de fatos.

76. Apesar da utilização positiva também desta tecnologia, nós destacamos a necessidade de regulação e controle de seu uso por parte do Estado. O uso dessas ferramentas em ampla coleta de informações dispersas em meio digital, que são capazes de detectar, analisar e produzir relatórios que detalham vínculos, acabam por extrapolar a atenção apenas por atividades criminosas, mas se estendem, de forma preocupante, ao monitoramento e perfilamento de atividades que traduzem um livre exercício de direitos civis e políticos.

77. Abaixo, indicamos como essas múltiplas funcionalidades se apresentam a partir de fatos concretos.

II.3.1. OSINT, Harpia Tech e extrapolação das capacidades de inteligência do Estado

78. Em 19 de maio de 2021, o Ministério da Justiça e Segurança Pública lançou o Edital de Licitação n. 03/2021[45], da modalidade pregão eletrônico, com objetivo de atender às necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas (SEOPI). O objeto do certame envolvia a aquisição de "Solução de Inteligência em Fontes Abertas, Mídias Sociais, Deep e Dark Web"[46].

[45]Edital de Licitação Nº03/202; Pregão Eletrônico Nº 3/2021; Processo Nº 08000.000865/2020-30. Disponível em :https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/procedimentos-2021/pregao-2-2021-1/edital_completo.pdf.

[46]"O objeto da presente licitação é a escolha da proposta mais vantajosa para a aquisição de Solução de Inteligência em Fontes Abertas, Mídias Sociais, Deep e Dark Web compreendendo o fornecimento, instalação e configuração, bem como o suporte técnico, em atendimento às necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas (DINT/SEOPI)" (nossos destaques) Edital de Licitação Nº03/202 p. 01.

79. Sua motivação estava atrelada à reestruturação do Subsistema de Inteligência e Segurança Pública (SISP)[47], buscando aumentar a capacidade analítica dos profissionais de inteligência, bem como permitir uma troca mais qualificada de informações entre eles. A empresa vencedora, a Harpia Tecnologia Eireli (Harpia Tech), ofereceu um lance de R$ 5.415.750,00 (cinco milhões, quatrocentos e quinze mil, setecentos e cinquenta reais)[48] para a coleta de informações em fontes abertas, retornando mais de 15.000 resultados por busca, como postagens em redes sociais, DarkWeb, *e-mail*, telefones de contato, informações demográficas, entre outros[49]. Além disso, a ferramenta permite a classificação de "*[...] pessoas*, *grupos*, *companhias*, *organizações*, *páginas web*, *infraestrutura de internet*, *frases*, *documentos*, *arquivos*, *dentre outras*", bem como visualizar todas essas informações em forma de relatórios.

80. Em termos mais precisos: "*[...] a ferramenta gera relatório de inteligência com diferentes perspectivas a respeito das coletas realizadas. Os itens constantes no relatório são, inclusive, passíveis de customização*"[50].

81. Por ser uma solução que coleta dados digitais, agregando e cruzando essas informações para desenvolver perfis de indivíduos para fins de inteligência, seu uso abre espaço para uma constante produção de perfis e para um permanente monitoramento de qualquer coisa que a Inteligência classifica como ameaça.[51]

---

[47]Atendimento às necessidades de aparelhamento da Agência Central do Subsistema de Inteligência, de integração às demais Agências de Inteligência de Segurança Pública (AISP) e atendimento aos objetivos estratégicos do Ministério da Justiça e Segurança Pública. Edital de Licitação Nº03/202 p. 24.

[48]Ministério da Justiça e Segurança Pública. Resultado do Julgamento Pregão Nº 3/202, publicado no DOU, Seção 3, Nº 152, quinta-feira, 12 de agosto de 2021. Disponível em:https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/procedimentos-2021/pregao-2-2021-1/resultado_de_julgamento__dou-pe-3.pdf.

[49] Processo Administrativo nº 08000.000865/2020-30.

[50]Processo Administrativo nº 08000.000865/2020-30, p. 6.

[51] Exemplos dados pela Harpia ao descrever as funcionalidades da solução: "No exemplo abaixo, a menção, por ator malicioso, de um IP da Polícia Federal desencadeia o processo de coleta, a partir de um grupo do serviço de mensageria IRC. A organização é devidamente categorizada. Ao clicar no link ao lado do nome da entidade, o usuário recebe todos os resultados do histórico de busca relativamente à entidade. O autor da publicação é igualmente catalogado, ao passo que o clique em seu nome redireciona o usuário para tela de análise específica sobre o indivíduo, que inclui gráfico temporal e análise de vínculos."; "Na tela abaixo, apresentamos atores monitorados em caráter sistemático pela ferramenta: [...] Na coluna presença virtual, é possível ver as diferentes redes e plataformas nas quais se monitora cada indivíduo (exemplos: twitter, reddit, facebook, youtube, github, discord...)." e "Tela de análise de um criminoso brasileiro. Na tela acima, além da linha do tempo, é possível visualizar análises

82. Nesse sentido, é acertado dizer que, da coleta de informações dessas diferentes fontes, resulta uma espécie de dossiê digital daquele(s) que está(ão) sendo investigado(s), que permite, justamente, a composição do referido cenário analítico. Embora não seja um dossiê em sentido clássico[52], a capacidade do *software* de agregar e integrar dados desagregados em tempo real, produzindo um conhecimento sobre o alvo desejado, gera um dossiê no sentido literal do termo: uma *coleção de informações* sobre um indivíduo, grupo ou organização.

83. Assim como os *spywares*, foco da presente manifestação, a disseminação de tecnologias de vigilância como OSINTs (*Open Source Intelligence*), sem estruturas adequadas de salvaguardas e testes de proporcionalidade à violação de direitos fundamentais, representa uma violação de direitos incompatível com o Estado Democrático de Direito e os direitos constitucionais.

84. Como argumentado por Steven Feldman, esses programas de computador organizados como OSINTS para vigilância podem não apenas agregar milhares de *data points* em um único *dashboard* de análise, mas podem também aplicar técnicas de Inteligência Artificial para análises inferenciais sobre perfis e sobre condutas tidas como suspeitas.[53] Mesmo não sendo a mesma coisa que Pegasus do NSO Group, não se pode ignorar os potenciais usos em violação a direitos fundamentais, especialmente quando são utilizadas técnicas de *targeting* e *profiling* persistente sobre uma pessoa.

---

de vínculos (itens "mencionados" e "relação entre atores"), as diferentes mídias em que a presença do criminoso é observada (no caso, twitter, facebook, youtube, skype, zone-h e github), a classificação de seu status, de filiação a determinado grupo, além de outras informações pertinentes." (destaques nossos)

[52] Como as antigas fichas produzidas pelo DOI-CODI na época da ditadura, sendo, por exemplo, utilizada massivamente pela Comissão Nacional da Verdade na investigação da violação de direitos humanos durante a ditadura civil-militar. Ver ZANATTA, Rafael. *A proteção coletiva dos dados pessoais no Brasil:* vetores de interpretação. Belo Horizonte: Letramento, 2023.

[53]FELDSTEIN, Steven. *The global expansion of AI surveillance*. Washington, DC: Carnegie Endowment for International Peace, 2019.

II.3.2. O potencial das OSINTs para a promoção dos direitos humanos e do jornalismo

85. Entre os usos das OSINTs que fomentam direitos fundamentais e bens públicos, podemos citar a sua atuação no jornalismo. Ela tem se colocado como um método disseminado entre jornalistas, ativistas e no sistema ONU[54], possibilitando as checagens colaborativas, por meio da inteligência de dados abertos, para identificação de violações de direitos humanos.

86. Segundo os pesquisadores Michael Glassman e Min Ju Kang[55], a OSINT não é um tipo novo de inteligência, mas em geral, surgiu na resolução de problemas humanos durante tipos específicos de atividades direcionadas por objetos. Sua prática é vista em perspectiva positiva, particularmente como um método de coleta de dados convencional que não viola os direitos humanos[56]. Listamos abaixo alguns exemplos.

87. O *Bellingcat*[57] é um grupo de jornalismo investigativo com sede na Holanda, especializado em verificação de fatos através das OSINTs. A *Bellingcat* publica reportagens sobre zonas de guerra, violações dos direitos humanos e do submundo do crime. A instituição investigou, por exemplo, a execução de pessoas pelo cartel no México[58] e assassinatos na Guerra da Síria[59]. A *Ceasefire Centre for Civilian Rights*[60] monitora possíveis violações do direito humanitário internacional e dos direitos humanos de forma descentralizada por meio de OSINTs. Um exemplo é

[54]A ONU utiliza OSINTs, por exemplo, no combate ao tráfico de drogas sintéticas, até mesmo oferecendo treinamento e ferramentas grátis aos Estados Membros. Disponível em https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/OSINT.html.

[55]GLASSMAN, MICHAEL; KANG, MIN JU. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, v. 28, n. 2, p. 673-682, 2012.Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0747563211002585

[56]HRIBAR, GAŠPER; PODBREGAR, IZTOK; IVANUŠA, TEODORA. OSINT: a "grey zone"? .*International Journal of Intelligence and CounterIntelligence*, v. 27, n. 3, p. 529-549, 2014.Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0747563211002585

[57]https://www.bellingcat.com/.

[58]COUNTERING the Cartel: Darktrace's Investigation into CyberCartel Attacks Targeting Latin America.*Darktrace*. 8 jan. 2024. Disponível em: https://darktrace.com/blog/countering-the-cartel-darktraces-investigation-into-cybercartel-attacks-targeting-latin-america.

[59]INSIDE SJAC's Open-Source Investigative Team. *Syria Justice and Accountability Centre.*16 nov. 2022. Disponível em: https://syriaaccountability.org/inside-sjacs-open-source-investigative-team/.

[60]Mais informações em: https://www.ceasefire.org/.

o caso de violação de direitos humanos contra as minorias Yazidi e Alawite após a invasão do norte da Síria[61].

88. No Brasil temos o Territórios de Exceção[62], uma iniciativa de pesquisa sobre o uso policial de helicópteros como plataforma de tiro em regiões densamente povoadas, especialmente em favelas, com foco no Complexo da Maré, no Rio de Janeiro. Utilizando OSINTs, a pesquisa identificou padrões na utilização deste aparato bélico na cidade durante os anos de 2018 e 2019, apurando 415 operações com uso de helicópteros, sendo que em pelo menos 60 delas há indícios de utilização das aeronaves como plataforma de tiro.

89. Por fim, o Amazônia Minada[63] mostra os processos minerários na Amazônia brasileira, obtidos por dados públicos da Agência Nacional de Mineração (ANM), mapeando e alertando quando processos de mineração se sobrepõem (total ou parcialmente) ou estão contíguos a terras indígenas e unidades de conservação integral da Amazônia Legal, cruzando dados abertos da Agência Nacional de Mineração, Funai, Ministério do Meio Ambiente e InfoAmazonia.

90. Os destaques acima têm como objetivo destacar a importância da separação conceitual entre OSINTs e *spywares*, apontando o uso das primeiras com seu potencial tanto para violação quanto promoção de direitos humanos. Nesse cenário, as salvaguardas e testes de proporcionalidade podem garantir um uso lícito das OSINTs. De outro lado, os *spywares* merecem maior atenção dos aplicadores do direito, em virtude de seu alto grau de invasão e possível violação de direitos fundamentais dos indivíduos que são vítimas dessas ferramentas.

III. O USO DE *SPYWARES* À LUZ DOS DIREITOS FUNDAMENTAIS

91. Após a análise do que seriam esses programas, faz-se necessário explicitar o que significa o descumprimento de preceito fundamental analisado por esta E. Corte: trata-se, nesses termos, de acabar por permitir a utilização de ferramentas tecnológicas extremamente invasivas por órgãos estatais e serviços de inteligência.

[61]CEASEFIRE. *The Yazidi Survivors' Law:* A step towards reparations for the ISIS conflict. [S.D.] Disponível em: https://www.ceasefire.org/wp-content/uploads/2021/05/Yazidi-Survivors-Law-Briefing-1.pdf.
[62] MEDIALAB.UFRJ; AGÊNCIA AUTÔNOMA. Territórios de Exceção: Violação de direitos e uso de helicópteros policiais no Rio de Janeiro. 2021. Disponível em: https://documental.xyz/pt/intervencao
[63] INFOAMAZONIA. Amazônia Minada. 2022. Disponível em: https://minada.infoamazonia.org/

Mais grave ainda, ferramentas estas que têm como corolário a compra e venda de vulnerabilidades na segurança da informação de todos os cidadãos, justamente em razão de como este mercado está estruturado.

92. Dessa forma, direitos fundamentais são colocados sob estado de grave ameaça de violação, como os direitos à privacidade, à segurança de comunicações, imagem, localização, entre outros.

93. O debate sobre como *spywares* afetam direitos fundamentais tem se intensificado nos últimos anos, com análises importantes do sistema internacional de direitos humanos. A relatora especial da ONU de contraterrorismo, Fionnuala Ní Aoláin, aponta que os diversos casos já documentados na Arábia Saudita, Sudão, Iraque e países com documentação de pessoas afetadas por *spywares* apontam para situações de múltiplas violações de normas internacionais de direitos humanos, como direito à vida, exposição ilegal à violência, prisões injustas, interferência desproporcional ao direito de privacidade, interferência desproporcional aos direitos de liberdade de expressão, liberdade de associação e liberdade religiosa.[64]

94. Verifica-se que o funcionamento desta indústria, sob o pretexto de combater crimes graves, como o terrorismo, afeta genericamente direitos fundamentais de indivíduos sem justificativa expressa prevista em lei ou outros limites que examinem a proporcionalidade do uso dessas ferramentas. O uso irrestrito e desregulamentado de muitas dessas ferramentas tecnológicas autoriza que o poder público investigue de forma arbitrária qualquer dado de cidadãos à procura de hipotéticas ilegalidades. Trata-se, portanto, de um exercício de tentativa e erro, por meio do qual usuários têm sua privacidade esvaziada e se tornam alvos de medidas coercitivas simplesmente porque haveria qualquer tipo de suspeita, ainda que mínima, em relação a eles.

95. De fato, a ausência de regulação acaba significando uma permissão irrestrita, já que não há qualquer parâmetro a se seguir para usar tais ferramentas ou uma proibição legal expressa. Permite-se, com isso, uma verdadeira "expedição de pesca" injustificável de pessoas insuspeitas para averiguação criminal, realizada de maneira oculta, sem que os atingidos tenham a oportunidade de se defender, já que

[64] NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 22-23.

tais tecnologias de invasão ocorrem sem mesmo que o indivíduo tenha conhecimento delas a qualquer tempo.

96. Ao possibilitar à autoridade investigativa o acesso irrestrito aos dados dos investigados, abre-se espaço para abusos de poder. Também, assume-se o risco de se estabelecer um Estado policial, em que os aparelhos celulares e todos os aplicativos neles presentes são transformados em ferramentas de vigilância, em violação a liberdades civis. Cuida-se de frustrar as garantias individuais previstas na Constituição e que gozam da estatura de direitos fundamentais.

97. Por tudo isso, defendemos nesta contribuição que o Estado possui o dever de não comprar ou de qualquer forma adquirir tecnologias de intrusão remota, que ameaçam gravemente o Estado Democrático e o direito de todos os cidadãos à privacidade e à liberdade de expressão.

98. Defendemos, nesse sentido, a existência de um direito à integridade dos sistemas informacionais, que decorre das proteções constitucionais já garantidas à privacidade e proteção de dados e reiteradamente reforçadas por diferentes momentos nesta E. Corte, e que impelem os órgãos da administração pública a agirem de forma a proteger - e não vulnerabilizar - a segurança das comunicações de seus cidadãos.

99. Por fim, defenderemos primariamente a inexistência de proporcionalidade e necessidade no uso de tecnologias de intrusão remota, considerando-se o grau de intrusividade e risco de tais medidas em relação aos seus potenciais benefícios para investigações criminais.

100. Nada obstante, subsidiariamente, nos casos em que seja necessária a utilização de ferramentas *spywares*, como única medida possível para a persecução penal, as Autoridades Brasileiras devem se atentar à estrita observância da necessidade e adequação da medida nos casos concretos, com critérios rígidos e tratamento análogo à regulamentação existente para as demais hipóteses de quebra de sigilo, além de regulação acerca da cadeia de custódia da prova, de importância ainda maior pelas próprias características dos mecanismos intrusivos.

101. Aos argumentos elencados acima, iremos dedicar os próximos tópicos desta contribuição.

III.1. O IMPACTO DEMOCRÁTICO DA EXPLORAÇÃO DE VULNERABILIDADES

102. Ao comprarem, adquirirem, ou usarem de qualquer maneira ferramentas de *spyware*, **órgãos estatais exploram uma indústria que cria vulnerabilidades sobre as comunicações e sistemas informacionais de todos os seus cidadãos.**

103. **Tais vulnerabilidades colocam em risco a segurança de usuários e de toda a cadeia de uso da infraestrutura das comunicações.** Isso inclui, também, setores produtivos e essenciais da economia como empresas financeiras[65] e de saúde[66], nos quais a necessidade de segurança no tráfego de informações e de sigilo quanto ao conteúdo transmitido é de importância fulcral para a existência confiável do mercado.

104. Frise-se, portanto, que a falha em se reparar uma vulnerabilidade no sistema não afeta unicamente uma pessoa que esteja sendo investigada de maneira eventual, mas **todo o sistema produtivo que depende da confiança nessas infraestruturas para realizar suas operações.**

105. Por certo, **diante de um cenário normativo-institucional em que vulnerabilidades não só existem, mas são incentivadas pelo Estado - por meio de incentivo financeiro reiterado ao país -, afeta-se também a qualidade do debate público e da confiança nas instituições democráticas.** Primeiro, pela possibilidade de usos por agentes públicos que fujam aos limites da legalidade, ética e proporcionalidade. Segundo, não apenas pela possibilidade fática e material de abusos no âmbito da administração pública, mas também pelos possíveis *efeitos inibidores* que o uso de tecnologias como estas pode acarretar sobre a liberdade de expressão.

106. Os casos recentes ocorridos no Brasil, mencionados anteriormente, evidenciam a primeira possibilidade. **Eles mostram que agentes estatais podem corromper suas atividades funcionais e utilizar tais ferramentas em benefício próprio.**

---

[65]CALLIESS, Christian; BAUMGARTEN, Ansgar. Cybersecurity in the EU the example of the financial sector: a legal perspective. *German Law Journal*, v. 21, n. 6, p. 1149-1179, 2020. Disponível em: https://www.cambridge.org/core/journals/german-law-journal/article/cybersecurity-in-the-eu-the-example-of-the-financial-sector-a-legal-perspective/E74D7AB0D2FDF2B0017BD93BD324267C.

[66]KRUSE, Clemens Scott et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, v. 25, n. 1, p. 1-10, 2017. Disponível em: https://content.iospress.com/articles/technology-and-health-care/thc1263.

107. **Os casos demonstram como o aparato de vigilância do Estado, quando não severamente limitado e condicionado a regras estritas, pode ser desvirtuado.** Em vez de servir para fins institucionais lícitos, como enfrentamento a crimes graves, pode ser usado para objetivos individuais e políticos que ameaçam o Estado Democrático de Direito e os princípios da impessoalidade e da legalidade na Administração Pública.

108. De outro lado, **a legitimação ao uso de ferramentas de monitoramento direcionado impõe um ambiente de desconfiança nas instituições democráticas**.

109. **Quanto a isso, privacidade e liberdade de expressão estão diretamente relacionadas.** A vigilância estatal que emerge sem controle ou justificativa exibe impactos prejudiciais sobre o comportamento humano, influenciando a forma como os indivíduos interagem na sociedade e até mesmo seu estado psicológico. Como argumenta Alan Westin, a privacidade possui relevância de natureza social e política, erigindo-se como um componente crucial nos sistemas democráticos[67]. A ausência de privacidade, por sua vez, implica efeitos nocivos sobre a autonomia individual, política, decisória e de opinião. Assegurar a preservação do direito à privacidade de todos os cidadãos, portanto, se apresenta como incumbência primordial do Estado Democrático de Direito, devendo servir como princípio orientador para todas as atividades estatais que impliquem na coleta e no tratamento de dados.

110. Nesse sentido, **efeitos inibidores relacionados às capacidades de vigilância do Estado sobre a liberdade de expressão têm sido amplamente estudados e evidenciados.**

111. Esta E. Corte já se pronunciou que faz parte do direito à liberdade de expressão "*a capacidade das pessoas de escolherem livremente as informações que pretendem compartilhar, as ideias que pretendem discutir, o estilo de linguagem empregado e o meio de comunicação*"[68]. No entanto, num ambiente de constante risco e medo de que a comunicação seja monitorada por terceiros, "*os cidadãos*

[67] WESTIN, A. F. *Privacy and freedom.* New York: Ig Publishing, 2015, p. 246.
[68] BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 5.527*. Voto Ministra Rosa Weber. 36 páginas. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf .

podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos"[69].

112. Esse fenômeno ficou conhecido pelos efeitos inibitórios (*chilling effects*) que expedientes estatais podem gerar na expressão de toda a comunidade, inclusive dos cidadãos que ainda não foram alvos de vigilância. As suas consequências vão "*desde a desconfiança em relação às instituições sociais, à apatia generalizada e a debilitação da vida intelectual, fazendo de um ambiente em que as atividades de comunicação ocorrem de modo inibido ou tímido*"[70]. A existência de *spywares* em órgãos estatais produz um ambiente intimidatório à comunicação, o que é por si só um dano à liberdade de expressão de milhares de cidadãos.

113. Isso se aplica não apenas quando uma pessoa *sabe* que está sendo vigiada, mas também a quando uma pessoa sabe que *existe a possibilidade de ser vigiada*, sem nunca ter a certeza de quando isso estará acontecendo. Conforme o jurista Daniel Solove:

> Uma razão mais convincente pela qual a vigilância secreta é problemática é que ela pode ter um efeito intimidador sobre o comportamento. Na verdade, pode haver um efeito ainda mais intimidador quando as pessoas estão geralmente cientes da possibilidade de vigilância, mas nunca têm certeza se estão sendo observadas em algum momento específico. [...] Assim, a consciência da possibilidade de vigilância pode ser tão inibitória quanto a vigilância real.[71]

114. O que se vislumbra, no cenário atual, é justamente a possibilidade de compra e utilização de ferramentas de vigilância direcionada, que operam sem que o alvo tenha qualquer ciência do monitoramento remoto ou capacidade de apresentar defesa. **A ausência de parâmetros legais evidentes e de critérios específicos que orientem as atividades das autoridades públicas torna a capacidade de uso dessas ferramentas absolutamente discricionária.**

115. Conquanto os órgãos de defesa e inteligência tenham normativas acerca de suas atividades e conselhos que, ao menos em tese, possuem a função de supervisionar as atividades da Agência, o que se vê na prática é a ausência de

[69] *Ibidem*, p. 10.
[70] *Ibidem*, p. 11.
[71] SOLOVE, Daniel J. A taxonomy of privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, jan. 2006, p. 494-495.

parâmetros normativo-institucionais que forneçam balizas às suas capacidades de investigação[72].

116. De outra parte, uma permissão genérica de compra e uso de tais ferramentas abarca não apenas a União e a Abin, mas também outros entes, como Estados e Municípios, que tenham interesse em adquiri-las. Nestes casos, os limites e a atenção aos parâmetros de legalidade e razoabilidade ficam ainda mais obscuros[73].

117. **Na medida em que esse cenário ocorre e se sustenta cotidianamente, o ambiente democrático já é afetado.** Ativistas políticos, jornalistas, acadêmicos, professores e membros de coletivos ou movimentos sociais tendem a se manter em um estado de suspeição contínua. Isso porque nunca sabem quando, se, e sob quais condições poderiam estar sendo monitorados por opositores políticos que ocupam cargos públicos dos mais diversos níveis da federação.

118. A capacidade de livre opinião, associação e expressão, nesse cenário, fica constantemente à sorte do jogo e da mudança de forças políticas. **Gera-se um ambiente de insegurança coletiva e de desconfiança nas instituições de segurança pública e defesa, nocivo a qualquer democracia moderna que depende também dessas instituições para sua continuidade.**

119. A utilização reiterada de ferramentas de *spywares* por autoridades estatais, portanto, implica em consequências nocivas ao ambiente democrático, seja **(i)** pelo impacto que isso oferece sobre a segurança da infraestrutura de telecomunicações, **(ii)** pelo impacto inibidor sobre a liberdade de expressão e confiança da população em relação às instituições, ou **(iii)** pela possibilidade de tais ferramentas serem facilmente utilizadas para finalidades antidemocráticas, que rompem com os princípios da legalidade e da impessoalidade da administração pública, como diversos casos já apontaram no Brasil e ao redor do mundo.

[72] INTERNETLAB. *O direito das investigações digitais no Brasil*: fundamentos e marcos normativos. São Paulo: InternetLab, 2022. Disponível em: https://internetlab.org.br/wp-content/uploads/2022/10/INTERNETLAB_O-DIREITO-DAS-INVESTIGACOES_PRINT_10-2022.pdf.

[73] AMARAL, P.; CANTO, M.; PEREIRA, M. C. M.; André Ramiro (coord.). *Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil*. Novembro de 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf.

120. O resultado exposto acima impõe que pensemos um dever do Estado de proteção sobre o ambiente informacional, a partir (i) da não utilização de ferramentas de intrusão remota sobre sistemas eletrônicos; (ii) do reconhecimento da ilegalidade na aquisição dessas ferramentas; e, por fim, (iii) do incentivo a políticas de divulgação de vulnerabilidades.

121. Mais do que isso, tais consequências reforçam a necessidade de defesa do direito à integridade dos sistemas informacionais, que decorre diretamente das proteções constitucionais garantidas à privacidade, à proteção de dados e à autodeterminação informativa, de fulcral importância para a manutenção de nosso ambiente democrático. É imperativo o reconhecimento de um direito de integridade dos sistemas informacionais como componente da tradição constitucional brasileira de proteção da dignidade da pessoa humana em um Estado Democrático de Direito, considerando que a autodeterminação informativa é um componente dos direitos da personalidade, como já decidido por esta Suprema Corte. É nesse sentido que o direito à integridade dos sistemas informacionais é reconhecido como um desdobramento da interpretação constitucional sobre o direito à proteção de dados pessoais, conectado com as cláusulas assecuratórias da liberdade e da dignidade da pessoa humana.[74]

III.2. OS DIREITOS FUNDAMENTAIS AO SIGILO DAS COMUNICAÇÕES E À PROTEÇÃO DE DADOS PESSOAIS

122. A Constituição Federal protege os direitos à intimidade, à privacidade, ao sigilo e à proteção de dados pessoais (art. 5º, X, XII e LXXIX).

123. Tais direitos delimitam espaços protegidos, cuja intrusão pelo Estado demanda justificação especial. Nesse sentido, esta Suprema Corte tem corretamente reconhecido que as transformações tecnológicas exigem uma constante reavaliação sobre como direitos fundamentais são afetados e como os valores normativos da Constituição podem ser efetivados à luz das novas mediações das tecnologias da informação. Uma tutela adequada do desenvolvimento livre da personalidade exige evitar a erosão da autonomia individual e a reafirmar os direitos fundamentais.[75]

[74] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *RJLB*, Ano, v. 5, p. 781-809, 2019.
[75] HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*: desafios para o direito. Rio de Janeiro: Forense, 2020.

124. Como bem observado na votação conjunta da ADI 6649 e ADPF 695, em voto do I. Ministro Gilmar Mendes:

> Na era digital, as novas tecnologias de comunicação se tornaram condição necessária para a realização de direitos básicos - como se faz evidente no campo da liberdade de expressão, de manifestação política e religiosa. Contudo, verifica-se que esses mesmos avanços tecnológicos suscitam riscos generalizados de violação de direitos fundamentais básicos. (...) É necessário que, diante das ameaças geradas pelo desenvolvimento da tecnologia, a jurisdição constitucional atue como instrumento de inovação jurídica, visando à constante atualização da tutela dos direitos fundamentais[76].

125. A proteção da privacidade, dita de forma ampla, é essencial para o devido exercício de diversos outros direitos fundamentais. Além disso, o direito à vida privada protege as pessoas do atentado contra o segredo e a liberdade da vida privada. Essa proteção, por sua vez, impede a perturbação de terceiros pela investigação de acontecimentos referentes à vida pessoal e familiar da pessoa e a seus dados pessoais. Como se sabe, o segredo da vida privada sofre ameaças pelas investigações indevidas e ilimitadas em dispositivos eletrônicos, potencializadas pelos instrumentos ora discutidos, os *spywares*.

126. A proteção da privacidade deve ser ainda mais rigorosa nesse caso, em que estamos a lidar com uma ferramenta tecnológica poderosa, que consegue incutir em diversos aspectos da vida do indivíduo, por meio de um monitoramento constante e em tempo real.

127. De fato, em relação aos riscos da utilização da tecnologia em detrimento do direito à privacidade, já afirmava José Afonso da Silva:

> O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.[77]

[76] SUPREMO TRIBUNAL FEDERAL. *ADI 6649 e ADPF 695*. Voto do Ministro Gilmar Mendes, p. 16-17.
[77] SILVA. José Afonso da. *Curso de Direito Constitucional positivo*. 34. ed. São Paulo: Malheiros, 2011, p. 209-2010.

128. Como amplamente discutido pela doutrina, Danilo Doneda leciona que o direito à privacidade não se confunde com o direito autônomo da proteção de dados pessoais, que está associado aos princípios de usos justos da informação e um conjunto de procedimentos que permitem, ao mesmo tempo, habilitar os fluxos de dados pessoais, mas reduzir as assimetrias de poder entre titulares e controladores, por meio de uma série de estratégias de mitigação de riscos e também de estruturas institucionais para aplicação de direitos sobre dados pessoais, como o papel exercido pelas Autoridades de Proteção de Dados Pessoais.[78]

129. Nesse sentido, partindo de uma formulação teórica clássica de Stefano Rodotà, a proteção de dados pessoais relaciona-se menos à "não intrusão" e às liberdades negativas, e relaciona-se mais aos poderes de controle sobre dados pessoais e às liberdades positivas em ambiente democrático.[79]

130. Essa formulação teórica foi muito bem reconhecida pela Suprema Corte no julgamento da ADI 6387 e na ADI 6649. A proteção de dados pessoais localiza-se dentro dos direitos da personalidade e exige, por parte do Estado, um conjunto de obrigações positivas para sua efetivação.

131. Por isso, a Corte corretamente delineou uma dimensão subjetiva aos direitos de proteção de dados pessoais (os direitos sobre dados que podem ser exercidos pelos cidadãos nos termos da Lei Geral de Proteção de Dados Pessoais) e uma dimensão objetiva desses direitos, que implica em um conjunto de salvaguardas e procedimentos administrativos aptos a diminuir riscos excessivos às liberdades e ao livre desenvolvimento da personalidade. A Emenda Constitucional nº 115/2022 sedimentou a diferenciação, apontando a proteção de dados enquanto direito fundamental autônomo no artigo 5º, inciso LXXIX.

132. O STF reconhece, portanto, que há deveres estatais de proteção de valores estruturantes do regime democrático, por meio da criação de salvaguardas institucionais que preservem a essência da cidadania.

[78] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Segunda Edição. Rio de Janeiro: Revista dos Tribunais, 2001. P. 165.
[79] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Segunda Edição. Rio de Janeiro: Revista dos Tribunais, 2019. P. 39.

133. No caso em tela, é fundamental que o Tribunal compreenda como as ferramentas de vigilância operadas pelo Estado afetam o sistema de garantias individuais de forma sistêmica sob a lógica da autodeterminação informativa.

134. Cunhado pelo Tribunal Constitucional Alemão no julgamento da Lei do Censo (*Volkszählungsurteil*), a autodeterminação informacional limita a influência no comportamento de indivíduos a partir do tratamento de dados pessoais. Ela materializa os direitos de personalidade e dignidade da pessoa humana frente a novas tecnologias, assegurando a indivíduos não a propriedade sobre seus dados, mas o controle que titulares têm sobre as informações que terceiros detêm de si.

135. No tratamento de dados pelo poder público e, especialmente, diante das ferramentas de invasão de dispositivos informáticos, a assimetria informacional entre Estado e indivíduos acentuam os riscos à proteção de dados pessoais. Enquanto detentor do monopólio de força coercitiva, as atribuições da administração pública podem, por si só, trazer uma série de violações a garantias constitucionais. O objeto da presente ação destaca ainda mais essa relação de poder, na medida em que a exploração de vulnerabilidades técnicas permite a invasão de dispositivos informáticos sem o conhecimento de seus alvos.

III.3. DO DIREITO À INTEGRIDADE DOS SISTEMAS INFORMACIONAIS COMO EXPRESSÃO DOS DIREITOS CONSTITUCIONAIS À PRIVACIDADE E PROTEÇÃO DE DADOS

136. Em diversos momentos, este Supremo Tribunal Federal teve a oportunidade de perquirir acerca da necessidade de vigilância e capacidades investigativas do Estado, por um lado, e dos direitos fundamentais dos cidadãos, por outro lado.

137. Nessas ocasiões, a Corte tem demonstrado uma forte tendência de reforçar o dever do Estado de não enfraquecer a segurança da comunicação de seus cidadãos e, assim, de assegurar uma infraestrutura democrática do debate público. A seguir citamos alguns exemplos desses casos.

138. Na ADPF 722[80], ocasião em que se discutia a inconstitucionalidade do relatório elaborado pelo Ministério da Justiça e Segurança Pública que identificava um

[80] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 772*. Requerente: Rede Sustentabilidade. Intimado: Ministro de Estado da Justiça e Segurança Pública.

grupo de servidores e professores como integrantes do "movimento antifascismo" sob a alegação de atividade de inteligência[81], a I. Ministra Cármen Lúcia realçou que:

> o serviço de inteligência do Estado, para segurança pública, para a segurança nacional e para a garantia de cumprimento eficiente dos deveres do Estado, é necessário, mas não pode ser desempenhado fora de estritos limites constitucionais e legais, sob pena de comprometer a democracia em sua instância mais central, que é a de garantia dos direitos fundamentais. Daí ser certo que órgãos de inteligência de qualquer nível hierárquico de qualquer dos poderes do Estado submetem-se também ao crivo do Poder Judiciário.[82]

139. A I. Ministra teceu considerações acerca das funções constitucionais de órgãos de inteligência, excluindo do escopo da instituição a elaboração de dossiê que serve para perfilizar e constranger opositores, como o dossiê antifascista:

> As atividades de inteligência, portanto, devem respeitar o regime democrático, no qual não se admite a perseguição de opositores e aparelhamento político do Estado. Aliás, o histórico de abusos relatados quanto ao serviço de inteligência acentua a imperiosidade do efetivo controle dessa atividade[83].

140. E concluiu que:

> É imprescindível que a colheita de dados, a produção de informações e o respectivo compartilhamento entre os órgãos integrantes do Sistema Brasileiro de Inteligência se opere com estrita vinculação ao interesse público, observância aos valores democráticos e respeito aos direitos e garantias fundamentais[84].

Relatora: Ministra Cármen Lúcia. Diário de Justiça Eletrônico. Brasília, 09 jun. 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354.

[81] TEIXEIRA, Lucas Borges. O que é, quem fez e quem está no dossiê antifascista. *Uol explica*, 18 ago. 2020. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2020/08/18/uol-explica-o-que-e-quem-fez-e-quem-atinge-o-dossie-antifascista.htm.

[82] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 772*. Requerente: Rede Sustentabilidade. Intimado: Ministro de Estado da Justiça e Segurança Pública. Relatora: Ministra Cármen Lúcia. Diário de Justiça Eletrônico. Brasília, 09 jun. 2022. p. 4.

[83] *Ibidem*, p. 6.

[84] *Ibidem*, p. 8.

141. Na ADPF 695[85], em que se questionou a constitucionalidade de atos do Poder Público que visavam ao compartilhamento de dados[86] constantes da base do DENATRAN, que engloba informações de 76 milhões de brasileiros, entre órgãos e entidades que não integram o Sistema Brasileiro de Inteligência e a Abin, o I. Ministro Gilmar Mendes defendeu que:

> O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, **a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais**.[87]

142. Já na ADI 6529[88], que teve o objetivo de conferir interpretação conforme ao parágrafo único do art. 4º. da Lei n. 9.883/1999, de modo a **exigir que as solicitações de informações de órgãos do Sistema Brasileiro de Inteligência pela Agência Brasileira de Inteligência sejam acompanhadas de motivação demonstrando a necessidade dos dados pretendidos e a adequação da solicitação às finalidades legais da entidade**, a I. Ministra Relatora Cármen Lúcia fixou a seguinte tese:

> A natureza da atividade de inteligência, que eventualmente se desenvolve em regime de sigilo ou de restrição de publicidade, não afasta a obrigação de motivação dos atos administrativos, especialmente se considerado que esses atos podem importar em acesso a dados e informações sensíveis dos cidadãos, limitando os direitos fundamentais à privacidade e à intimidade.[89]

[85]BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 695*. Requerente: Partido Socialista Brasileiro - PSB. Intimado: União. Relator: Ministro Gilmar Mendes. Diário de Justiça Eletrônico. Brasília, 15 set. 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693.

[86] STF valida compartilhamento de dados mediante requisitos. STF, 15 set. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227&ori=1.

[87] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 695.* Diário de Justiça Eletrônico. Brasília, 15 set. 2022. p. 2.

[88] BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6529*. Requerentes: Rede Sustentabilidade e Partido Socialista Brasileiro - PSB. Intimados: Presidente da República e Congresso Nacional. Relatora: Ministra Cármen Lúcia. Diário de Justiça Eletrônico. Brasília, 22 out. 2021. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837.

[89]*Ibidem*, p. 25.

143. Nas ADIs 6.389, 6.390, 6.393, 6.388 e 6.387[90], em que o Plenário referendou a medida cautelar deferida para suspender a eficácia da Medida Provisória 954/2020. A MP autorizava o compartilhamento de dados de milhões de usuários brasileiros de telefonia fixa e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE). Na ação, a I. Ministra Relatora Rosa Weber **reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional**, destacando que:

> **Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.** Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. (ADI 6.387, p. 16 do acórdão).

144. E concluiu explicitando que:

> (...) não se pode fazê-lo de uma forma que não garanta mecanismos de proteção compatíveis com as cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Assim como o exigir que automóveis sejam providos de freios, *airbags* e espelhos retrovisores não significa criar obstáculos para a indústria automobilística, o exigir que normas que envolvam direitos fundamentais e da personalidade observem requisitos mínimos de adequação constitucional tampouco pode ser lido como embaraço à atividade estatal. (ADI 6.387, p. 28 do acórdão).

145. Vê-se, portanto, que **ao longo de anos, esta E. Corte tem se manifestado no sentido de não apenas reconhecer o direito autônomo à proteção de dados pessoais e à autodeterminação informativa, mas também de condicionar as atividades do Estado à garantia desses direitos e ao não enfraquecimento do ambiente de informação e comunicação de seus cidadãos**.

---

[90] BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6387*. Requerente: Conselho Federal da Ordem dos Advogados do Brasil - CFOAB. Intimado: Presidente da República. Relatora: Ministra Rosa Weber. Diário de Justiça Eletrônico. Brasília, 12 nov. 2020. Tramitaram em conjunto por determinação da relatora, pois ambas buscavam impugnar a validade constitucional da Medida Provisória nº 954/2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165.

146. No debate sobre criptografia, esta também é, até o momento, a interpretação que tem prevalecido.

147. No Brasil, o questionamento da constitucionalidade da quebra da criptografia começou a ser aventado entre 2015 e 2016, período em que o aplicativo WhatsApp foi alvo de quatro bloqueios por ordens judiciais ao redor do país[91]. Nesses casos, a argumentação gravita em torno de recusas da empresa em atender pedidos judiciais de acesso a dados de seus usuários. Então, no mesmo ano, a fim de discutir a questão jurídico-constitucional controvertida, pano de fundo dos bloqueios, figuram, ao menos, duas ações no STF (ADPF 403[92] e ADI 5527[93]).

148. Aqui, registramos que ministros desta E. Corte fizeram contribuições de extrema relevância para a temática. Os julgamentos da ADPF e da ADI estão ocorrendo conjuntamente e os votos dos relatores, Ministro Edson Fachin e Ministra Rosa Weber, respectivamente, trazem ensinamentos para a tratativa jurídico-constitucional da questão dos *spywares*. Tais contribuições são importantes, pois oferecem interpretações a direitos que são centrais para o presente caso e não reproduzem simplificações reducionistas do problema. A seguir expomos brevemente o cenário das ações sobre criptografia, uma síntese dos argumentos dos votos publicados até o momento e, por fim, como tais argumentos podem auxiliar na elucidação do presente caso.

149. Em síntese, ambas as ações se referem à extensão do art. 12 do Marco Civil da Internet, embora sob diferentes contornos[94]. No entanto, a questão jurídica

[91] G1. *WhatsApp já foi bloqueado por decisão judicial em 2015 e 2016 no Brasil*. 18 mar. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/03/18/whatsapp-ja-foi-bloqueado-por-decisao-judicial-em-2015-e-2016-no-brasil.ghtml.

[92] BRASIL. Supremo Tribunal Federal. *Ação de Descumprimento de Preceito Fundamental n.º 403*. Requerente: Cidadania. Intimado: Juiz de Direito da Vara Criminal da Comarca de Lagarto. Relator: Ministro Edson Fachin. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500..

[93] BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 5.527*. Requerente: Partido da República. Intimados: Presidente da República e Congresso Nacional. Relatora: Ministra Rosa Weber. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282.

[94] Discute-se se o artigo 12 diz apenas respeito ao descumprimento das normas de proteção de registros, dados pessoais e comunicações privadas previstas nos Artigos 10 e 11 ou se sua interpretação se estende também ao descumprimento de ações judiciais que pedem acesso a dados pessoais para fins de persecução penal. A ADPF 403 questiona uma das decisões que bloqueou o WhatsApp e requer que o STF proíba ordens judiciais que visam suspender serviços de mensageria privada, como o WhatsApp, sob o fundamento de que tais atos violam o "*direito à comunicação de milhares de*

controvertida mediata, e que nos interessa para a presente contribuição, é a interpretação do direito constitucional à privacidade e ao devido processo legal e, assim, às garantias devidas ao cidadão no âmbito das investigações sobre comunicações digitais no Brasil. Em seguida, faremos um breve recorte das contribuições dos votos dos ministros Rosa Weber e Edson Fachin, nas ADI 5527 e na ADPF 403, respectivamente. Aqui, o foco será especialmente nos argumentos que os ministros elaboraram acerca das responsabilidades do Estado em relação à infraestrutura das telecomunicações e sistemas informacionais.

150. Em seu voto[95] no julgamento da ADI 5527, a I. Relatora e ex-Ministra desta E. Corte, Rosa Weber, reconhece a virtualização da privacidade dos indivíduos e equipara os dispositivos móveis, por exemplo, a "*janelas luminosas para a nossa intimidade*"[96]. Weber defende que os celulares "*guardam muito mais da vida privada e intimidade de seus proprietários do que as portas e paredes, gavetas e armários da residência de cada um deles, e a inviolabilidade do domicílio não temos dificuldade alguma em reconhecer.*"[97]

151. Diante do quadro legislativo e jurisprudencial de salvaguarda de direitos, a Ministra, acertadamente, decide que o Estado não tem o poder de obrigar empresas que "*prestem serviços de comunicações privadas a adotarem mecanismos que assegurem o acesso ao conteúdo das conversas*"[98] e, assim, enfraqueçam a sua criptografia. Weber vai além e defende que a criptografia tem exercido papel central na efetiva proteção dos direitos humanos como a liberdade de expressão e a privacidade, mas também a própria segurança. Segundo a I. Ministra:

> O *trade-off* aqui, portanto, não se dá entre segurança pública e privacidade, pois a pretensão que ameaça a privacidade, ainda que fundada no combate a uma ameaça

cidadãos". Por sua vez, a ADI 5527 requer a inconstitucionalidade do artigo 12, III e IV do Marco Civil da Internet, que prevê sanções de suspensão e proibição de exercício de atividades a plataformas e serviços de internet, e também requer que apenas decisões em persecução penal possam possibilitar a quebra de sigilo das comunicações nessas plataformas.

[95]BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 5.527*. Voto Ministra Rosa Weber. 36 páginas. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf .

[96]BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 5.527*. Voto Ministra Rosa Weber. 36 páginas. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf, p. 6.

[97]*Ibidem*, p. 7.

[98]*Ibidem*, p. 27.

> imediata à segurança, vulnera, no longo prazo, também a segurança das redes e seus usuários como um todo, expondo-os a maiores riscos de ciberataques, fraudes, roubos de identidade, invasão da intimidade extorsão etc.[99]

152. Por sua vez, na ADPF 403[100], o I. Ministro Relator Edson Fachin acompanhou, em grande medida, os argumentos e conclusões da Ministra Rosa Weber. Cabe ressaltar, inclusive, que ambas as ações tiveram contribuições da mesma audiência pública[101].

153. O I. Ministro Fachin faz uma síntese de seu voto a partir das sete premissas basilares da argumentação. As cinco primeiras premissas reafirmam as defesas de que: i) os avanços tecnológicos devem ser acompanhados por uma atualização do alcance e garantia dos direitos fundamentais; ii) os direitos se estendem ao mundo digital; iii) o direito à privacidade e à liberdade de expressão são condições para o pleno exercício do acesso à internet; iv) a privacidade é o direito de manter o controle sobre a sua informação e de determinar a maneira de construir sua própria esfera pública; v) a liberdade de expressão constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito[102].

154. A sexta e a sétima premissas dizem diretamente sobre a centralidade da proteção da segurança e integridade dos sistemas comunicacionais para proteger direitos fundamentais como privacidade e liberdade de expressão.

155. O Ministro destaca que a criptografia, assim como o anonimato, são garantidores no desenvolvimento e compartilhamento de opiniões, guardando estreita relação com a liberdade de expressão. Ainda, defende que é contraditório que "*em nome da segurança pública, deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado*."[103] Em sua última

---

[99] *Ibidem*, p. 31.

[100] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental n.º 493*. Voto Ministro Edson Fachin. 76 páginas. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf .

[101] InternetLab. *Audiência Pública sobre Criptografia e Bloqueios do WhatsApp*: argumentos diante do STF. ABREU, Jacqueline. 29 jun. 2017, Disponível em: https://internetlab.org.br/pt/noticias/audiencia-publica-sobre-criptografia-e-bloqueios-whatsapp-argumentos-diante-stf/.

[102] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental n.º 493*. Voto Ministro Edson Fachin. 76 páginas. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf, p. 1-2.

[103] I*bidem*, p. 2.

premissa, o Ministro Fachin dissolve o falso dilema entre segurança e privacidade, e argumenta que o enfraquecimento da criptografia também ofende o dever de segurança do Estado. Assim, o Ministro decide por julgar procedente a ADPF para:

> declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, de modo a **afastar qualquer interpretação** do dispositivo **que autorize ordem judicial que exija acesso excepcional** a conteúdo de mensagem criptografada ponta-a-ponta **ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet.**[104]

156. Ambos os votos nos permitem argumentar que temos um direito à integridade e segurança na utilização de sistemas informáticos e comunicacionais.

157. A proteção de dados pessoais é um pressuposto do engajamento dos indivíduos em questões públicas e pressuposto funcional da comunicação democrática. Conforme doutrina do direito constitucional, as regras de proteção de dados pessoais e integridade dos sistemas informáticos criam condições de continuidade do Estado Democrático de Direito. Como reconhecido pelo professor Fabiano Menke, "*o direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais atualiza a proteção da personalidade à realidade tecnológica do século XXI*"[105], conectando-se com as normas constitucionais de proteção da dignidade da pessoa humana e a liberdade. O reconhecimento desse direito opera como uma barreira normativa, considerando que sua restrição só pode ocorrer diante de postulados claros de proporcionalidade, adequação e necessidade.

158. **Conclui-se, desse modo, que o Estado não só é proibido de vulnerabilizar esses sistemas, como tem o dever de protegê-los e aprimorá-los. Por essa mesma razão, a utilização de tecnologias de intrusão remota deve ser considerada inconstitucional, tendo em vista a corrosão que causa na segurança e integridade dos sistemas comunicacionais e dos direitos dos usuários.**

[104]BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental n.º 493*. Voto Ministro Edson Fachin. 76 páginas. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf, p. 73.

[105] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *RJLB*, Ano, v. 5, 2019, p. 801-802.

IV. DA ANÁLISE DA NECESSIDADE E PROPORCIONALIDADE NO USO DE *SPYWARES* NAS INVESTIGAÇÕES CRIMINAIS

159. Uma vez defendida a existência de um direito autônomo à integridade dos sistemas informacionais, que impele o Estado ao dever de não adquirir tecnologias de intrusão remota, passamos em seguida à consideração a respeito do uso de tais ferramentas diante das normas constitucionais, infraconstitucionais e garantias do direito processual penal.

160. **Defendemos, neste tópico, que não há equilíbrio entre necessidade e proporcionalidade no uso de ferramentas de intrusão remota e que, mesmo que se considere o sopesamento necessário, as salvaguardas legais hoje existentes em relação à quebra de sigilo de dados e interceptações não são suficientes para dar amparo à utilização dessas ferramentas.**

IV.1. QUEBRA DO SIGILO DE DADOS: FUNDAMENTOS E LIMITES

161. É certo que a quebra de sigilo é possível no direito brasileiro, mas deve ela respeitar balizas legais expressamente estabelecidas. Nosso ordenamento jurídico prevê diferentes e específicos procedimentos para que as autoridades públicas acessem dados pessoais no âmbito de investigações criminais. Trata-se de relevantes restrições legais, com vistas a dar concretude aos direitos fundamentais constitucionalmente previstos.

162. Nesse sentido, e em primeiro lugar, a Lei das Interceptações Telefônicas (Lei nº 9.296/1996) permite a "*interceptação do fluxo de comunicações em sistemas de informática e telemática*" em determinadas hipóteses, proibindo-a caso não haja "*indícios razoáveis de autoria ou participação em infração penal*" (art. 2º, I).

163. Da mesma forma, o Código de Processo Penal (CPP) prevê a possibilidade de obtenção de dados de localização referentes a crime de tráfico de pessoas[106] em curso, de forma que se permita a localização da vítima e dos suspeitos, e, no caso da

[106] "Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados - como sinais, informações e outros - que permitam a localização da vítima ou dos suspeitos do delito em curso."

Lei de Interceptações Telefônicas, a possibilidade de acesso às referidas comunicações em determinados casos, desde que demonstrados indícios razoáveis de autoria do crime que se quer investigar.

164. Mais ainda, as Leis de Lavagem de Dinheiro (Lei nº 9.613/1998, alterada pela Lei nº 12.683/2012) e da Organização Criminosa (Lei nº 12.850/2013) dispõem sobre a necessidade de autorização judicial específica para a obtenção de dados do investigado que ultrapassem a sua qualificação pessoal, filiação e endereço. Uma vez mais, as distintas legislações foram se somando à interpretação consagrada do texto constitucional de restrição às intrusões nas vidas dos cidadãos.

165. Conforme consta das redações do art. 17-B da Lei nº 9.613/1998 e do art. 15 da Lei nº 12.850/2013, as autoridades investigadoras terão acesso, independentemente de autorização judicial, apenas "*aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito*". *A contrario sensu*, portanto, as demais formas de dados serão obtidas apenas com ordem judicial específica, que enfrente e explique a necessidade daquela medida extrema de quebra de sigilo de dados.

166. Na sequência, o Marco Civil da Internet, reconhecendo a proteção da privacidade e do sigilo de dados como princípios gerais da internet e como direitos dos usuários (arts. 3º, 7º, e 8º), permite o fornecimento de registros de conexão (art. 5º, VI) e de acesso a aplicações (art. 5º, VIII) de usuário envolvido em ato ilícito praticado pela internet, mas exige, de maneira expressa, ordem judicial baseada em fundados indícios de ato ilícito e justificativa motivada da utilidade dos dados requeridos (art. 22).

167. Ou seja, nas circunstâncias excepcionais em que o interesse público se sobrepõe ao interesse privado da inviolabilidade das comunicações ou, ainda, do sigilo de dados, inerentes ao direito à privacidade constitucionalmente tutelado, faz-se necessária a obtenção de ordem judicial específica, fundamentada e individualizada. Trata-se de condição incontornável para a realização da excepcional medida de quebra de sigilo de tais dados constitucionalmente protegidos.

168. Como se percebe, nenhuma das hipóteses previstas na legislação brasileira admite a possibilidade de intrusão remota em dispositivos eletrônicos. Pelo contrário: o ordenamento pátrio estabelece uma relação necessária entre uso de dados pessoais em investigações, de um lado, e elementos que demonstrem o potencial envolvimento do indivíduo afetado em atividades ilegais, de outro.

IV.2. DA AUSÊNCIA DE NECESSIDADE E PROPORCIONALIDADE NO USO DE FERRAMENTAS DE *SPYWARE* NAS INVESTIGAÇÕES CRIMINAIS

169. A partir do tópico acima, temos a conclusão de que **toda interceptação, requisição, compartilhamento e quebra de sigilo de dados deve ter fundamentação clara, tanto no respeito à estrita letra da lei quanto na justificativa a que se chega** após efetivo sopesamento entre o interesse público na investigação criminal e os sensíveis riscos que se apresentam aos direitos e liberdades fundamentais do titular dos dados pessoais.

170. Nesse sentido, deve-se ressaltar a adesão do Brasil ao Pacto de Direitos Civis e Políticos (PIDCP) e à Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), diplomas que protegem os direitos de todos à opinião e liberdade de expressão, garantindo proteção contra ingerências arbitrárias e abusivas na vida privada. Tal proteção se estende às comunicações privadas e aos dados associados a tais comunicações.

171. Quaisquer restrições a esses direitos, conforme o art. 19 do Pacto e de definição da própria Corte Interamericana de Direitos Humanos[107], devem obedecer a um teste tripartite que exige, no mínimo, atendimento aos seguintes critérios: **(a) devem estar legalmente definidas e limitadas, (b) devem atender a critérios de necessidade e proporcionalidade e (c) quando necessárias para alcançar um objetivo legítimo,** que envolva a segurança nacional, a ordem pública, a saúde pública ou os costumes.

172. Sendo assim, o Estado tem o ônus de provar uma conexão direta e imediata entre uma possível ameaça e a consequente restrição a direitos, bem como

[107] A aplicação do teste tripartite à verificação da legitimidade de ingerências à privacidade no âmbito das comunicações foi afirmada pela Corte Interamericana de Direitos Humanos (Corte IDH) nos casos Tristán Donoso *vs* Panamá e Escher e outros *vs* Brasil.

de impor o instrumento menos intrusivo entre aqueles que podem alcançar a mesma função protetora.

173. Como ressaltado pela Ministra Carmen Lúcia em seu voto nas Ações Diretas de Inconstitucionalidade n. 6.387, 6.388, 6.389, 6.390, 6.393[108]:

> Em caso de restrição ao direito à privacidade, o Direito Internacional dos Direitos Humanos exige seja determinado o limite legalmente definido, apenas se legitimando se for para alcançar objetivo legítimo (...), e desde que se qualifique como necessária e proporcional ao objetivo buscado.[109]

174. Ao detalhar os requisitos de necessidade e proporcionalidade no Parecer Consultivo OC-5/85[110], a Corte Interamericana de Direitos Humanos destacou que não é suficiente demonstrar que a restrição cumpre um propósito útil ou oportuno, mas deve ser justificada de acordo com um objetivo legítimo que prepondere claramente sobre a necessidade social do pleno gozo do direito e não limite mais do que estritamente necessário o direito protegido.

175. No que toca ao acesso a dados associados às comunicações, Relatores Especiais para a Liberdade de Expressão das Nações Unidas e da Comissão Interamericana de Direitos Humanos (CIDH) repetidamente salientaram que a

[108] Tramitaram em conjunto por determinação da relatora Min. Rosa Weber, pois ambas buscavam impugnar a validade constitucional da Medida Provisória nº 954/2020.

[109]BRASIL. Superior Tribunal Federal (Plenário). *Ação Direta de Inconstitucionalidade 6.387*. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *FUMUS BONI JURIS*. *PERICULUM IN MORA*. DEFERIMENTO. Relatora: Min. Rosa Weber, 07 de maio de 2020. Lex. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629..

[110]CORTE INTERAMERICANA DE DIREITOS HUMANOS. Parecer Consultivo OC-5/85. O registro obrigatório de jornalistas (artigos 13 e 29 da Convenção Americana sobre Direitos Humanos). 13 nov. 1985. Disponível em: https://www.corteidh.or.cr/docs/opiniones/seriea_05_por.doc.

vigilância massiva não atende ao requisito da proporcionalidade, mesmo que sirva a um propósito legítimo (ONU, A/HRC/27/37)[111]; CIDH/RELE/INF.17/17)[112].

176. Nesse sentido, cabe questionar quando, e se, a utilização de ferramentas de vigilância direcionada pelo Estado poderia ser considerada proporcional diante do crivo do direito humanitário. Isto é: considerando-se que a existência de lei e de ordem judicial seriam parâmetros mínimos para a possibilidade de utilização dessas ferramentas, seria possível pensar em objetivos legítimos que justificassem a consideração dessas medidas como necessárias e proporcionais em casos excepcionais?

177. Frise-se, aqui, que ferramentas de *spyware* estão entre os instrumentos mais intrusivos à disposição do Estado. A possibilidade de acesso remoto a um dispositivo eletrônico sem conhecimento do usuário não deve ser simplesmente equiparada à interceptação telefônica ou à invasão de um domicílio, uma vez que o grau de intrusividade da medida sobre a vida privada pode ser, inclusive, considerado pior[113]. Informações de um dispositivo eletrônico podem revelar aspectos profundos da identidade digital de seu titular, desde sua moradia a seus costumes, renda, pessoas com quem se encontra etc. Assim, compõem e formam um retrato abrangente e particular da vida privada de um indivíduo: seus hábitos de vida, interesses, preferências, associações familiares, políticas, profissionais, religiosas e sexuais podem ser revelados ou inferidos.

178. Não bastasse a extensão do poder de vigilância nesses casos, invasões do tipo são capazes de permitir que o agente de investigação use o aparelho como se fosse o investigado, o que é capaz de comprometer severamente a confiabilidade da

[111]RELATÓRIO DO ESCRITÓRIO DO ALTO COMISSARIADO DAS NAÇÕES UNIDAS PARA OS DIREITOS HUMANOS. *O direito à privacidade na era digital.* UN Doc. A/HRC/27/37, 30 jun. 2014. Trad. Instituto de Referência em Internet e Sociedade. p. 12. Disponível em: https://irisbh.com.br/wp-content/uploads/2022/12/O-direito-a-privacidade-na-era-digital-Relatorio-do-Gabinete-do-Alto-Comissariado-das-Nacoes-Unidas-para-os-Direitos-Humanos.pdf.

[112]RELATORIA ESPECIAL PARA A LIBERDADE DE EXPRESSÃO DA ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Mandados do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão e do Relator Especial para a liberdade de expressão da Comissão Interamericana de Direitos Humanos. OEA CIDH/RELE/Art. 41/7-2020/65. 3 jul. 2020. Disponível em:https://www.oas.org/es/cidh/expresion/documentos_basicos/PORTCARTAONUCIDHBRASILINTERNET2020.pdf.

[113]ANTONIALLI, Dennys. ABREU, Jacqueline. *E quando o policial vira hacker?.* INTERNETLAB, 17 jul. 2017, Disponível em: https://internetlab.org.br/pt/noticias/e-quando-o-policial-vira-hacker/.

prova que se resulte deste meio[114] e, portanto, cria desafios para a preservação da cadeia de custódia.

179. Há, na atualidade, inúmeras outras técnicas e ferramentas de investigação à disposição do Estado, menos gravosas que a invasão direta a um dispositivo eletrônico. Diante do avanço de tecnologias de informação e comunicação, e da profusão de meios de obtenção de provas digitais, é possível identificar a autoria de crimes por meios ordinários de investigação, em especial por procedimentos menos restritivos de direitos.

180. Nesse sentido, não parecem existir casos excepcionais que justifiquem a adoção de uma medida de tamanha intrusividade como uma ferramenta de *spyware*. Não há, portanto, razoabilidade em se supor que a utilização de *spywares* seria "necessária e proporcional" em qualquer caso.

181. Ainda que se considere que um sopesamento entre riscos e benefícios deverá ser feito casuisticamente, fato é que nosso quadro normativo atual não está suficientemente adequado para dar amparo à utilização de tais ferramentas sem que elas arrisquem gravemente o ambiente democrático e os direitos e liberdades civis de todos os cidadãos brasileiros.

182. Dessa forma, conclui-se pela inconstitucionalidade do uso de ferramentas do tipo *spyware* pelo Estado. Com efeito, evidenciou-se que essas ferramentas têm como corolário a compra e venda de vulnerabilidades na segurança da informação de todos os cidadãos de sociedades democráticas. Assim, os direitos fundamentais de privacidade, segurança de comunicações, imagem, entre outros, são violados. De tal modo, não é possível que o Estado adquira qualquer tipo de tecnologia de intrusão remota, na medida em que há uma grave ameaça do Estado Democrático de Direito. Deve-se, por outro lado, defender o direito à integralidade dos sistemas informacionais, ideia esta que é conforme as garantias constitucionais.

[114] ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (coord.). *O direito das investigações digitais no Brasil: fundamentos e marcos normativos*. São Paulo: InternetLab, 2022. p.73. Disponível em: https://internetlab.org.br/wp-content/uploads/2022/10/INTERNETLAB_O-DIREITO-DAS-INVESTIGACOES_PRINT_10-2022.pdf

V. DA RESIDUAL HIPÓTESE DESTA E. CORTE DECIDIR PELA NECESSIDADE DO USO DE FERRAMENTAS SPYWARES

183. Subsidiariamente, na hipótese em que esta C. Suprema Corte não entenda pela inconstitucionalidade do uso de *spywares* pelo Estado, a despeito dos vastos argumentos tecidos acima, faz-se imprescindível a demarcação de uma disciplina específica que faça frente ao uso indiscriminado dessas tecnologias, a fim de conferir proteção adequada e eficiente aos direitos fundamentais atingidos por tais mecanismos.

184. Esta disciplina constitucional para utilização de ferramentas de intrusão virtual remota deve considerar o seguinte, ao menos: (i) a necessidade de decisão judicial prévia e de respeito à rigidez similar às demais situações de quebra de sigilo; (ii) a interpretação constitucional sobre o sigilo das comunicações atualizada aos padrões de intrusividade contemporâneos; (iii) inclusão de mecanismos de respeito à cadeia de custódia; (iv) a individualização de sujeitos à procedimento de intrusão; (v) a construção de demais parâmetros compatíveis com a ordem constitucional. Tais elementos dessa disciplina devem inclusive constar em qualquer injunção realizada ao Congresso Nacional, por decorrerem diretamente da leitura constitucional adequada às situações consideradas neste caso.

V.1. DA NECESSIDADE DE DECISÃO JUDICIAL PRÉVIA E DE RIGIDEZ EQUÂNIME ÀS DEMAIS SITUAÇÕES DE QUEBRA DE SIGILO E DEMAIS PARÂMETROS CONFORMES ÀS PREVISÕES JÁ EXISTENTES NO ORDENAMENTO JURÍDICO

185. Decerto, em um Estado Democrático de Direito, como é o brasileiro, não se pode conceber a utilização de ferramentas de intrusão virtual remota sem que haja decisão judicial prévia que demonstre a necessidade, adequação e proporcionalidade da medida, de modo a salvaguardar as garantias à intimidade, à privacidade e ao sigilo dos dados e das comunicações. Pelo contrário, estar-se-á reduzindo, de forma injustificada e arbitrária, o nível de proteção dos direitos fundamentais.

186. Com efeito, considerando o impacto que proporciona na vida dos indivíduos e os efeitos para o exercício de direitos e liberdades fundamentais em um Estado Democrático de Direito, é indiscutível que o uso de *spywares* deve obedecer a certos critérios: i) sujeição à lei específica; ii) cumprimento de requisitos rigorosos, em tratamento análogo à regulamentação existente para as demais hipóteses de

quebra de sigilo; iii) estipulação de prazo razoável de duração (com previsão de prorrogação ou não); iv) individualização dos alvos da medida; v) direcionamento exclusivo para investigação criminal e instrução processual penal; vi) preservação da cadeia de custódia, dentre outras especificações.

187. Nesse sentido, é possível vislumbrar, na legislação nacional vigente, um arcabouço normativo que pode ser utilizado como base para a fixação de uma regulamentação própria que disponha sobre o uso de programas de intrusão virtual remota e ferramentas de monitoramento secreto e invasivo, com o objetivo de estabelecer exigências e formalidades necessárias a esse tipo de atividade.

188. A Lei n. 9.296/1996, por exemplo, ao disciplinar a interceptação de comunicações telefônicas, determina que a medida depende de autorização judicial fundamentada, bem como estabelece exigências mínimas que também podem nortear o balizamento a ser instituído concernente à matéria em apreço. Veja-se:

> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I – não houver indícios razoáveis da autoria ou participação em infração penal;
> II – a prova puder ser feita por outros meios disponíveis;
> III – o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.
> Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:
> I – da autoridade policial, na investigação criminal;
> II – do representante do Ministério Público, na investigação criminal e na instrução processual penal.

189. Além disso, determina que a medida não poderá ultrapassar o prazo de quinze dias, sendo que, para a sua renovação - por igual tempo -, é necessária a comprovação da indispensabilidade do meio de prova (art. 5º).

190. Cabe destacar, também, as introduções feitas pela Lei n. 13.964/2019, em relação à captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, com aplicação subsidiária das regras da interceptação telefônica e telemática. Conforme a regulação específica, o requerimento da medida deve conter a descrição circunstanciada do local e da forma de instalação do dispositivo de captação

ambiental. Outrossim, deve haver a demonstração de que a prova ou informação que se pretende obter não pode ser alcançada por outros meios de prova, não podendo a captação durar mais de quinze dias, renovável mediante nova decisão judicial fundamentada. Confira-se:

> Art. 8º-A. Para investigação ou instrução criminal, poderá ser autorizada pelo juiz, a requerimento da autoridade policial ou do Ministério Público, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, quando: (Incluído pela Lei nº 13.964, de 2019)
> I – a prova não puder ser feita por outros meios disponíveis e igualmente eficazes; e (Incluído pela Lei nº 13.964, de 2019)
> II – houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a 4 (quatro) anos ou em infrações penais conexas. (Incluído pela Lei nº 13.964, de 2019)
> § 1º O requerimento deverá descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental. (Incluído pela Lei nº 13.964, de 2019)
> § 2º A instalação do dispositivo de captação ambiental poderá ser realizada, quando necessária, por meio de operação policial disfarçada ou no período noturno, exceto na casa, nos termos do inciso XI do caput do art. 5º da Constituição Federal. (Incluído pela Lei nº 13.964, de 2019) (Vigência)
> § 3º A captação ambiental não poderá exceder o prazo de 15 (quinze) dias, renovável por decisão judicial por iguais períodos, se comprovada a indispensabilidade do meio de prova e quando presente atividade criminal permanente, habitual ou continuada. (Incluído pela Lei nº 13.964, de 2019)
> § 4º A captação ambiental feita por um dos interlocutores sem o prévio conhecimento da autoridade policial ou do Ministério Público poderá ser utilizada, em matéria de defesa, quando demonstrada a integridade da gravação.(Incluído pela Lei nº 13.964, de 2019)(Vigência)
> § 5º Aplicam-se subsidiariamente à captação ambiental as regras previstas na legislação específica para a interceptação telefônica e telemática. (Incluído pela Lei nº 13.964, de 2019)

191. Outra questão de grande relevância, que merece ser destacada, é o descarte de provas, notadamente quando, através da medida, são obtidas informações de terceiros, ou até mesmo dos próprios investigados, mas que envolvem dados irrelevantes para o objetivo pretendido pela atividade investigativa e fiscalizatória, e que podem comprometer demasiadamente a esfera privada dos indivíduos atingidos, dada sua sensibilidade. Nessas situações, as informações obtidas devem ser preservadas apenas de forma parcial, descartando-se tudo aquilo que não for útil e necessário, sempre com supervisão dos órgãos de controle. É o que preceitua o art. 9º da citada legislação federal:

> Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.
> Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.

192. Não é despiciendo registrar, ademais, a previsão contida no art. 8º da Lei n. 9.296/1996, a qual determina a necessidade de preservação do sigilo das diligências, gravações e transcrições com base nela determinadas.

193. Nesse microssistema normativo que visa à proteção dos dados e comunicações, também é possível extrair demarcações importantes estabelecidas pela Lei n. 12.965/2014 (Marco Civil da Internet), tais como requisitos mínimos parao requerimento judicial de afastamento do sigilo dos registros de conexão ou de acesso a aplicações de internet. Nos termos do art. 22 da legislação, a autoridade investigante, para requerer acesso a dados telemáticos, com o fito de angariar conjunto probatório em processos criminais, deverá demonstrar fundados indícios da ocorrência do delito, justificando de forma motivada a utilidade dos registros solicitados, assim como delimitando o respectivo período ao qual se referem.

194. Ademais, em que pese a inaplicabilidade da Lei 13.709/2018 (Lei Geral de Proteção de Dados) às atividades de investigação e repressão de infrações penais (art. 4º, III, d), sua base principiológica é de essencial relevância para assegurar garantias constitucionais relacionadas ao manejo de dados pessoais, na medida em que prevê a observância aos princípios da finalidade, adequação, necessidade, segurança, prevenção, dentre outros (art. 6º).

195. De todo modo, o que se pretende revelar é que a ausência de um arcabouço normativo próprio para tutelar o uso dos *spywares*, com imposição de limites, requisitos, procedimentos e processos legais, macula a segurança jurídica e a proteção eficiente de direitos fundamentais relacionados à intimidade e privacidade, dando espaço para que abusos sejam cometidos por parte dos órgãos e autoridades de investigação, em detrimento de garantias constitucionalmente asseguradas.

V.2. INTERPRETAÇÃO CONSTITUCIONAL SOBRE O SIGILO DAS COMUNICAÇÕES ATUALIZADA AOS PADRÕES DE INTRUSIVIDADE CONTEMPORÂNEOS

196. Ocorre que determinar **o mero requerimento de ordem judicial para casos de intrusividade virtual remota é medida insuficiente para garantir rigidez constitucional equânime aos demais mecanismos de quebra de sigilo** - em especial porque a interpretação constitucional deve ter como parâmetro a proteção maior justamente nos casos nos quais é maior o potencial de lesão a direito fundamental.

197. Na prática, a intrusão remota a dados armazenados em dispositivo eletrônico, por exemplo, implica devassa muito mais significativa sobre as informações da vida de uma cidadã ou um cidadão do que a captura de um trecho de conversa telefônica. Estar-se-á falando de todas as conversas possivelmente realizadas em um aplicativo de mensagens, todas as mensagens de correio eletrônico trocadas, a localização do sujeito e muitas outras informações.

198. Assim, a legislação que regulamenta as condições de quebra de sigilo deve ser interpretada com atenção às condições contemporâneas de evolução tecnológica das comunicações. Dessa maneira, esta E. Corte dará consequência completa aos mandamentos constitucionais de proteção da vida privada e da intimidade (inciso X do artigo 5º da Constituição) e do sigilo (inciso XII do artigo 5º da Constituição), frente ao rápido desenvolvimento tecnológico.

199. Com este fim, desde logo cabe indicar a inadequação do binômio "em fluxo - estáticos" para descrever adequadamente a transmissão de dados na internet e, em consequência, para constituir um critério de (des)proteção. Portanto, deve ser aplicada a proteção estabelecida no inciso XII do artigo 5º da Constituição Federal, da qual deriva a maior proteção oferecida, por exemplo, pela já citada Lei n. 9.296/1996.

200. O paralelo com as comunicações telefônicas e telegráficas não tem se revelado adequado para endereçar os riscos associados a comunicações de dados, que podem ser compreendidas como a transferência de sinais, mensagens escritas, imagens, sons, dados ou inteligência - não necessariamente componentes de um processo comunicativo entre sujeitos - por um sistema eletrônico.

201. Diferentemente de uma carta, cuja entrega delimita o termo final da transmissão, e cuja guarda assume uma dimensão espacial, o fim da transmissão de

dados é frequentemente arbitrário e, quanto ao seu conteúdo, também reversível, diante da possibilidade posterior de edição. O armazenamento de dados por um dispositivo (remoto ou não) se afasta, nesse sentido, de uma noção de conservação estática. Este argumento é fruto de atualização de todo um campo de estudos que dá sinais claros de desenvolvimento, sendo certo que um até então defensor de tal posição de menor proteção de dados "estáticos" perante esta Corte, o professor Tercio Sampaio Ferraz Júnior, recentemente reviu seus posicionamentos em Congresso organizado pelo InternetLab. Veja-se trecho particularmente elucidativo:

> "Importante perceber, nessa esteira, que a confluência tecnológica – caso ostensivo do celular – acabou, então, por alterar a percepção tradicional no que se refere à relação entre fluxo e dados armazenados. Basta ver, hoje, a facilidade com que se copia e cola no fluxo mesmo da comunicação. Por isso, para sua compreensão, entra inevitavelmente uma ponderação entre o direito individual à livre comunicação (liberdade de e direito à informação) e o valor atribuível à promoção da segurança pública (inviolabilidade do sigilo). Particularmente isso afeta a hipótese de uma autorização judicial para qualquer acesso privilegiado de parte de um agente estatal (investigação criminal), que deve, então, levar em conta a possibilidade de uma vulnerabilidade ao sistema comunicacional no contexto da inviolabilidade à comunicação em termos de um conteúdo privado/social, indivíduos nucleares em sistema de acesso. Nesse sentido, a garantia de um direito fundamental à confidencialidade e integridade dos sistemas significa para os usuários que a ruptura da esfera de intimidade de qualquer pessoa, quando ausente a hipótese configuradora de causa provável revela-se incompatível com o modelo consagrado na Constituição da República, pois a quebra de sigilo não pode ser manipulada, de modo arbitrário pelo Poder Público. **Não fosse assim, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada, que daria, ao Estado – não obstante a ordem judicial – o poder de vasculhar registros sigilosos de pessoas indeterminadas, sem quaisquer indícios concretos, de modo a viabilizar, mediante uma ilícita utilização do procedimento de devassa indiscriminada (que nem mesmo o Judiciário pode ordenar)**, o acesso a dados supostamente impregnados de relevo jurídico-probatório, em função dos elementos informativos que viessem a ser eventualmente descobertos.[115]"

202. Desta maneira, <u>é urgente uma leitura contemporânea do artigo 5º, XII, da Constituição,</u> pois mesmo aqueles que defendiam que sua interpretação de décadas atrás deveria se guiar pelo binômio "estático - em fluxo" compreendem que ela não capta as peculiaridades da comunicação de dados e dá ensejo a abusos, felizmente contornados pelos Tribunais Brasileiros.

[115]FERRAZ JR, Tercio Sampaio Ferraz. Sigilo De Dados, O Direito À Privacidade E Os Limites Do Poder Do Estado: 25 Anos Depois. In: ANTONIALLI, D.; ABREU, J. (eds). *Direitos Fundamentais E Processo Penal Na Era Digital:* Doutrina e prática em debate. Vol. 1. InternetLab: São Paulo, 2018, p. 103-104, com grifos nossos.

203. É o caso do recurso em Habeas Corpus nº 99.735/SC, julgado em 27 de novembro de 2018 pelo STJ, contra ordem judicial que autorizou, com base na Lei de Interceptações Telefônicas, o acesso a comunicações, mediante a apreensão do dispositivo móvel e posterior "espelhamento", na modalidade WhatsApp Web. No caso, a impossibilidade de analogia entre o instituto da interceptação telefônica (art. 1º, da Lei 9.296/1996) e a medida de espelhamento foi reconhecida pelo acesso ilimitado a conversas passadas, presentes e futuras, com atualização automática, e possibilidade de edição, o que inviabiliza qualquer controle sobre os elementos informativos eventualmente trazidos aos autos.

204. Mais consistente com os aspectos técnicos da comunicação de dados e com os riscos experimentados na era digital é a posição sinalizada no âmbito do voto da I. Ministra Rosa Weber, nos autos da ADI 5527, segundo o qual a disponibilização do conteúdo de comunicações privadas – em fluxo ou armazenadas – somente pode ser determinada em "*ordem judicial, nas hipóteses e na forma que a lei estabelecer*", transitando no "*campo semântico demarcado pelo art. 5º, XII, da Constituição da República*, (...) *para fins de investigação criminal ou instrução processual penal*". O armazenamento, portanto, não descaracteriza a necessidade de proteção.

205. Assim, torna-se essencial uma leitura contemporânea do artigo 5º, XII, da Constituição sobre os temas em comento. Mesmo aqueles que outrora defendiam uma interpretação baseada no binômio "armazenado - em fluxo", agora entendem que tal visão não abrange as peculiaridades da comunicação de dados, permitindo possíveis abusos. Assim, uma proteção desproporcional dos dados em fluxo é ultrapassada e contraintuitiva para os tempos atuais e não oferecerá o grau de proteção que a mais contemporânea e adequada interpretação constitucional do sigilo das comunicações exige.

V.3. INCLUSÃO DE MECANISMOS DE RESPEITO À CADEIA DE CUSTÓDIA

206. Para além da necessidade de decisão judicial prévia, da observância de parâmetros já existentes no ordenamento jurídico, como a previsão de um prazo máximo para a medida, descarte das provas que não guardam relação com o objeto investigado etc. e a proteção dos dados em fluxo, deve-se observar as garantias referentes à cadeia de custódia.

207. A observância da manutenção da cadeia de custódia garante que seja mantida a integridade e autenticidade das provas coletadas durante uma investigação. Trata-se de medida fundamental para assegurar a confiabilidade da prova e preservar sua validade na persecução penal, bem como a proteção dos direitos individuais, evitando a obtenção de provas ilícitas.

208. Devido às particularidades das provas digitais, é necessária a intervenção legislativa que estabeleça regras próprias para a cadeia de custódia, contemplando as fases de produção, admissão e valoração. Deve-se, portanto, englobar técnicas específicas para a individualização e apreensão dessas provas, sob pena de inutilização dessa prova[116].

209. Em relação às provas digitais, nota-se as características de desmaterialização e dispersão. Ou seja, trata-se de provas voláteis e frágeis[117], o que demanda maior preocupação com a falsificação ou destruição – há uma fácil alterabilidade da prova, que por sua própria natureza permite a contaminação, de modo que deve ser manejada com maior cuidado.

210. Dessa forma, é necessária a criação de técnicas para construir uma prova utilizável ao se tratar de provas obtidas por meios digitais, como os *spywares*. Deve-se, entre outros, após a obtenção do dado digital, conservar os dados em local seguro e adequado, com a análise dos dados obtidos relevantes para o objeto da investigação. Também, faz-se imprescindível apresentar a prova em juízo juntamente a produção de prova pericial e eventuais esclarecimentos de peritos.

211. É essencial a documentação da cadeia de custódia especialmente no caso da análise de dados digitais, a fim de excluir possíveis alterações indevidas do material

[116] BADARÓ, Gustavo. *A cadeia de custódia da prova digital*. Artigo elaborado para apresentação de palestra, com mesmo tema, no Congresso Internacional de Direito Probatório, realizado nos dias 18 e 19 de novembro de 2021, em Porto Alegre/RS, pela Pontifícia Universidade Católica do Rio Grande do Sul e pela Universidade Alberto Hurtado, com apoio do IBDP e da Procnet. Disponível em: https://edisciplinas.usp.br/pluginfile.php/8351444/mod_resource/content/0/BADARO%CC%81%20-%20A%20cadeia%20de%20custo%CC%81dia%20da%20prova%20digital%20PUCRS.pdf

[117] São características das provas digitais a não materialidade, volatividade e fragilidade, que demandam maior preocupação, cf. MASSENA, Caio Badaró. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa, *Boletim IBCCRIM*, n. 368, jul. 2023, p. 19-21.

obtido. Sendo assim, é necessária a juntada de um laudo técnico com extensa descrição dos sistemas informáticos utilizados, os instrumentos e os dados obtidos.

212. Relembra-se que a cadeia de custódia foi disciplinada entre os artigos 158-A a 158-F do Código de Processo Penal, a partir da Lei n. 13.964/2019. Estabeleceu-se, portanto, a documentação da cadeia de custódia como: "*Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte*", conforme o art. 158-A.

213. Cuida-se da sucessão de todas as pessoas que tiveram contato com a fonte de prova, desde colhida até sua apresentação em juízo. Em outras palavras, todas as pessoas que tiveram contato com a prova, bem como todos os momentos específicos que tiveram contato devem ser documentados, sendo da responsabilidade de todos os envolvidos na cadeia de custódia o registro e o devido manejo (art. 158-D, §4º, CPP).

214. Demais disso, as etapas da cadeia de custódia foram previstas no art. 158-B do CPP, que são: (i) reconhecimento; (ii) isolamento, (iii) fixação; (iv) coleta; (v) acondicionamento; (vi) transporte; (vii) recebimento; (viiii) processamento; (ix) armazenamento; e (x) descarte. Todas essas etapas devem ser observadas e documentadas extensivamente, especialmente no caso das provas digitais.

215. Reforça-se, desse modo, a necessidade de assegurar a análise forense das provas obtidas por meio digital, com a elaboração de laudos periciais detalhados e minuciosos, dispondo sobre cada etapa da cadeia de custódia, inclusive sobre a necessidade de transferência da prova e dos armazenamentos decorrentes.

216. Por fim, entende-se que no caso das provas obtidas por *spywares*, devido ao alto grau de intrusividade do meio de prova e fragilidade das informações, deve-se considerar que a constatação de vícios na cadeia de custódia deve levar necessariamente à ilicitude ou ilegitimidade. Nessa hipótese, não é adequado deixar essas questões para serem resolvida no momento da valoração pelo Magistrado, de modo que **se não houver uma documentação completa da cadeia de custódia da prova, os arquivos digitais obtidos devem ser inadmitidos no processo penal**.

V.4. INDIVIDUALIZAÇÃO DE SUJEITOS A PROCEDIMENTOS DE INTRUSÃO

217. A capacidade técnica das ferramentas de vigilância adquiridas pelo poder público brasileiro traz uma preocupação quanto à possibilidade de investigações massivas, afetando centenas de indivíduos sem critérios rígidos de adequação das condutas à violação de direitos fundamentais, como privacidade e proteção de dados, no âmbito de investigações e inteligência.

218. Todas as categorias de *spywares* aqui apresentadas têm implicações nesse sentido. *Softwares* de extração de informações, derrubada de chaves criptográficas, arquivos deletados e em nuvem coletam de forma indiscriminada os dispositivos eletrônicos que são alvo da busca, corroborando para um risco de *fishing expedition*. Sem uma imposição de necessária continência e conexão com o delito o qual se investiga, corre-se o risco de minar a justa causa, incitando a perseguição de sujeitos e abusos do poder estatal.

219. Destaca-se, ainda, a capacidade que ferramentas de exploração de vulnerabilidades em infraestruturas têm de monitorar milhares de pessoas. O FirstMile, por exemplo, fornece licença para monitoramento de 10 mil indivíduos, sendo improvável a comprovação documental sobre os critérios estabelecidos para escolha de tamanha vigilância. No caso de extração de informações por inferência, a opacidade dos critérios utilizados pelos algoritmos coloca em risco pessoas que tenham se relacionado com os alvos da investigação, expandindo ainda mais a rede de monitoramento remoto.

220. Toda medida de monitoramento precisa necessariamente ser direcionada e limitada às pessoas identificadas como causadoras da ameaça[118]. Vale destacar que em nenhuma hipótese poderia tal monitoramento violar o núcleo da intimidade e das formas de vida privada do indivíduo[119].

[118]MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). Direito, inovação e tecnologia. São Paulo: Saraiva, 2015. p. 224.

[119]MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal?. JOTA. 05 jul. 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acessado em 18 de julho de 2024.

221. No contexto brasileiro, tecnologias de coleta e processamento de dados pessoais são utilizadas pelo Sistema Brasileiro de Inteligência sem a observância desses critérios. A identificação de perigo ou ameaça concreta a um bem jurídico fundamental é imprescindível, pois impede o infundado e desproporcional monitoramento da população. Afinal, se não é possível identificar o perigo ou a ameaça, o que se está investigando? Uma vez que não há um alvo específico que motive a intervenção na integridade e confidencialidade dos sistemas técnico-informacionais, todos passam a ser o alvo, abrindo margem para atuação discricionária e arbitrária do agente público.

222. Sendo assim, é imperativa a devida individualização dos sujeitos que seriam alvos do uso dessa medida, bem como da conduta ilícita que se apura. Caso contrário, incorrer-se-ia em uma devassa inexplicável na vida dos afetados e uma manifesta violação do direito à privacidade e intimidade. Deve-se, portanto, afastar qualquer possibilidade de um uso abusivo dessas ferramentas, com a máxima determinação do objeto de investigação, a fim de evitar a configuração de um Estado de vigilância em plena ordem democrática.

V.5. A NECESSÁRIA CONSTRUÇÃO DE DEMAIS PARÂMETROS COMPATÍVEIS COM A ORDEM CONSTITUCIONAL

223. Verifica-se que a ilegalidade do tratamento de dados pessoais realizado pelos órgãos de Inteligência e Segurança Pública está, também, na ausência de instruções procedimentais e de salvaguardas positivadas para promover a devida tutela dos titulares de dados. Diante do vasto aparato tecnológico do Estado, o cidadão encontra-se desamparado, sofrendo as graves consequências do devassamento da sua vida privada.

224. Conforme já explicado anteriormente, a infiltração dos spywares permite uma coleta de dados muito mais ampla do que a mera interceptação telefônica ou telemática, pois não se está a falar somente na interceptação de determinado tráfego de dados, mas, sim, da coleta de todos os dados de certo aparelho já armazenados, ou que estão sendo produzidos em tempo real.

225. À luz desse alto grau de interferência na vida humana e da sensibilidade das informações que podem ser coletadas, além da elaboração de uma lei específica autorizativa que legalize o uso dos *spywares* pelas autoridades investigativas, bem

como a presença de autorização judicial, também se faz imprescindível a i) identificação de um perigo concreto a um bem jurídico, no caso em concreto, além da ii) garantia do núcleo da intimidade, isto é, sempre que informações extremamente íntimas forem coletadas, faz-se necessário que elas sejam descartadas ou protegidas de uma forma mais segura pela autoridade policial.

226. Nesse contexto, cumpre trazer à baila determinados parâmetros elencados pela Doutora Laura Schertel Mendes, em sede de audiência pública ocorrida no âmbito desta ADPF, para quem a infiltração dos dispositivos pelas autoridades competentes, por meio dos *spywares*, apenas pode ocorrer quando i) condições específicas forem atendidas, como uma ii) base jurídica segura, com a iii) clareza necessária sobre a finalidade do tratamento de dados para que se avalie o nível de intervenção nos direitos fundamentais, seja também iv) proporcional, adequada e necessária à finalidade pretendida, adotando, ainda as v) providências preventivas mínimas de cunho procedimental e organizacional, orientadas à segurança dos cidadãos envolvidos e à diminuição dos riscos de danos a seus direitos à personalidade.

227. Dito de outra forma, quanto mais grave for a restrição aos direitos fundamentais, mais contundentes devem ser as justificativas, os critérios e as precauções.

VI. DOS PEDIDOS

228. Ante o exposto, os *amici curiae* devidamente admitidos por esta E. Corte para auxiliar no julgamento do feito requerem que este E. Tribunal Superior declare a inconstitucionalidade do uso de *spywares* pelo Estado, ante a violação de direitos fundamentais e o contexto pelo qual são utilizadas, explorando as vulnerabilidades de outras plataformas para as quais deve-se priorizar o direito à integralidade dos sistemas informacionais.

229. Subsidiariamente, requer seja determinada a imediata suspensão do uso de ferramentas de *spywares* pelas Autoridades Brasileiras, até que o uso seja devidamente regulamentado por legislação no Congresso Nacional. Nessa hipótese, requer a fixação de critérios rígidos para utilização de *spywares*, em tratamento análogo à regulamentação existente para as demais hipóteses de quebra de sigilo, em especial i) a necessidade de decisão judicial prévia e de respeito à rigidez similar

às demais situações de quebra de sigilo; (ii) a interpretação constitucional sobre o sigilo das comunicações atualizada aos padrões de intrusividade contemporâneos; (iii) inclusão de mecanismos de respeito à cadeia de custódia; (iv) a individualização de sujeitos à procedimento de intrusão; (v) a construção de demais parâmetros compatíveis com a ordem constitucional.

Nestes termos, pede deferimento.
Brasília/DF, 29 de julho de 2024

Bárbara P. Simão
OAB/SP n. 428.335

Danyelle Reis
CPF n. 111.020.786-70

Francisco Brito Cruz
OAB/SP n. 314.332

André Houang
OAB/SP n. 463.200

Pedro Saliba
OAB/RJ n. 211.334

Vinicius Fernandes da Silva
CPF n. 403.305.468-56

Rafael A. F. Zanatta
OAB/SP n. 311.418

Felipe Fernandes de Carvalho
OAB/DF n. 44.869

Ivan Cândido da Silva de Franco
OAB/SP n. 331.838

Cíntia Anacleto Isawa
OAB/SP n. 451.872

Amanda Boukai Chapaval
OAB/SP n. 508.238