

Ofício nº 005/2023

Exmo. Sr. Dr. Carlos Bruno Ferreira da Silva

Procuradoria-Geral da República
Ministério Público Federal**Assunto:** Utilização ilícita do sistema FirstMile pela Agência Brasileira de Inteligência

Prezado Sr. Procurador da República Carlos Bruno,

Vimos, por meio deste Ofício, trazer manifestações da **Associação Data Privacy Brasil de Pesquisa**, entidade civil sem fins lucrativos sediada em São Paulo, sobre a utilização do sistema **First Mile** pela Agência Brasileira de Inteligência, denunciada pelos jornalistas Patrik Camporez, Dimitrius Dantas e Thiago Bronzatto em matéria assinada pelo **jornal O Globo**.¹

A matéria mencionada apresentou elementos factuais importantes para a discussão de proteção de direitos fundamentais no contexto das atividades de inteligência e uso de tecnologias invasivas e lesivas a direitos, em especial:

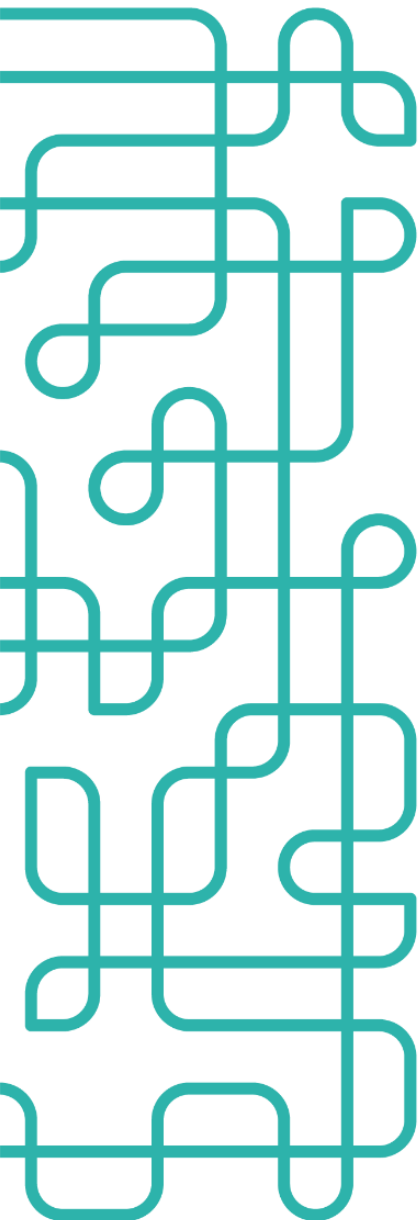
1. A contratação da ferramenta **First Mile** pela Agência Brasileira de Inteligência em 2018, em procedimento obscuro,

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

¹ Ver a matéria na íntegra, apontando a utilização da solução para monitoramento de geolocalização, a partir de denúncias e fontes da própria Agência Brasileira de Inteligência: <https://oglobo.globo.com/politica/noticia/2023/03/especialistas-apontam-falta-de-previsao-legal-e-afronta-a-direitos-constitucionais-em-uso-de-programa-secreto-de-monitoramento-pela-abin.ghtml>



que ofereceu à agência de inteligência a possibilidade de identificar a “localização da área aproximada de aparelhos que utilizam as redes 2G, 3G e 4G”;

2. A ausência de procedimento licitatório para contratação e ausência de documentação pública sobre as capacidades da ferramenta **First Mile**, desenvolvida pela empresa israelense **Cognyte**, comercializada no Brasil por subsidiária que integra o grupo econômico Verint Systems;
3. O fato de que qualquer celular identificado como alvo poderia ser rastreado pelo programa, com limite de 10 mil proprietários de aparelhos a cada 12 meses. O mecanismo era usado sem a necessidade de registros sobre quais pesquisas eram realizadas. Na prática, qualquer celular poderia ser monitorado pelo programa sem uma justificativa oficial;
4. A justificativa legal utilizada pela Abin, de acordo com fontes da matéria, era de que o acesso a metadados do celular não está expressamente proibido na lei brasileira, inexistindo quebra de sigilo telefônico por ser uma investigação para fins de segurança nacional;

Além das importantes revelações trazidas pelo trabalho jornalístico do **O Globo**, com base em levantamentos feitos pela Data Privacy Brasil entre os dias 14 e 15 de março de 2023, também identificamos que:

1. O **First Mile** funciona como "serviço de geolocalização de dispositivos móveis em tempo real, capaz de decodificar as identidades lógicas dos dispositivos e de gerar alertas sobre a rotina de movimentação dos alvos de interesse";
2. A empresa desenvolvedora da **First Mile**, Cognyte, é uma empresa conhecida por violações sistemáticas de direitos humanos da perspectiva das consequências dos usos de suas tecnologias. A *Cognyte Technologies Israel*, anteriormente conhecida como *Verint Systems Ltda - Israel*, ofereceu serviços para a empresa pública *Myanmar Posts and Telecommunications*, em 2021, em Myanmar, antes do golpe que levou à prisão de

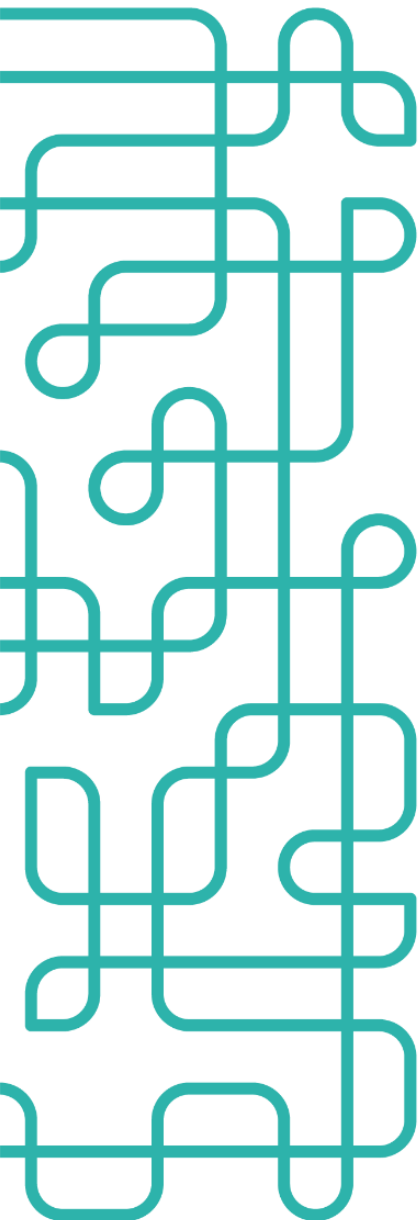
Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

**Endereço**

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

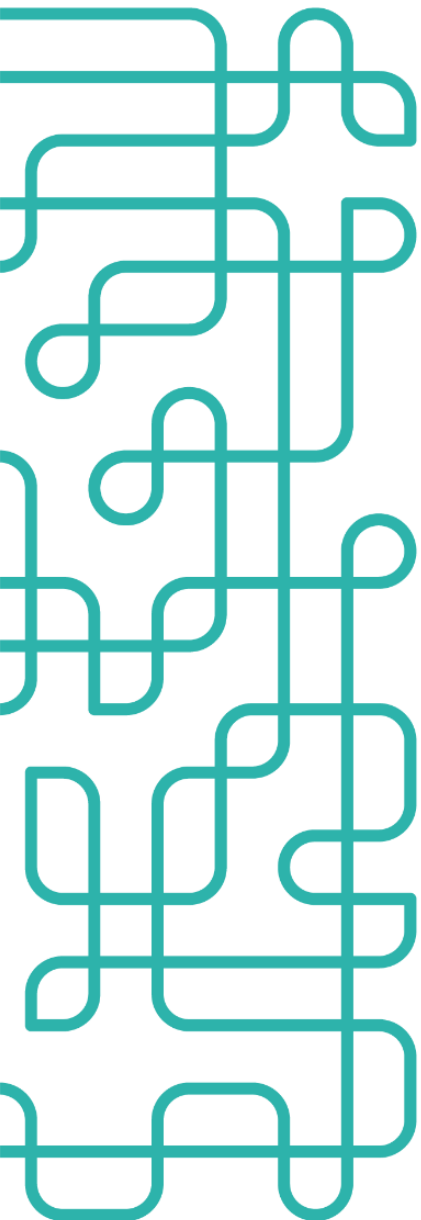
mais de 12.000 pessoas e assassinato de 1.600 pessoas em Myanmar, país do sul da Ásia continental. O escopo do contrato era precisamente o uso de tecnologias GLMC/SMLC para **real time GPS positioning tracking for target user**. Detalhes deste contrato podem lidos na matéria "*Myanmar Acquired Spyware From Israeli Cyber-intelligence Firm Cognyte, New Docs Reveal*", escrita por Oded Yaron e publicada no jornal Haaretz em 15 de janeiro de 2023.²

3. De acordo com o relatório *These walls have ears: The chilling effect of surveillance in South Sudan*, produzido pela Amnesty International em 02 de fevereiro de 2021, serviços providos pela Cognyte foram utilizados pelo governo do Sudão para instrumentalizar perseguição e violação de direitos de opositores.³
4. Em 17 de junho de 2022, o Conselho de Ética para Investimentos do Fundo de Pensão do Governo da Noruega publicou recomendações para **exclusão da Cognyte Software Ltd do seu portfólio de investimentos**.⁴ O motivo principal, segundo este documento público, a razão de exclusão é o “nível inaceitável de risco que a companhia gera para sérios abusos de direitos humanos”. O Conselho de Ética argumentou que a tecnologia habilita uma série de violações extremas de direitos humanos, o que permite casos de sequestro, tortura e outras formas de perseguição de grupos vulneráveis e opositores políticos.
5. Em parecer técnico assinado em 23 de julho de 2021 por Armando Lemos, diretor técnico da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança, nota-se que a First Mile (“Serviço de geolocalização de aparelhos móveis”) funciona como “acesso remoto agnóstico a tipo de dispositivo e integração nativa com os sensores táticos COGNYTE (GI2)”

² Ver a matéria de Oded Yaron, que enfatiza ausência de documentação pública e o caráter secreto da contratação pela empresa estatal, responsável pela gestão do setor de telecomunicações: <https://www.haaretz.com/israel-news/security-aviation/2023-01-15/ty-article/israel-myanmar-acquired-spyware-from-cognyte-new-docs-reveal/00000185-b415-d2c1-afe7-fc37abf40000>

³ Ver relatório completo em: <https://www.amnesty.org/en/documents/afr65/3577/2021/en/>

⁴ Ver documento traduzido para o inglês no sítio do Conselho de Ética do governo: <https://files.nettsteder.regjeringen.no/wpuploadso1/sites/275/2022/12/Rec-Cognyte-ENG.pdf>

**Endereço**

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

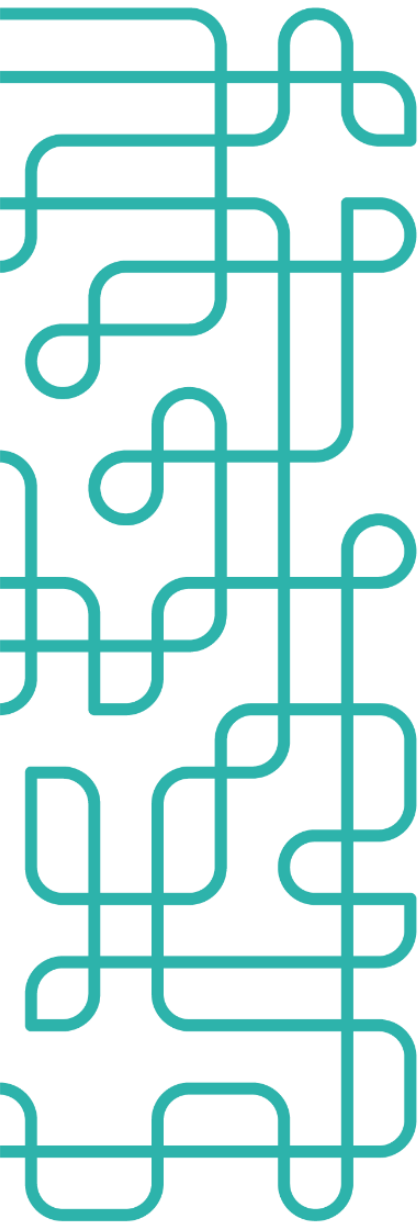
dataprivacybr.org

e as “plataformas analíticas (Clarian)”. O serviço “utiliza a infraestrutura principal GMLC e sistema de sinalização por canal comum”⁵.

6. Conforme estudo realizado por Lucas Teixeira em 28 de julho de 2017, “o Sistema de Sinalização N° 7 (Signalling System N° 7) é a sétima versão de um protocolo usado por centrais telefônicas ao redor do mundo para trocar informações de “sinalização”, que seus equipamentos usam para encaminhar mensagens e chamadas para o telefone certo, redirecionar chamadas, funcionar em roaming e tudo mais que é necessário para que possamos ligar para o Japão com a mesma facilidade (mesmo que não pelo mesmo preço) de ligar para alguém de outro estado ou da vizinhança. há uma mensagem no protocolo SS7 chamada “anyTimeInterrogation”, que permite pedir o ID da célula em que um número se encontra. A partir desse ID, é possível saber a atitude e longitude a partir de bancos de dados disponíveis comercialmente. Essa mensagem específica foi criada para ser usada internamente pela operadora — o SS7 é usado tanto entre duas operadoras quanto dentro de cada uma delas, para a comunicação de seus diferentes servidores e dispositivos — mas descobriu-se que nenhuma operadora bloqueava esses pedidos quando vindos de fora, tornando possível que uma operadora em qualquer lugar do mundo pudesse fazer ilimitados pedidos sobre números de outros países”⁶. A hipótese do pesquisador é que falhas do protocolo de sinalização por canal comum, típico das operadoras de telecomunicações, foram exploradas pela Verint para venda de produtos como a **First Mile**.
7. No artigo técnico *3G: Practical Attacks Against the SS7 Signaling Protocol* escrito em 2021, Ben Mahar, da empresa Kroll, também explica em detalhes o funcionamento dos ataques nos protocolos SS7, que foram concebidos na década de 1970. A arquitetura celular das redes 3G e do Universal Mobile Telecommunications System (UMTS) e Code Division

⁵ Ver https://abimde.org.br/media/declaracao/D.N.S_011.21_COGNYTE_NOVA-Manifesto.pdf

⁶ O estudo de Lucas foi produzido pela ONG Coding Rights, que integra a Coalizão Direitos na Rede. Ver o ensaio na íntegra, explorando a falha, em: <https://medium.com/codingrights/consultando-o-espi%C3%A3o-de-bolso-vulnerabilidades-ss7-e-rastramento-global-bc9920008c3c>



Multiple Access 2000 (CDMA2000) são habilitadores desse tipo de vulnerabilidade. Em linhas gerais, o Equipamento do Usuário conecta-se à rede local terrestre (UTRAN) e à rede central (CN), o que também permite conexão com redes externas (EN). Dentro das redes locais terrestres (sigla UTRAN) estão as redes de celulares e os radio network controllers (RNCs). A rede central (CN) divide-se em vários componentes, como Home Location Register, Visitor Location Register, Mobile Switching Centre, Gateway MSC, Service GPRS Support Node e Gateway GPRS Support Node. O que Ben Mahar demonstra é que ferramentas de simulação de ataque, como jss7-attack-simulator (desenvolvido na Universidade de Ciência e Tecnologia da Noruega), permitem a verificação da dinâmica de funcionamento de ataques usando a função Any Time Interrogation. O Home Location Register da rede central possui informações do Equipamento do Usuário. O atacante, no caso, configura o número do alvo e obtém, por meio dessa troca de informações no protocolo SS7, a informação de localização da estação rádio-base, o que se configura como clara violação de privacidade. Como argumentado por Mahar, empresas se especializaram na exploração deste tipo de vulnerabilidade e de violação do direito à privacidade, criando negócios que são ilícitos.

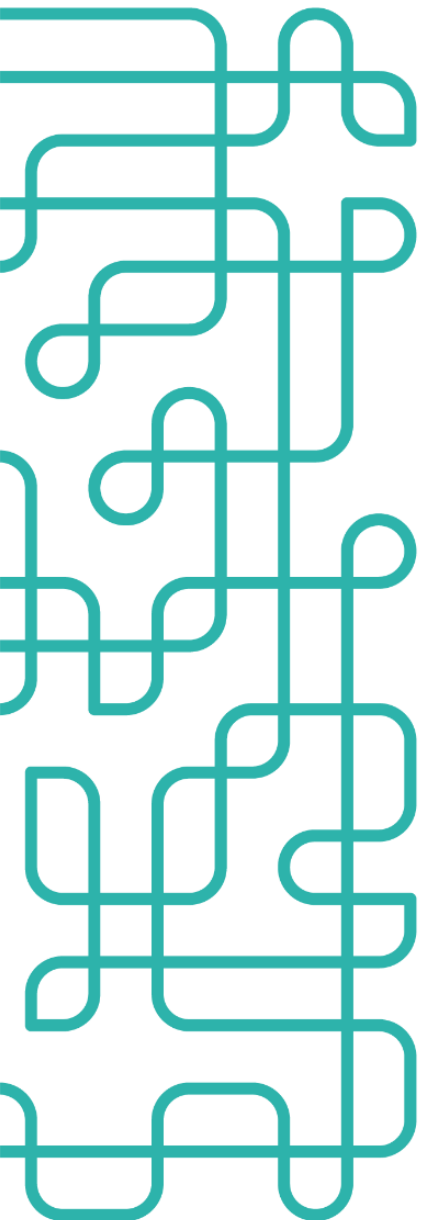
Diante desses elementos factuais e dos dados coletados, entendemos que a utilização do serviço **First Mile**, desenvolvido pela **Cognyte**, é incompatível com o sistema jurídico brasileiro.

Primeiro, pois o modelo de negócios que embasa o produto oferecido pela Cognyte estrutura-se numa exploração ilícita de dados pessoais, que são obtidos por ataques às redes de telecomunicações. Nesse sentido, há um objeto jurídico ilícito, que, por sua própria natureza, contraria o direito fundamental à privacidade.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org



Segundo, pois há relatos consistentes de que os serviços de obtenção de informações de geolocalização, de forma individualizada, são habilitadores de violações sistemáticas aos direitos fundamentais e direitos humanos. Esses relatos reforçam a necessidade de análise da utilização do **First Mile** da Cognyte pelo prisma do **Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos** (“1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas”) e do **Artigo 12 da Declaração Universal de Direitos Humanos** (“Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”).

Transpondo a discussão para o Brasil, é evidente a relação entre liberdades e a proteção contra interferências ilegais e arbitrárias em sua privacidade e correspondência. Entre os Direitos e Deveres Individuais e Coletivos insculpidos no título sobre Direitos e Garantias Fundamentais da Constituição Federal, encontra-se o inciso X, que diz que “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”, além do inciso XII, que diz que “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”.

A violação da privacidade de dados de telecomunicações ocorre sem ordem judicial e sem investigação criminal ou instrução processual penal em curso. Basta a inclusão dos celulares tidos como alvo para que, por meio de serviço *Software as a Service*, a Cognyte oferece um mapa completo de geolocalização e movimentações dos indivíduos, a partir das informações obtidas de seus aparelhos celulares.

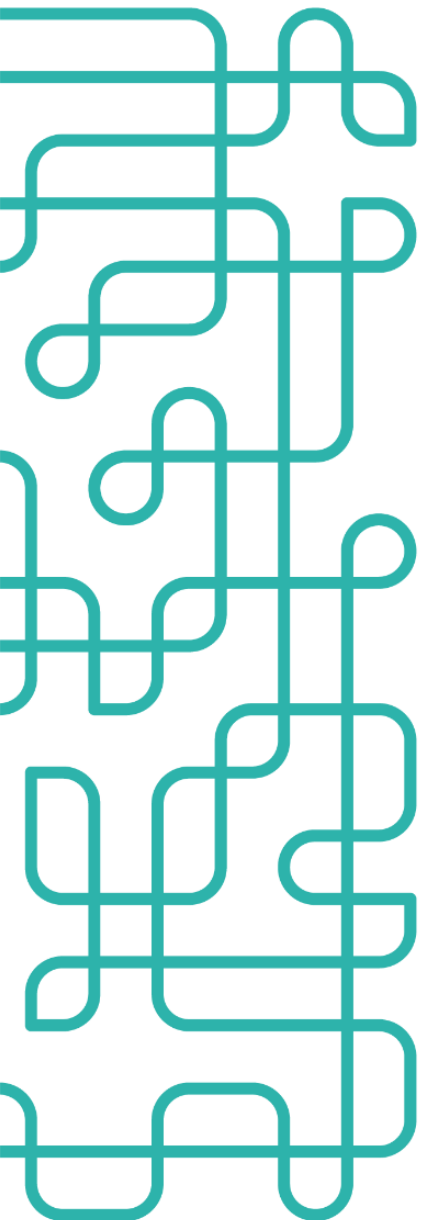
Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org



Terceiro, pois a utilização do **First Mile** pela Abin apresenta um grave problema de violação do direito fundamental autônomo à proteção de dados pessoais.

Diante da expansão do uso de softwares para apoio à atividade de inteligência e investigação criminal, o Conselho Nacional do Ministério Público reconheceu que meios de investigação podem “atingir direitos e garantias individuais, a exemplo daqueles usados para atividades de interceptação telefônica, de telemática ou de informática (Resolução CNMP nº 36/2009); soluções de análise e para coleta de dados; soluções de intrusão, bem assim ferramentas análogas” (Portaria n. 82, de 20 de agosto de 2021). No coração dessa preocupação está o direito fundamental à proteção de dados pessoais, que possui um status autônomo, conforme reconhecido pelo Supremo Tribunal Federal.

Esse direito à proteção de dados aplica-se também às atividades de inteligência em razão de sua natureza constitucional. Não se trata de mera aplicação da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), **mas sim de reconhecimento da natureza constitucional desse direito, o que transpassa a mera aplicação de uma legislação federal.** Esse reconhecimento está explícito na orientação do Supremo Tribunal Federal em casos recentes. Na ADPF 695, o ministro Gilmar Mendes fez um importante enquadramento epistemológico sobre a questão da proteção de dados pessoais diante das tentativas da Agência Brasileira de Inteligência de obtenção de dados de milhões de motoristas brasileiros via Denatran:

“Em primeiro lugar, é importante situar epistemologicamente que o parâmetro de controle invocado nesta ADPF está relacionado à afirmação do direito à proteção de dados enquanto categoria autônoma de direito fundamental na ordem constitucional brasileira, especialmente na forma de uma projeção alargada do direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, consagrado no art. 50, inciso X, da CF” (ADPF 695, Min. Gilmar Mendes)

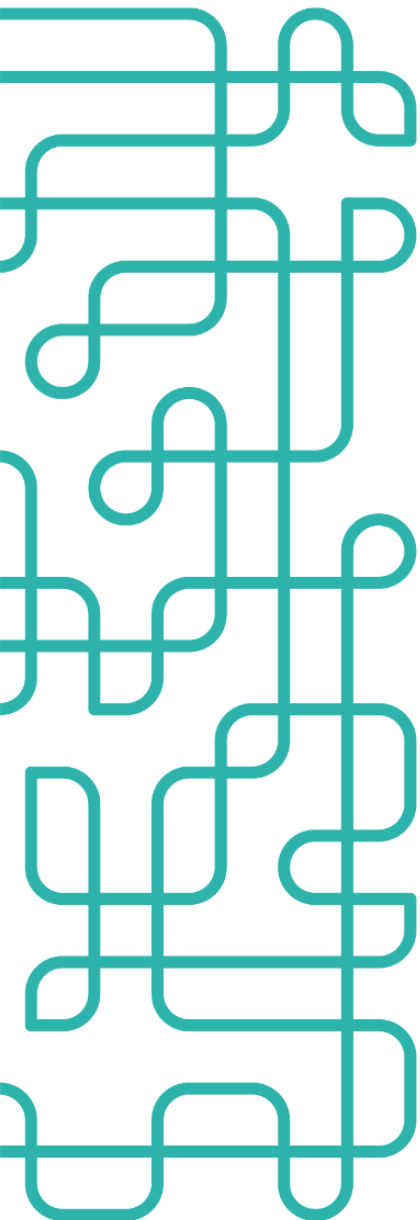
Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org



A discussão sobre direitos fundamentais não passa ao largo do enquadramento democrático sobre os limites das atividades de inteligência, como ocorreu com o também paradigmático caso dos Dossiês Antifascistas, julgado pela ministra Carmen Lúcia em 2020 no Supremo Tribunal Federal:

“Direitos fundamentais não são concessões estatais e sim garantias humanas conquistadas para além do Estado, que visam a possibilitar o sossego pessoal e a dignidade individual. É evidentemente inconstitucional a prática de investigação sem objetiva e formal definição das bases e dos limites legais, sob o manto de segredo institucional e salvaguarda de documentos de inteligência. (...) Órgãos de inteligência de qualquer nível hierárquico dos poderes do Estado se submetem ao crivo do Poder Judiciário, que tem a função-dever de julgar os casos que chegam a ele e garantir o cumprimento da Constituição” (ADPF 722, Min. Carmen Lúcia)

Diante da expansão dos usos de softwares de vigilância individualizada de cidadãos e as potenciais ameaças ao livre desenvolvimento de personalidade, é crucial a parametrização das salvaguardas e procedimentos organizacionais que podem garantir as condições mínimas de respeito à dignidade humana e ao livre desenvolvimento da personalidade, pilar do direito constitucional à proteção de dados pessoais. É preciso, portanto, promover uma leitura rigorosa do que significa a **dignidade humana** como um dos fundamentais centrais do regime jurídico do Sistema Brasileiro de Inteligência, a partir do § 1º, Art. 1º da Lei 9.883/1999. Essa requalificação do significado do § 1º, Art. 1º da Lei 9.883/1999 implica em uma nova forma de incidência dos princípios constitucionais, estruturados a partir de uma **concepção forte de proteção de dados pessoais, para as atividades típicas de inteligência**, como a “atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo

Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado”.

Não se trata, portanto, de interromper as atividades de inteligência. Tampouco se trata de interromper a utilização de tecnologias e OSINTs que, se bem utilizadas, podem ser cruciais para prevenção de atentados, práticas terroristas e atos de desestabilização da República. Trata-se de dizer que, por decorrência da obrigatoriedade de respeito à dignidade humana e minimização dos riscos gerados aos direitos da personalidade, a utilização desses softwares precisa ser amplamente documentada e amparada em razões públicas que justifiquem a potencial violação de direitos coletivos. Trata-se de ônus em razão do potencial dano causado. Esse é o fundamento das recentes decisões constitucionais sobre proteção de dados pessoais em Cortes Constitucionais, que reconhecem uma necessidade de teste tripartite, centrado em necessidade, adequação e proporcionalidade, como reconhecido também pelo Supremo Tribunal Federal em 2020 no caso IBGE.

Diante desses fatos e desse enquadramento jurídico, julgamos que é relevante que o Ministério Público Federal, em sua missão central de respeito e proteção dos direitos fundamentais e direitos coletivos, possa investigar e elucidar as seguintes questões:

1. A solução adotada pela **First Mile** utiliza de exploração ilícita de vulnerabilidade de redes telecom e do protocolo SS7? Os dados são obtidos a partir de uma exploração ilícita de vulnerabilidades que afetam a privacidade de dados de telecomunicações?
2. Quantas licenças foram habilitadas para o uso do **First Mile** pela Abin? Há registro dos números de telefone incluídos como input para obtenção das informações de geolocalização?
3. A Abin consegue demonstrar “severidade de perigo” como critério de proporcionalidade na inclusão dos números tidos como alvo? Que procedimentos amparam a atuação e

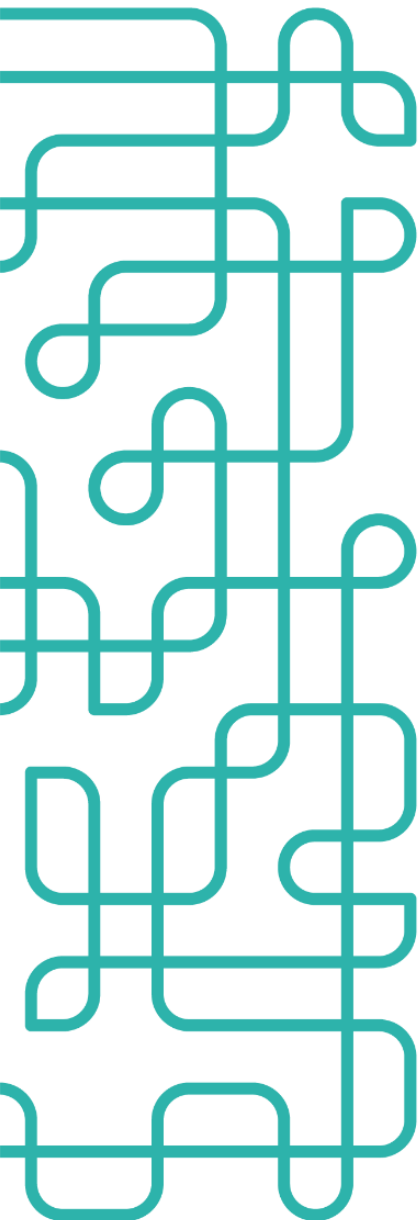
Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org



demonstram que os números selecionados como alvo possuem uma relação de causa provável com salvaguarda da segurança da sociedade e do Estado?

4. Que relação existe entre a pesquisa individualizada de geolocalização de pessoas e a produção de conhecimento sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental? Inexistindo tal relação, não há necessidade de intervenção Judiciária imediata para cessar uma situação de ilicitude e incompatibilidade com os princípios constitucionais?

Esperamos que este Ofício possa contribuir para o aprimoramento do trabalho desenvolvido pela Procuradoria-Geral da República do Ministério Público Federal. Nos colocamos à disposição para eventuais esclarecimentos.

Cordialmente,



Rafael A. F. Zanatta

Diretor - Associação Data Privacy Brasil de Pesquisa


Bruno Bioni

Diretor - Associação Data Privacy Brasil de Pesquisa

Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org