DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.7 >

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / ANDRÉ HOUANG (ED.) / CLEUNICE PITOMBO / DANIEL EDLER / DANYELLE REIS CARVALHO / FERNANDA DOS SANTOS RODRIGUES SILVA / GUSTAVO BADARÓ / JACQUELINE ABREU / JULIANA VIEIRA DOS SANTOS / LUIZA CORREA DE MAGALHÃES DUTRA / MARINA COELHO ARAÚJO / PABLO NUNES / PAULO RENÁ DA SILVA SANTARÉM / UDBHAV TIWARI / VALDEMAR LATANCE NETO / VITOR SANTOS VILANOVA / WILSON GUILHERME DIAS PEREIRA / YURI CORRÊA DA LUZ

INTERNETLAB

2ª EDIÇÃO

DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.7 >

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / ANDRÉ HOUANG (ED.) / CLEUNICE PITOMBO / DANIEL EDLER / DANYELLE REIS CARVALHO / FERNANDA DOS SANTOS RODRIGUES SILVA / GUSTAVO BADARÓ / JACQUELINE ABREU / JULIANA VIEIRA DOS SANTOS / LUIZA CORREA DE MAGALHÃES DUTRA / MARINA COELHO ARAÚJO / PABLO NUNES / PAULO RENÁ DA SILVA SANTARÉM / UDBHAV TIWARI / VALDEMAR LATANCE NETO / VITOR SANTOS VILANOVA / WILSON GUILHERME DIAS PEREIRA / YURI CORRÊA DA LUZ

INTERNETLAB

2ª EDIÇÃO · SÃO PAULO, 2025

O InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

Citação sugerida
BRITO CRUZ, Francisco; SIMÃO, Bárbara; HOUANG, André (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. VII. São Paulo. InternetLab, 2024.

Avenida Ipiranga 344 cj 11B | 01046-010 | São Paulo | SP | Brasil
ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA
www.internetlab.org.br

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Direitos fundamentais e processo penal na era digital [livro eletrônico] : doutrina e prática em debate : vol. 7. -- 2. ed. -- São Paulo : InternetLab, 2025.

Vários autores.
Bibliografia.
ISBN 978-65-88385-21-0.

1. Direitos fundamentais **2.** Direito processual penal **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação.

25-262542 **CDU-343.1:004**

Índices para catálogo sistemático:
1. Direito e tecnologia : Direito processual penal
343.1:004
Aline Graziele Benitez - Bibliotecária - CRB-1/3129

AUTORES /

< BÁRBARA SIMÃO >

Advogada, mestre em direito e desenvolvimento pela Fundação Getúlio Vargas (FGV Direito SP) e graduada pela Faculdade de Direito da Universidade de São Paulo (FDUSP). Atuou como pesquisadora na área de direitos digitais do Instituto Brasileiro de Defesa do Consumidor (Idec), entre 2017 e 2020, e como coordenadora de pesquisa no InternetLab entre 2021 e 2024.

< CLEUNICE PITOMBO >

Advogada, doutora e mestre em processo penal USP. Professora no curso de especialização em direito e tecnologia da Poli. Autora de livros e artigos acadêmicos. Conselheira do Ibccrim.

< DANIEL EDLER >

Daniel é pesquisador associado do Departamento de Política e Estudos Internacionais da Universidade de Glasgow e do Núcleo de Estudo da Violência da Universidade de São Paulo (NEV/USP). Daniel fez o doutorado no Departamento de War Studies do King's College London (KCL) e já trabalhou em diversas instituições, incluindo: Universidade de Southampton, PUC-Rio, Fundação Getulio Vargas, Escola de Guerra Naval e Fundação Konrad Adenauer. Sua pesquisa atual se desdobra em três eixos principais: (1) práticas de vigilância; (2) novas tecnologias no policiamento urbano; e (3) controvérsias públicas no campo da ciência e tecnologia.

< DANYELLE REIS CARVALHO >

Danyelle Reis Carvalho é mestra em Filosofia e Teoria Geral do Direito pela Universidade de São Paulo (FDUSP). Foi pesquisadora do Centro de Análise da Liberdade e do Autoritarismo (LAUT) e do Centro de Estudos sobre Liberdade de Expressão (CELEX-USP). Foi bolsista e monitora em Filosofia do Direito e Metodologia do Estudo do Direito no Programa de Aperfeiçoamento de Ensino (PAE-FDUSP). Foi representante discente da pós-graduação. Graduada em Direito pela Universidade Federal de Lavras (UFLA). Na graduação, foi bolsista de monitoria do Programa Institucional de Bolsas e voluntária no Programa de Iniciação Científica. Integrante da associação de pesquisa "Serras de Minas de Teoria da Justiça e do Direito". Atualmente, é pesquisadora do InternetLab.

< FERNANDA DOS SANTOS RODRIGUES SILVA >

Doutoranda em Direito, Tecnociências e Interdisciplinaridade pela Universidade Federal de Minas Gerais (UFMG). Mestre em Direitos na Sociedade em Rede e graduada em Direito pela Universidade Federal de Santa Maria (UFSM). Coordenadora de pesquisa e pesquisadora no Instituto de Referência em Internet e Sociedade. Fellow dos programas LACNIC 2023 e Policy Shapers 2024.

< GUSTAVO BADARÓ >

Professor Titular de Direito Processual Penal pela Faculdade de Direito da Universidade de São Paulo, pela qual também é Livre-Docente em (2011), Doutor (2002) e Mestre (1999) e na qual obteve o grau de bacharel (1993). É membro do Instituto Ibero-Americano de Direito Processual (IIDP), Instituto Brasileiro de Direito Processual (IBDP), Instituto Brasileiro de Ciências Criminais (IBCCrim), Instituto Brasileiro de Direito Processual Penal (IBRASPP) e Instituto dos Advogados de São

Paulo (IASP). Membro do Conselho Científico do Centro de Estudos de Direito Penal e Processual Penal Latino-Americano, do Instituto de Ciências Criminais, da Georg-August de Göttingen Alemanha. Conselheiro Federal da Ordem dos Advogados do Brasil, por São Paulo. Sócio Fundador do Badaró, Falk e Maximo Advogados e Consultor Jurídico.

< JACQUELINE ABREU >

Doutora em Direito pela Faculdade de Direito da Universidade de São Paulo e advogada. Mestra em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Foi membro da Comissão de Juristas da Câmara dos Deputados encarregada de elaborar o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigações Criminais. Foi assistente de pesquisa visitante do Berkman Klein Center for Internet and Society da Harvard University, aluna do Summer Doctoral Programme do Oxford Internet Institute e coordenadora da área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em direito e tecnologia.

< JULIANA VIEIRA DOS SANTOS >

Diretora de Assuntos Parlamentares da Secretaria Nacional de Assuntos Legislativos do Ministério da Justiça e Segurança Pública. Advogada Licenciada. Mestre pela Harvard Law School e Doutora em Direito do Estado pela Faculdade de Direito da Universidade de São Paulo (USP). Foi Coordenadora Jurídica da Rede Liberdade. Foi conselheira da Associação de Advogados de São Paulo – AASP e do LAUT – Centro de Análise da Liberdade e do Autoritarismo.

< LUIZA CORREA DE MAGALHÃES DUTRA >

Doutoranda e mestra em Ciências Criminais pela Pontifícia Universidade do Rio Grande do Sul. Especialista em Segurança Pública, Cidadania e Diversidade pela Universidade Federal do Rio Grande do Sul. Bacharela em Ciências Sociais pela UFRGS, com período sanduíche realizado no Science-Po Rennes, França, e Bacharela em Direito pela PUCRS. Pesquisadora.

< MARINA PINHÃO COELHO ARAÚJO >

Advogada. Doutora em Direito Penal pela Faculdade de Direito da Universidade de São Paulo. Especialista em Direito Penal Econômico pela Universidade de Coimbra. Membro do Instituto de Defesa do Direito de Defesa – IDDD. Professora no INSPER. Consultora da Comissão de Direito Penal da OAB/SP. Foi Presidente do IBCCRIM no Biênio 2021/2022. Autora do livro Tipicidade Penal: Uma análise funcionalista, além de diversos artigos sobre Direito Penal Empresarial. Pesquisadora na Universidade de Munique (LMU) entre 2003 e 2004 e pesquisadora na New York University (NYU) em 2012.

< PABLO NUNES >

Doutor em Ciência Política pelo Iesp-Uerj e Coordenador do CESeC. Atuo nas áreas de segurança pública, novas tecnologias e justiça criminal. Coordenador do Panóptico e da Rede de Observatórios da Segurança.

< PAULO RENÁ DA SILVA SANTARÉM >

Doutorando e Mestre em Direito, Estado e Constituição na Universidade de Brasília (UnB). Pesquisador bolsista no Instituto de Referência em Internet e Sociedade (IRIS); integrante voluntário do Aqualtune LAB: Direito, Raça e Tecnologia; ex-Diretor

Presidente do Instituto Beta Internet e Democracia (IBIDEM), três ONGs componentes da Coalizão Direitos na Rede (CDR). Consultor Sênior de Políticas Públicas do Capítulo Brasileiro da Internet Society (ISOC Brasil) para os temas Responsabilidade de Intermediários e Criptografia. Conselheiro Consultivo do centro de pesquisa Internetlab. Consultor Associado da Veredas – Estratégias em Direitos Humanos. Servidor Público Federal no Tribunal Superior do Trabalho (TST), foi gestor do processo de elaboração coletiva do Marco Civil da Internet na Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL-MJ).

< UDBHAV TIWARI >

Udbhav Tiwari é o *Director of Global Product Policy* na Mozilla e trabalha para manter a Internet aberta, segura e acessível, defendendo regulações progressivas no setor da tecnologia. Foi Non-Resident Scholar no Carnegie Endowment for International Peace, Índia; membro do Conselho Consultivo do Digital Equity Accelerator do Aspen Institute; e trabalhou na equipe de políticas públicas da Google e no Centre for Internet and Society (Índia). Já foi citado como especialista em vários meios de comunicação nacionais e internacionais, incluindo a CNN, The Guardian, Wired UK, Financial Times, BBC, Reuters e Times of India. Também fez parte da lista "India Tomorrow" do India Today em 2020.

< VALDEMAR LATANCE NETO >

Possui graduação em Direito pela Universidade de Sorocaba (2002). Especialista em Inteligência Policial pela Academia Nacional de Polícia (2014). Delegado de Polícia Federal, atualmente é Coordenador-Geral de Combate a Crimes Cibernéticos da Diretoria de Combate a Crimes Cibernéticos (DCIBER/PF) e vice-líder do grupo de pesquisa em Criminalidade Organizada Cibernética. Professor da Academia Nacional de Polícia (ANP/PF) da disciplina "Crimes Cibernéticos: Prevenção e Investigação" na Pós-Graduação em Segurança Pública Contemporânea. É autor do livro "DISPENSA E INEXIGIBILIDADE DE LICITAÇÃO: A responsabilidade civil e criminal de seus agentes".

< VITOR SANTOS VILANOVA >

Pesquisador no InternetLab. Graduando em Direito pela USP (Universidade de São Paulo). É professor-convidado da Escola de Formação Pública da Sociedade Brasileira de Direito Público (SBDP). Foi editor na Revista Acadêmica São Francisco (RASF).

< WILSON GUILHERME DIAS PEREIRA >

Pesquisador e Bolsista do Instituto de Referência em Internet e Sociedade – IRIS, Mestre em Direitos Humanos e Desenvolvimento da Justiça, pela Universidade Federal de Rondônia – UNIR; Graduado em Direito pela Faculdade Interamericana de Porto Velho; Advogado Autônomo; Alumni da Escola de Governança da Internet – EGI 2023; Youth do Comitê Gestor da Internet no Brasil – CGI.BR em 2023. Mentore e ex-embaixador do Programa Cidadão Digital – Safernet Brasil; Ex-Coordenador de Práticas, Pesquisas e Extensões Jurídicas da Faculdade Católica de Rondônia – FCR (2022); Bolsista do programa sobre saúde mental para crianças e adolescentes da ASEC; Integrante da Coalizão Direitos na Rede – CDR no Grupo de Trabalho sobre Privacidade e Vigilância, representando o IRIS; Tem como área de interesse: direitos humanos, infâncias e juventudes, sexualidade, raça e gênero, intersecionalização entre tecnologia e educação para direitos humanos, tecnologia e região amazônica.

< YURI CORRÊA DA LUZ >

Yuri Corrêa da Luz é Professor de Direito Penal da ESPM-SP, Doutor em Direito Penal pela USP, com período de pesquisa na LMU-München, na Alemanha, pesquisador do Núcleo Direito e Democracia do Cebrap e Procurador da República em São Paulo/SP.

SUMÁRIO /

APRESENTAÇÃO DOS EDITORES /

Um dos grandes temas de 2023 foi *democracia*. Os ataques ao Congresso e ao Supremo Tribunal Federal ocorridos em janeiro de 2023 evidenciaram a importância de se compreender como a defesa da democracia é mobilizada por diferentes atores no Poder Público. Ao longo do ano, foi possível notar o enrobustecimento do discurso de combate ao terrorismo e crimes contra a democracia, com novas propostas penais, pedidos judiciais de acesso a dados e debates sobre a responsabilidade das plataformas na moderação de conteúdos. Simultaneamente, órgãos de defesa nacional foram investigados pelo uso de ferramentas de intrusão remota (*spywares*), levantando discussões sobre privacidade, proteção de dados e o alcance das capacidades estatais de controle e investigação.

Diante desse cenário, o VII Congresso Direitos Fundamentais e Processo Penal na Era Digital não poderia ter outro fio condutor: "democracia e capacidades de investigação" foi o mote que deu o tom aos painéis e discussões da edição, ocorrida entre os dias 29 e 31 de agosto de 2023.

Organizado desde 2017 pelo InternetLab, com o apoio institucional da Faculdade de Direito da Universidade de São Paulo (FDUSP), o Congresso tem o intuito de sediar debates na intersecção entre processo penal e tecnologia e refletir sobre as atuais questões do campo.

Neste livro, trazemos contribuições relacionadas às palestras, que abordaram temas como o uso de câmeras corporais por forças policiais, o uso (e a legalidade) de sistemas de intrusão remota por órgãos de inteligência e defesa nacional, os impactos de métodos de investigação sobre a criptografia de ponta a ponta, a extensão de empresas de vigilância privada sobre espaços públicos, assim como atuais discussões relacionadas às provas digitais no âmbito do Poder Legislativo.

Todas as contribuições do Congresso estão também registradas em vídeo e disponíveis para acesso online. Nosso objetivo é elaborar e compartilhar reflexões que atualizem e aprofundem os desafios que o desenvolvimento tecnológico e o uso de dados impõem às garantias do processo penal.

Boa leitura!

FRANCISCO BRITO CRUZ
BÁRBARA SIMÃO
ANDRÉ HOUANG

São Paulo, setembro de 2024.

APRESENTAÇÃO DOS EDITORES À SEGUNDA EDIÇÃO /

Desde 2017, o Congresso Direitos Fundamentais e Processo Penal na Era Digital é realizado pelo InternetLab com o apoio da Faculdade de Direito da Universidade de São Paulo. Depois de 7 edições, o Congresso já se consolidou como um importante evento que sedia anualmente debates acadêmicos entre processo penal e novas tecnologias. É natural que a discussão acadêmica se dê entre pessoas com posições, metodologias e argumentos diferentes. Em um campo tão sensível quanto o do Congresso, que envolve a defesa e equilíbrio entre diferentes direitos fundamentais, é esperado que as discordâncias possam ser especialmente acentuadas.

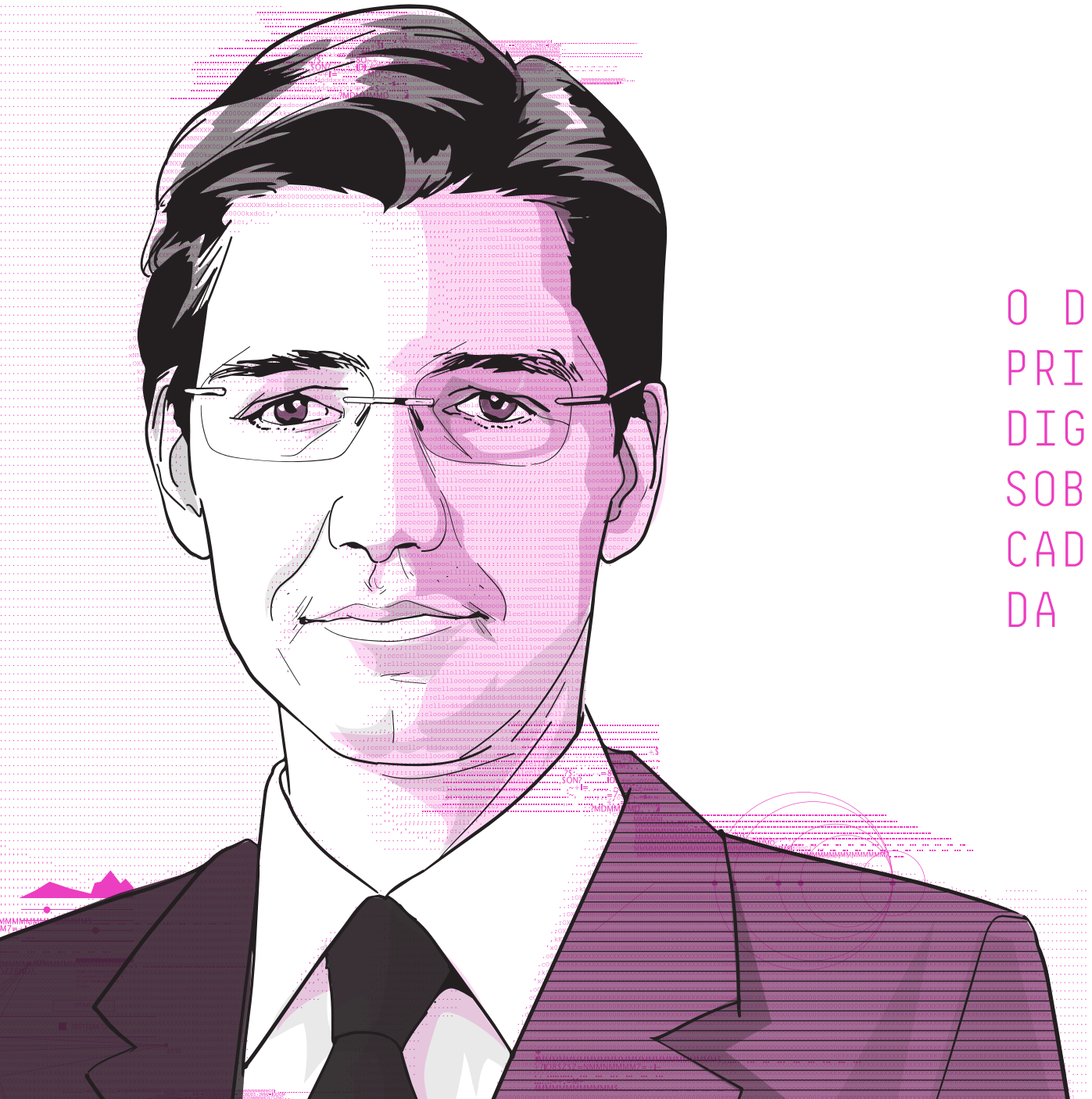
Nesta segunda edição do sétimo volume dos anais do Congresso trazemos um texto adicional para o debate sobre o uso de ferramentas de varredura pelo lado do cliente. Esta temática carrega muitos desafios, particularmente sensíveis no que diz respeito a potenciais riscos a direitos fundamentais, que devem sempre ser ponderados com cautela, sobretudo quando o assunto é proteção de crianças e adolescentes. Na edição anterior trouxemos apenas uma perspectiva desse debate. Por valorizar a riqueza do debate acadêmico e por entender que a pluralidade de pontos de vista sobre como lidar com esses desafios é essencial na busca por boas soluções, essa nova edição busca corrigir isso com um artigo adicional que reflete sobre o uso dessas tecnologias de varredura e suas implicações para o direito à privacidade.

Esperamos que essa leitura agregue ao debate acadêmico e ao desenvolvimento de políticas para a proteção dos direitos fundamentais na aplicação do processo penal na era digital.

Boa leitura!

FRANCISCO BRITO CRUZ
E ANDRÉ HOUANG

São Paulo, 2025.



01.

O DIREITO À PRIVACIDADE NA ERA DIGITAL: REFLEXÕES SOBRE PROVAS E CADEIA DE CUSTÓDIA DA PROVA DIGITAL[1]

Gustavo Badaró

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Camilly Vitória Silva.

INTRODUÇÃO E CUMPRIMENTOS

Obrigado, Bárbara. Em teu nome eu cumprimento todos do Internetlab e a Professora Marta Saad.

O único título que eu gosto mesmo é que eu sou professor da São Francisco. Esse aí eu faço questão sempre. Talvez se um dia eu tiver que pedir que escrevam alguma coisa na minha lápide, se tiver isso, já vai estar bom.

Gostaria de cumprimentar a Cleunice Pitombo, a Marina Coelho e a Anamara Osório. É um prazer estar aqui, cumprimentar todos que estão na audiência. É sempre muito gratificante participar dos eventos do Internetlab, seja assistindo, seja, com maior razão ainda, participando da mesa.

1. INTRODUÇÃO

Bem, eu vou procurar me ater ao meu tempo e falar de alguns aspectos do tema que me foi colocado: a cadeia de custódia da prova digital.

Mas, como nós estamos falando de prova digital e normalmente isso envolve aspectos da privacidade, eu vou começar lendo um grande autor do processo penal, de verdade, Dostoiévski. E tem um livro dele sobre Memórias do Subsolo que ele diz o seguinte:

> "Existem nas recordações de todo homem coisas que ele só revela aos seus amigos. Há outras que não revela nem mesmo aos amigos, mas apenas a si próprio, e assim mesmo em segredo. Mas também há, finalmente, coisas que o homem tem medo de desvendar até a si próprio, e, em cada homem honesto, acumula-se um número bastante considerável de coisas no gênero. E acontece até o seguinte: quanto mais honesto é o homem, mais coisas assim ele possui".[2]

2. DOSTOIÉVSKI, F. M. (Trad. Boris Schnaiderman). Memórias do subsolo. São Paulo: Editora 34, 2000, p. 52.

Se nós vamos falar de meios de obtenção de prova no processo penal e da necessidade de proteção da privacidade dos investigados, há uma premissa óbvia: existem investigados que são culpados, mas também existem investigados que são honestos. E, portanto, essa proteção não se destina apenas a criminosos.

Não tenho certeza, espero não estar errando: ninguém aqui cometeu um crime recentemente. Então eu pergunto a vocês: quem está disposto a me emprestar o notebook para eu conectar aqui do projetor e passar seu histórico de navegação para o público?

Vocês não são criminosos, certo? Quem vai me emprestar o notebook para eu pôr aqui e passar para todo mundo o histórico de navegação? Ninguém! E, por quê? Por que nós somos criminosos? Não. Porque nós temos direito a isso para desenvolver nossa personalidade.

Eu tenho direito, inclusive, de ter uma personalidade privada e me apresentar ao público de outra maneira. Eu posso fazer pesquisas na internet porque eu sou um católico fervoroso e eu quero encontrar uma mulher virgem para me casar, porque eu acredito que assim deve ser. Como eu posso ser uma pessoa com uma vida sexual liberal e eu só quero procurar uma mulher liberal, porque eu gostaria de ir em casa de swing com a minha esposa. E assim pode ser. E eu posso ser qualquer um desses dois, mas querer me apresentar em público dizendo: "Sou uma pessoa normal, não sou machista, não sou feminis-

ta. Eu casei, minha mulher não era virgem. A gente leva uma vida como todo e qualquer casal". É meu direito. Então nós precisamos entender a importância disso.

2. A DISCIPLINA DA PROVA DIGITAL

Como já foi dito aqui, é necessário que nós pensemos em uma disciplina específica para a prova digital. Eu não diria, necessariamente, que existem duas espécies diferentes de documentos, o documento analógico e o documento digital. Mas cada um deles tem peculiaridades muito distintas, que exigem disciplinas legais específicas.

Em termos de prova digital, é importante que nós percebamos que quase tudo está voltado para a fase de investigação. Que, aliás, é a fase mais maltratada do processo penal brasileiro. E olha que eu falo isso ao lado da Cleunice Pitombo, e o professor Pitombo que foi um dos maiores Professores desta Casa, especialmente preocupado com o inquérito policial,[3] e a Professora Marta Saad, que escreveu sua Dissertação de Mestrado sobre o Direito de defesa na investigação criminal.[4]

3. PITOMBO, S. M. M. Inquérito policial: novas tendências. Belém: Cejup, 1987.

4. SAAD, M. O Direito de Defesa no Inquérito Policial. Editora Revista dos Tribunais, São Paulo, 2004.

Parece que na academia há um fetichismo pelo processo de conhecimento. Tem-se estudado desde a denúncia até o trânsito em julgado. Mas, quase todo mundo esquece da execução da pena, outra fase importantíssima, e esquece da investigação.

Por outro lado, Marina, quando se fala em "processo acusatório", se nós vamos pensar no processo acusatório, com ampla oralidade, tenho sérias dúvidas se ele vai servir para prova digital. É adequado para o crime de rua, para a pessoa que é pega e há uma testemunha que o viu em flagrante delito.

Já a prova digital vai se concentrar numa análise do que foi obtido na fase de investigação. E, basicamente, menos sobre o seu conteúdo e mais sobre a fiabilidade dessa prova.

3. A VERDADE PARA O PROCESSO PENAL NA ERA DIGITAL

É uma conquista da epistemologia moderna que, ainda que trabalhemos com o conceito de verdade como correspondência, o conteúdo do enunciado fático é verdadeiro quando ele corresponde à realidade exterior ao processo. Se eu falar que "José matou a Maria", esse enunciado só é verdadeiro se, realmente, José tiver matado a Maria. Se não foi o José, a assertiva é falsa. Se a Maria não morreu, também é falso. Se quem o José matou foi outra pessoa, ele é falso. Isso não quer dizer, que seja possível, a qualquer sujeito cognoscente, atingir o conhecimento pleno e total, para saber se esse enunciado é absolutamente verdadeiro.

Mesmo assim, não precisamos falar "a verdade é relativa". Verdade, para quem trabalha com a noção de verdade como correspondência, é um conceito categórico. Ou há absoluta identidade entre o enunciado e a realidade, e o conhecimento é verdadeiro, ou não.

Por outro lado, nosso conhecimento sobre os fatos será sempre limitado. Logo, isso nos força ainda mais a estabelecermos standards e padrões para dizer quando podemos considerar que um conhecimento de um enunciado está suficientemente justificado para que o juiz o adote como se verdadeiro fosse e trabalhe com ele na premissa menor do silogismo judicial.

E, no tema das provas digitais, isso se concentra, ao meu ver, de forma muito forte na cadeia de custódia.

4. ANÁLISE DO PROJETO DE CÓDIGO DE PROCESSO PENAL

Ao falar da cadeia de custódia da prova digital, gostaria de analisar alguns aspectos do Projeto de CPP, sobre a prova digital em geral. O Projeto disciplina alguns meios de obtenção de prova digital, entre eles, a busca e apreensão digital. E aqui, que eu concordo totalmente, há uma inversão na ordem normal entre a busca e a apreensão de coisas materiais.

Na casa das pessoas, primeiro eu busco e vejo tudo que há, mas só apreendo aquilo que eu buscava e encontrei. Já na prova digital, primeiro eu apreendo tudo e depois, dentro daquele tudo que foi coletado, que a polícia já apreendeu e tem ao seu dispor, é que se vai procurar se há algo que interessa para a prova. Só que diferente da prova analógica que se eu vasculhar, abrir a gaveta da pessoa e avistar lá algo que pudesse causar algum constrangimento, o investigador vai olhar, vai dar uma risadinha e vai dizer: "ah você, hein"! Mas vai deixar aquilo lá, porque não interessa para ele. Já na prova digital tudo já terá sido coletado e estará à disposição do órgão público.

Por isso, o ponto que me parece mais criticável do Projeto de CPP é a falta de uma delimitação muito clara e restrita, das hipóteses e dos requisitos para uma busca e apreensão digital. O art. 308 dispõe que: "a ordem judicial para obtenção de prova digital para fins de investigação em processo penal deve descrever os fatos investigados com indicação de materialidade e autoria". Até aqui, tudo bem. E segue: "indicando motivos, necessidade e os fins da diligência, estabelecendo os limites da atividade e o prazo para seu cumprimento". Ou seja, essa segunda parte é extremamente aberta. Estabelece o que a decisão deve conter, mas não define quais os parâmetros. Quais motivos são legítimos e quais não o são, para que o juiz autorize a busca e apreensão digital? Que tipos de necessidade a justificam?

/ ENTÃO, ATUALMENTE, O POTENCIAL DE INVASÃO AQUI É ENORME E, NESSE PONTO, A LEGISLAÇÃO PRECISARIA EVOLUIR MUITO MAIS /

Posso dar um exemplo: se o Ministério Público requerer uma interceptação telefônica em investigação de um crime punido com detenção. O motivo pode ser legítimo: investigar tal delito. O meio é necessário, porque eu preciso conhecer o conteúdo da conversa para saber quem é o seu autor. Mas o juiz vai dizer: "para esse fim, essa diligência não é permitida". Já na busca e apreensão digital não haverá essa delimitação.

Ao mais, em termos de dados digitais, aqui não estou falando de dados pessoais, mas de dados enquanto elementos de prova, há um volume absurdo de informações disponíveis. Eu queria destacar só essa característica.

Quando se analisa a prova digital, destaca-se sua volatilidade, possibilidade de fácil adulteração, ou mesmo de ser um registro em linguagem não natural. Mas há outro aspecto relevantíssimo. Os aparelhos eletrônicos permitem armazenar um conjunto brutal de informações, em espaços minúsculos, como pendrives que, hoje, têm capacidade de 2TB! Seu conteúdo impresso representaria muito mais do que nossos avós ou mesmo nossos pais tinham, se somasse todos os documentos, fotografias, cartas e escritos em geral, que armazenavam em suas casas, durante a vida inteira. Então, atualmente, o potencial de invasão aqui é enorme e, nesse ponto, a legislação precisaria evoluir muito mais.

Especialmente sobre a cadeia de custódia da prova digital, considero adequada a disciplina legal projetada. O Projeto de CPP exige um auto circunstanciado com o registro da custódia do que foi apreendido na diligência, indicando os custodiantes e as transferências havidas. Quanto à finalidade, a lei projetada prevê que se proceda de acordo com as boas práticas aplicáveis, o que é muito importante, porque é como se fosse uma norma penal em branco, que incorpora boas práticas de órgãos relevantes. Ainda é previsto que a prova digital deve ter preservada as seguintes características: integridade, completude, autenticidade, auditabilidade, reprodutibilidade dos métodos de análise. E, por fim, o que me parece mais importante: está previsto que a admissibilidade da prova nato digital exigirá a disponibilidade dos metadados e a descrição dos procedimentos de custódia.

A situação é diferente da disciplina atual da cadeia de custódia. As normas do CPP, que regem as "provas analógicas", não definem, expressamente, se a documentação completa da cadeia de custódia é requisito de admissibilidade ou se, sua ausência, é apenas um fator de diminuição de seu valor probatório.

Nas provas digitais, o projeto toma uma posição clara e estabelece que a documentação da cadeia de custódia da prova digital é um dos requisitos de sua admissibilidade.

Essa me parece uma posição correta. Isso porque, se eu tiver um papel e eu falar "olha, me mostraram um papel" vocês vão dizer "ah eu lembro era um papel de tempo". Alguém vai dizer que estava escrito cinco minutos, outro vai dizer que não, pois viu que eram dois minutos. Mas a pessoa se lembra. Por que? Porque a linguagem é natural e porque nós acessamos diretamente o conteúdo do documento. Já ao se pensar na prova digital, verdadeiramente digital, um arquivo, não é possível saber qual seu conteúdo. Trata-se de um conjunto de impulsos elétricos, de zeros e uns. Então, ainda que eu tenha tido nas minhas mãos um suporte material contendo um arquivo digital, não haverá como saber qual era o seu conteúdo e, muito menos, se o conteúdo que eu tive acesso, depois da intermediação de um equipamento que traduz o arquivo digital em uma linguagem natural, é autêntico ou não.

E aqui eu não estou desconfiando ou falando "ah o Ministério Público vai trocar um sim pelo não no documento"; "a polícia vai adulterar a data em que foi celebrado o contrato".

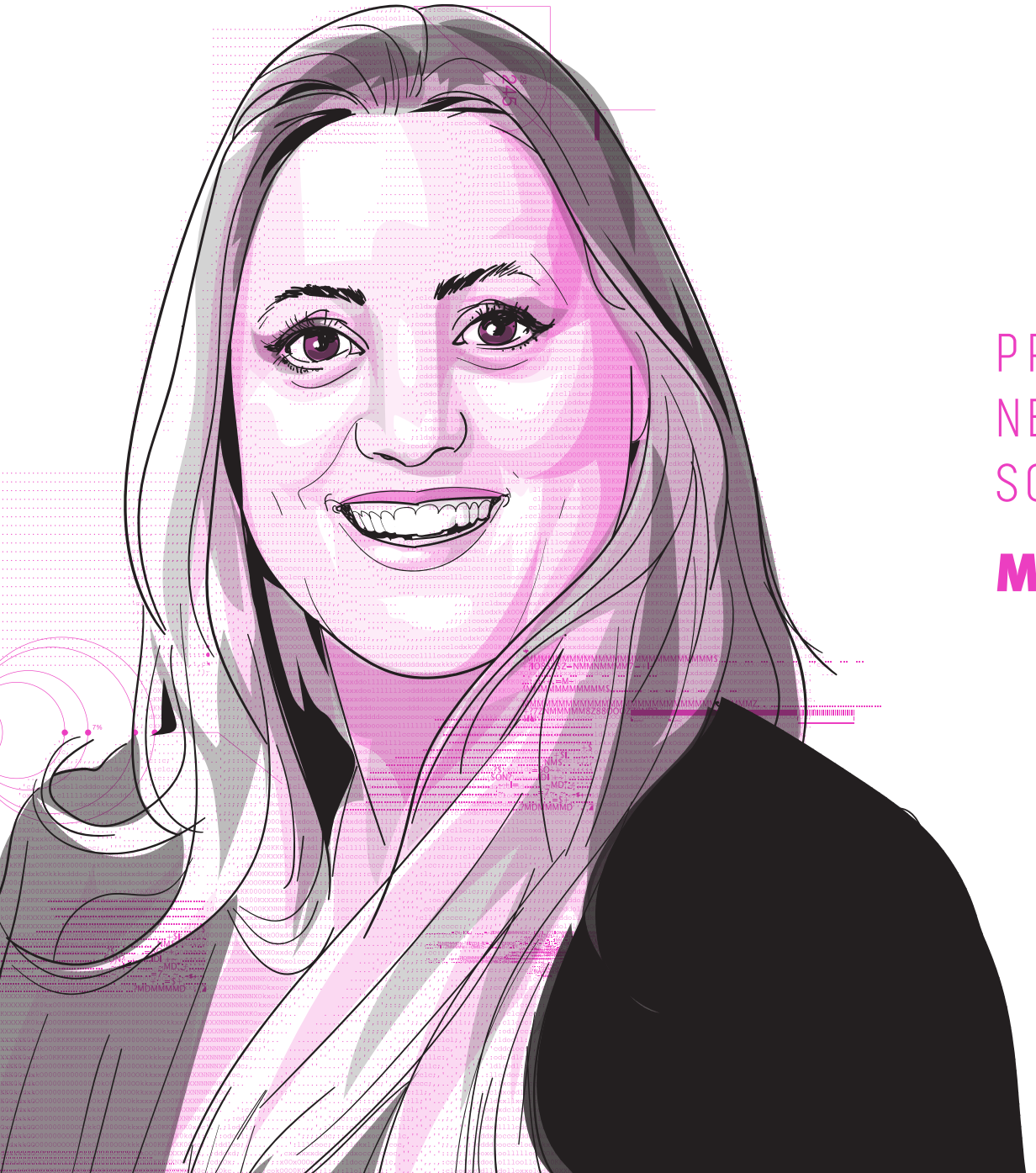
É perfeitamente possível ocorrerem erros honestos. Às vezes, até um perito com alguma habilidade pode, pelo manuseio equivocado do arquivo digital, ou por não empregar a melhor técnica, acabar manipulando erroneamente aquele dado e comprometendo a autenticidade e a integridade deste elemento de prova digital. Então, este me parece um ponto importante.

Assim, toda a discussão sobre a prova do enunciado, me parece, nas provas digitais, elas tenderão a se concentrar muito mais na fiabilidade da prova em si, isto é, daquilo que os espanhóis chamam de metaprova ou "prova sobre prova" do que propriamente no conteúdo da prova. Se eu vir um vídeo, eu entendo o que está passando no vídeo. Se eu leio um documento em PDF, eu sei qual é aquele conteúdo. Mas a questão é: esse era o conteúdo originário dele? Esse conteúdo era autêntico? Esse vídeo não foi criado por inteligência artificial? Hoje é possível, por exemplo, utilizar o conteúdo gravado dessa fala, em português, e transformá-lo em um vídeo, com o nosso rosto e a nossa voz, com a nossa boca mexendo corretamente, mas fazendo a mesma exposição em espanhol, francês ou inglês. É claro que aquele vídeo traduzido não é original, mas pode enganar muita gente. Então a integridade e a autenticidade da prova digital serão bastante importantes.

E o STJ decidiu, no que diz respeito à cadeia de custódia das provas normais, em caso relatado pelo Min. Rogério Schietti Cruz, no HC 653.515/RJ, envolvendo a questão de tráfico de drogas, no qual a droga teria sido colocada em um saco do supermercado, deu um nó e depois falou "essa foi a droga que foi apreendida com ele". O tribunal resolveu o problema na valoração e não na admissibilidade. Não se considerou que a prova era ilícita e, portanto, inadmissível. O que foi decidido é que se trata de prova que não tem potencial epistêmico algum, sendo impossível considerar que o que foi encontrado com a pessoa era ou não a droga que estava no saco plástico e foi periciada, absolvendo o acusado.

Por outro lado, especificamente no caso de prova digital, e acredito que seja a esse precedente que você se referia, Marina, o Ministro Ribeiro Dantas, no Agravo Regimental no RHC 143.169/RJ, considerou que a "autoridade policial responsável pela apreensão de um computador" – portanto, estamos falando de prova digital – "ou outro dispositivo de armazenamento de informações deve copiar integralmente, bit a bit, o conteúdo do dispositivo". E segue, no acórdão: tem que usar algoritmo hash e que com o hash é possível calcular a entrada e a saída para verificar a integridade do documento. E mais: "é ônus do Estado comprovar a integridade e a confiabilidade das fontes de prova por ele apresentadas", acrescentando que não cabe ao Poder Judiciário uma ideia de uma fé cega no outro órgão, simplesmente porque o órgão é estatal, o que ele chama de uma "auto proclamada confiança que o Estado-acusação deposita em si mesmo". No caso, como a polícia não havia documentado nenhum dos atos praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, concluiu-se que essas provas eram inadmissíveis e que também eram ilícitas as provas delas derivadas.

Portanto, mesmo antes de termos a lei, o Superior Tribunal de Justiça tem trabalhando com uma ideia de inadmissibilidade da prova digital que não tenha documentação da cadeia de custódia. Por quê? Porque sem essa comprovação de autenticidade e integridade, a fiabilidade epistêmica daquilo é praticamente um nada probatório.



02.

PROCESSO LEGISLATIVO: NECESSÁRIA ATUAÇÃO DA SOCIEDADE ACADÊMICA[1]

Marina Coelho Araújo

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Vitor Vilanova.

Agradeço à professora Marta Saad pelo convite e fiquei muito contente em participar do painel com Cleunice Pitombo, Gustavo Badaró e Anamara Osório.

Primeiro: falamos aqui de projeto legislativo. Eu confio e espero muito do nosso Congresso Nacional. Pode parecer difícil escrever isso, mas não é. Eu me envolvi durante dois anos semanalmente com o Poder Legislativo Nacional, entre 2021 e 2022, sobre o projeto de um novo Processo Penal (PL 8045/2010). E com tal experiência, trago minha conclusão de que a sociedade acadêmica pode – e deve – participar muito mais do processo legislativo nacional.

Sei que muito desta omissão diz sobre nossa compreensão a respeito do resultado, teria que ser perfeito, do nosso jeito. Para a academia, o Legislativo não poderia alterar o que foi feito pelos profissionais e não poderia utilizar aquele texto para negociações mútuas com todos os setores sociais. Não é assim que funciona a racionalidade legislativa. Não existe algo ideal, existe o resultado de um processo legislativo. E no Brasil, temos resultados muito positivos em várias questões. Não digo que é perfeitamente imaginado, mas muita coisa evoluiu em processo penal nos últimos anos nas casas legislativas.

Não foi o Legislativo que barrou e desconfigurou o juiz de garantias. O Supremo Tribunal Federal foi o responsável pela paralisação da implantação do instituto. Não acredito, pois, que levar os assuntos às Casas Legislativas seja colocar o tema em risco. Não enxergo assim, como muitos o fazem. E afirmo, ainda, que a percepção um tanto quanto generalizada de que "pode ficar pior do que está", muito diz respeito à sociedade civil e a nós acadêmicos, que podemos contribuir mais para que a discussão envolva aspectos relevantes e democráticos. A racionalidade legislativa de ponderação de interesses, de negociação, do que deve preponderar, é algo que não buscamos conhecer, nem estudar. Quais os custos das alterações legislativas, também não nos ocupamos em trazer às Casas.

Submeto, aqui, um exemplo. Provas digitais é um tema relevante e importante hoje. O projeto do deputado Hugo Leal (PSD/RJ - PL 4349/2020) não foi incorporado no substitutivo. Ele está apensado, mas ele não foi incorporado. O projeto da deputada Margarete Coelho (PP/PI), da cadeia de custódia, foi sugerido, está no quadro comparativo, mas não foi decidido pelo GT, que é o grupo de trabalho, extinto já, mas que deveria ter trabalhado esse tema. Não foi incluído, então, todo o conteúdo naquele projeto de reforma.

Pela nossa compreensão, o tema das provas digitais não poderia ser um capítulo à parte. Deve ser algo que remeta à própria compreensão da realidade da prova, de sua essência. Não existe prova digital e prova que não é digital. A lógica do fato hoje é uma lógica que compreende a digitalidade. Não tem como separar. Então o projeto de Código de Processo Penal está totalmente desatualizado nisso e teria que ser alterado neste sentido, com dispositivos de parte geral que reconhecessem esta situação.

Fizemos enorme esforço para inserir as provas digitais junto com as provas que não são digitais, porque é evidente que uma estará imbricada na outra, e as regras não podem ser diferentes. Trabalhamos também para inserir, como proposta do IBCCRIM (Instituto Brasileiro de Ciências Criminais), cinco princípios, o que foi feito em conjunto com vários professores de Processo Penal:

< I > a integridade
< II > a completude

< III > a autenticidade
< IV > a auditabilidade
< V > a reprodutibilidade dos métodos.

Analisando a perspectiva prática: uma prova é produzida pela autoridade policial, e vem ao Ministério Público e ao juízo só o relatório que a polícia fez. A prova completa, não vem. Só vem o relatório da polícia. Aí pede-se o completo, e a polícia não sabe onde está. Pergunta-se de onde que tirou isso, também não tem cadeia de custódia. "*Ah, não, mas eu ouvi, eu ouvi aqui, eu vi, eu li, eu tenho fé pública, eu sou policial*". Não, não pode! A prova tem que ser completa. A gente tem que ser auditável. E não me parece isto um problema de digitalidade só. Já teria que ser assim com a prova material. Vamos considerar que isso daí já é um problema prévio.

Essa questão de como a gente produz provas no Brasil nunca foi resolvida. Nós temos um Código Penal de 1940 e nós estamos em 2023, são quase 100 anos! Temos uma questão. O problema que nós temos no Código de Processo Penal não é digital. O problema que temos é muito mais amplo. A gente tem um projeto que não é e não está de forma nenhuma atualizado com a situação real da produção de provas, de como a gente quer o processo penal. Precisamos produzir este texto!

O sistema que temos aprofunda as desigualdades sociais e a seletividade social utilizando a justiça criminal. As formas de produção de prova dificultam a defesa e a proteção do cidadão frente ao Estado. Neste sentido, precisamos de regras que nos tragam as vantagens da tecnologia para ampliar o standard probatório, aumentar a segurança das condenações e diminuir a estrutura de opressão da máquina estatal. A sociedade acadêmica precisa construir estas soluções e levar à análise do Poder Legislativo.

/ NÃO EXISTE PROVA DIGITAL E PROVA QUE NÃO É DIGITAL. A LÓGICA DO FATO HOJE É UMA LÓGICA QUE COMPREENDE A DIGITALIDADE. NÃO TEM COMO SEPARAR /

A jurisprudência já tem se movimentado no sentido de criar regras para a produção de provas, abarcando a perspectiva digital. O STJ, na votação do RHC 143.169, decidiu pela nulidade de uma operação da polícia no Rio de Janeiro em razão da quebra da cadeia de custódia, utilizando-se de argumentos que não são, necessariamente, ligados à digitalidade. A cadeia de custódia integra o próprio conceito de vestígio, rastreabilidade.

O texto do projeto referido nomeia, por exemplo, o que são as provas digitais. Quais são as provas digitais? Aleatoriamente o texto enumera: dispositivo eletrônico, sistema informático, protocolos de rede. Reflete algo da Convenção do Cibercrime (de Budapeste): protocolo de rede, rede de dados, pacote de dados, dados em transmissão, dados em repouso. Refere, ainda, a prova nato-digital. Essa é outra questão discutível: prova digitalizada é prova digital? Mas enfim, o que difere prova digital de prova digitalizada? O projeto de texto legal não evidencia isto.

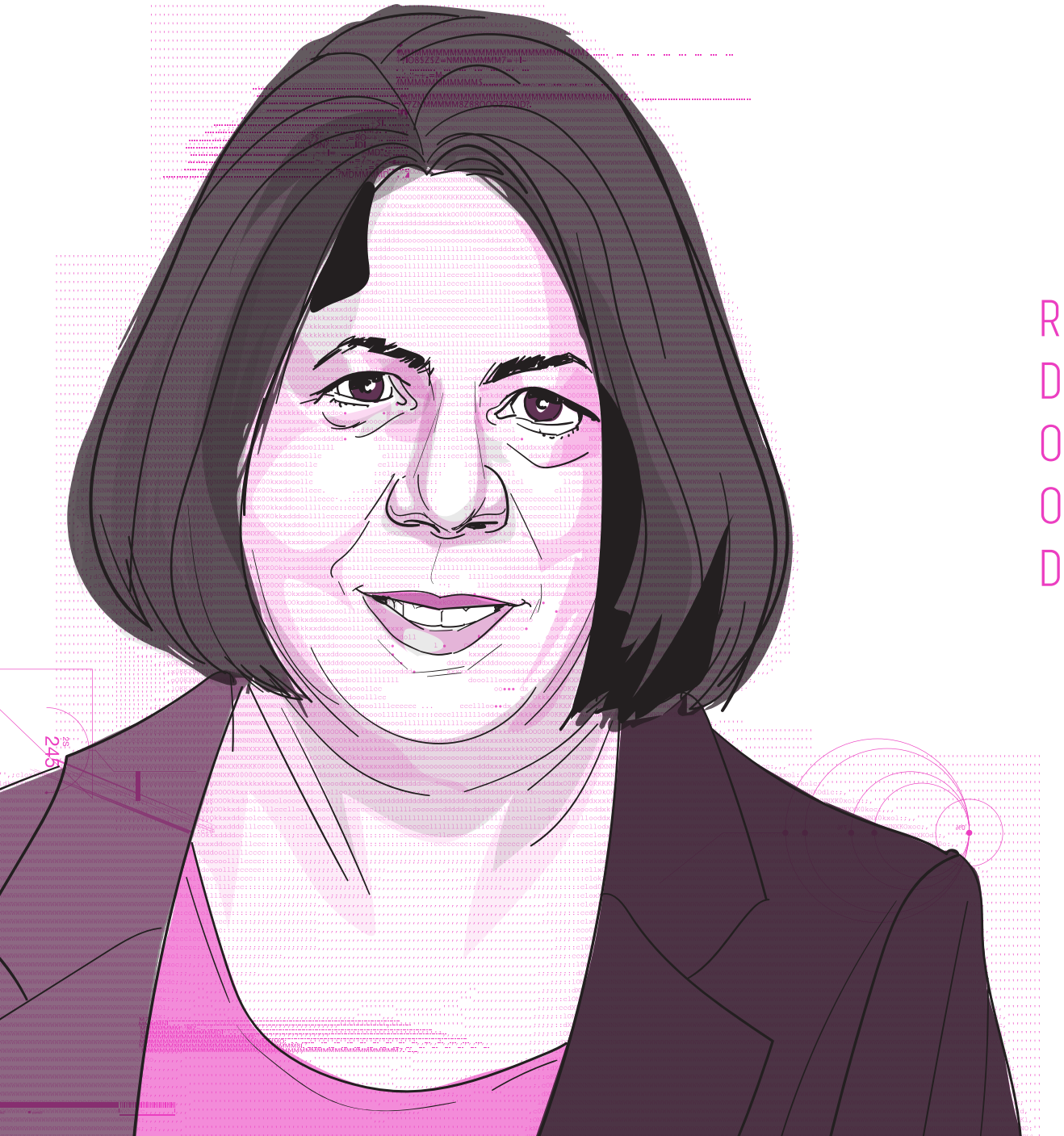
Tem um tema discutido em artigo da professora Maria Thereza de Assis Moura e do Daniel Barbosa Marchionatti[2] que aloca a discussão sob a perspectiva constitucional, o que traz à superfície a necessidade de se organizar sistematicamente os conceitos e assim os considerar nas discussões legislativas. Não se pode alocar textos em projetos de lei que não respeitem a sistemática constitucional.

2. MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In: LUCON, Paulo Henrique dos Santos et al. (coord.). **Direito, processo e tecnologia**. São Paulo: Revista dos Tribunais, 2020. p. 477-502.

E por fim: falta para nossa estrutura legal uma legislação de LGPD Penal. A LGPD Penal seria muito relevante para reconhecer algumas diretrizes para a análise dos sistemas e das questões de prova, principalmente digital. Algumas molduras precisam ser definidas sobre a questão de dados, proteção de dados e a estrutura de inteligência artificial, para daí evoluirmos para conceitos de limites e racionalidade na produção das provas.

O processo penal busca descortinar a verdade dos fatos. Precisamos enfrentar, no direito penal, a absoluta inexistência e impossibilidade de um contexto de verdade na estrutura digital e de inteligência artificial com os mesmos parâmetros com que sempre trabalhamos. Como estruturamos os nossos paradigmas de processo se eu não sei se aquela fotografia é real? Um dia desses uma pessoa me mostrou uma foto e disse: "olha que legal, a gente fez um almoço de família, minha mãe não quis ir, mas a gente colocou ela na foto". E a mãe estava lá. Como a gente vai lidar com isso?

Precisamos entender de onde vamos partir. Proponho o ponto de partida da lei. Construir parâmetros e conceitos legais que possam reduzir a complexidade na interpretação da realidade concreta pode ser muito produtivo a reduzir a litigiosidade e os problemas do convívio social. É por isto que conclamo a academia a trabalhar neste modelo, e contribuir, para um novo padrão de Processo Penal que envolva a digitalidade como essência dos fatos hoje *sub judice*. Vamos unir mais uma vez a Academia e o Poder Legislativo a enfrentar um tema tão complexo e tão desafiador.



03.

REFORMA DO CÓDIGO DE PROCESSO PENAL: OBSERVAÇÕES SOBRE OS MEIOS DE OBTENÇÃO DE PROVA DIGITAL[1]

Cleunice Pitombo

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Camilly Vitória Silva.

Bom dia. Em primeiro lugar, eu quero cumprimentar o InternetLab por esse seminário, que é extremamente importante para as discussões sobre direito e tecnologia. Quero agradecer e cumprimentar a professora Marta Saad, que é a grande patrona deste evento e saudar os meus colegas de mesa Professor Gustavo Badaró, Anamara Osório, Marina Coelho e Bárbara Simão.

O tempo para a exposição é curto, são apenas dez, quinze minutos, então, vamos tentar apresentar a proposta de Código de Processo Penal em discussão no Congresso Nacional trazendo uma breve cronologia da sua tramitação.

A proposta de reforma do Código de Processo Penal começou no Senado Federal com o PL 156 de 2009, após a tramitação no Senado o projeto foi enviado à Câmara dos Deputados e recebeu o número de PL 8.045 de 2010. O projeto foi discutido, recebeu várias emendas e sugestões da sociedade civil, porém, ele ficou parado sem tramitação por vários anos. Em 2021, a Câmara dos Deputados instituiu um Grupo de Trabalho para elaborar proposição legislativa do Novo Código de Processo Penal, sob a coordenação da Deputada Margarete Coelho e relatoria do Deputado João Campos. Nós estamos, portanto, falando de um projeto que tem 13 anos.

Vejam a idade do projeto de Código de Processo Penal que nós estamos analisando. Depois de tanto tempo, quantas mudanças legislativas significativas não surgiram? Além disso, quantas novas leis foram incorporadas ao Código de Processo Penal, modificando, inclusive, a estrutura do processo penal? Apenas para exemplificar, podemos destacar a Lei 13.964/19 que introduziu o juiz de garantias e a cadeia de custódia.

Em 30/07/2021, o Deputado João Campos apresentou um substitutivo ao PL 8045/2010. E como o processo legislativo tem uma lógica muito própria, algumas discussões e propostas realizadas no PL 8045, não foram incorporadas e novas propostas surgiram nesse substitutivo do Deputado João Campos. Causou surpresa, quando nós fomos pegar o projeto para ler, surgiram novos e desconhecidos dispositivos legais. Assim, a lógica na tramitação legislativa é uma das primeiras dificuldades na análise de projetos de lei. Nem sempre o projeto que estava sendo discutido, recebendo emendas, é o projeto levado à votação nas Comissões.

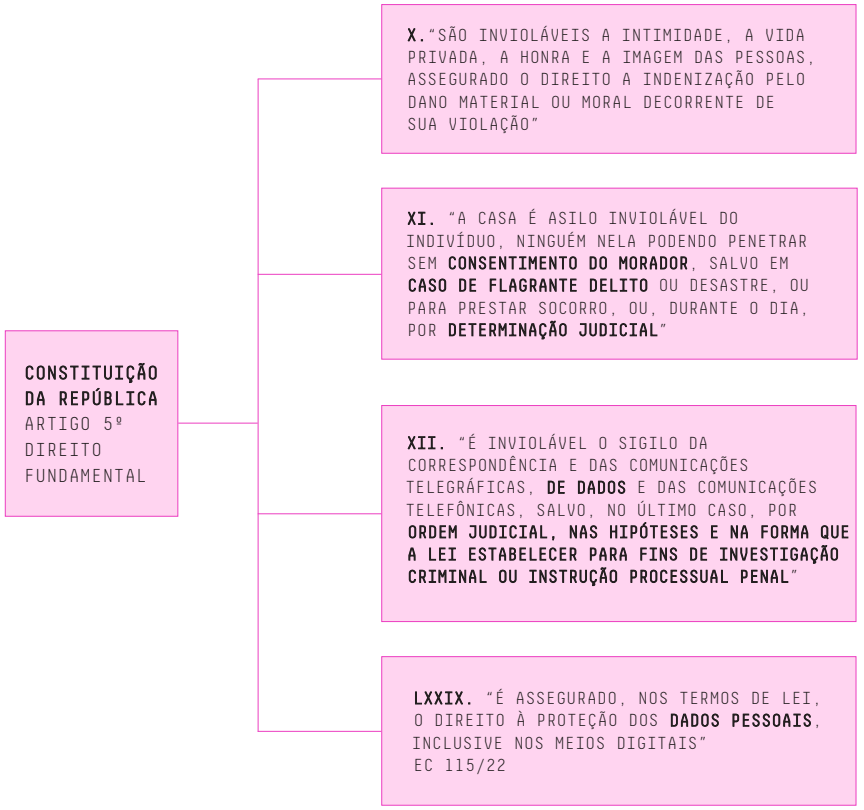
No tocante às provas digitais, o que há de novo em relação ao projeto de 2010? Em 2021, foram incorporados ao substitutivo do Deputado João Campos, um projeto do deputado Hugo Leal (PL 4939/20) que tramitava em separado no Congresso Nacional e outro da deputada Margarete Coelho (PL 4291/20). O primeiro projeto mencionado cuida de provas digitais, disciplinando em particular a busca e apreensão de dados digitais e o segundo dispõe sobre a cadeia de custódia dos elementos contidos em sistemas computacionais.

Por que eu estou dizendo isso? Eu acho que todo mundo que tentou procurar os projetos que estão sendo discutidos no Congresso Nacional, percebe que é extremamente difícil. Você não sabe onde acha, como acha, ou o que foi inserido e o que não foi inserido. Então, sobre provas digitais, basicamente nós estamos tratando do PL 4939/2020 do Deputado Hugo Leal, do PL 4921/2020 da Deputada Margarete Coelho e da versão antiga sobre meios de obtenção de prova existente no PL 8045/2010.

Ultrapassado esse aspecto formal, eu gostaria de trazer aqui o que a Constituição prevê e o que deve regrar a discussão sobre a reforma do Código de Processo Penal.

A análise deve partir das garantias constitucionais, especialmente aplicáveis à produção da prova digital, que são: a inviolabilidade da intimidade, a inviolabilidade da casa, a inviolabilidade das correspondências, mas, em particular, é

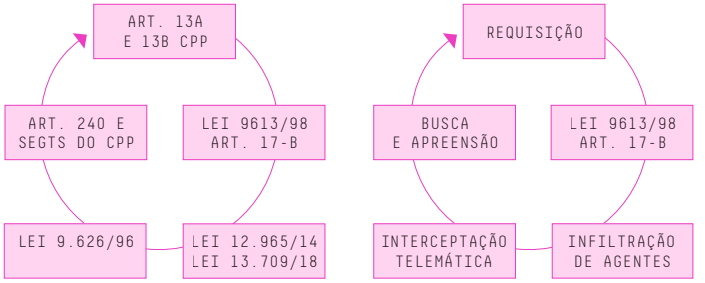
necessário dar destaque ao novo direito fundamental que foi inserido pela Emenda Constitucional 115 de 2022, que assegura textualmente a proteção dos dados pessoais, inclusive em meios digitais. Portanto, dados pessoais, assim como os outros dados, estão protegidos. É direito fundamental. Se é direito fundamental, ele só pode ter restrições diante da estrita legalidade. Assim, toda a reforma do Código de Processo Penal, em especial no tocante às provas digitais, deve observar este novo direito fundamental.



Há também em trâmite no Congresso Nacional a PEC 86 de 2015, que assegura a inviolabilidade do sigilo das comunicações realizadas por meios digitais. No dia 9 de agosto, ela foi discutida na Comissão de Justiça, foi aprovada com votos divergentes, mas de qualquer forma, nós não podemos ignorar essa PEC. Assim, a discussão sobre prova digital deve ter este enfoque constitucional.

Depois, devemos olhar para o panorama legal em vigor e verificar quais são as normas que regem ou disciplinam a obtenção de prova, prova física ou prova digital. Este é o conjunto de normas que hoje nós trabalhamos para obtenção das provas.

LEGISLAÇÃO APLICÁVEL
PROCURA, OBTENÇÃO, REMOÇÃO E GUARDA DE DADOS DIGITAIS



E vejam, neste conjunto de normas se faz, na verdade, uma interpretação extensiva, analógica - eu não sei qual o termo que nós daríamos para isso, professor Gustavo -, mas na verdade se faz aí uma composição de leis para se obter provas digitais.

E aqui começa a primeira questão de duvidosa legalidade sobre este arranjo legislativo para obtenção de provas, especialmente provas digitais, quando na verdade nós estamos falando de direito fundamental. Este é o panorama para sabermos um pouco sobre o que estamos falando: a garantia constitucional e a inexistência de uma lei ordinária específica disciplinadoras de hipóteses de restrição ao direito fundamental, no tocante às provas digitais.

Atualmente, há total ausência de disciplina. E mais, assim como se falou aqui nos painéis anteriores, todas as provas hoje são digitais. Praticamente todas. Não dá mais para falarmos em processo penal sem discutirmos a estrita legalidade na obtenção da prova digital. O novo código deve olhar o presente e mirar o futuro. O projeto de reforma que estamos discutindo, porém, está totalmente ultrapassado e velho. Parece uma colcha de retalhos que reúne um sistema analógico e outro digital, nos meios de obtenção de prova.

Vejam que o projeto no capítulo III cuida dos seguintes **meios de obtenção de provas**:

< I > da busca e da apreensão pessoal e domiciliar (Seção I, art. 263/274);

< II > acesso a informações sigilosas e a dados cadastrais (Seção II, art. 275/279),

< III > interceptação das comunicações telefônicas e da localização de celular (Seção III, art. 280/297);

< III.1 > fluxo de comunicação em sistemas de informática e telemática;

/ VEJAM A IDADE DO PROJETO DE CPP QUE NÓS ESTAMOS ANALISANDO. DEPOIS DE TANTO TEMPO, QUANTAS MUDANÇAS LEGISLATIVAS SIGNIFICATIVAS NÃO SURGIRAM? /

/ EM PRIMEIRO LUGAR, É PRECISO UNIFICAR OS MEIOS DE OBTENÇÃO DE PROVA EM UM ÚNICO CAPÍTULO /

< III.2 > outras formas de comunicação por transmissão de dados, sinais, sons ou imagens;

< III.3 > ambiental de sinais eletromagnéticos;

< IV > localização de sinal de aparelho móvel (art. 297).

No Capítulo IV, porém, o projeto disciplina os seguintes **meios de obtenção da prova digital**:

< I > a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo;

< II > a coleta remota, oculta ou não, de dados em repouso acessados à distância;

< III > a interceptação telemática de dados em transmissão (Seção II);

< IV > a coleta por acesso forçado de sistema informático ou de redes de dados (Seção IV, 307);

< V > o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.

Em primeiro lugar, é preciso unificar os meios de obtenção de prova em um único Capítulo.

É imprescindível que se discuta efetivamente quais são os meios de provas admissíveis em face da Constituição e quais são os necessários em face do avanço tecnológico. Lembrando

que alguns desses institutos e meios de provas estão apenas com o título. Não há disciplina. "Já ouvi falar nisso, coloquei aqui", mas não há uma disciplina efetiva. Alguns dizem "Bom, mas qual disciplina?". É imprescindível. Não adianta nominar um meio de obtenção prova sem disciplinar os seus limites e requisitos.

No tocante ao aspecto formal, seria preferível algumas mudanças na estrutura do projeto, por exemplo:

< 1 > Incluir no Capítulo I, "Das disposições gerais" (art. 194 a 199) as disposições gerais relativas à prova digital, que estão sendo tratadas no Capítulo IV (art. 298 a 303);

< 2 > Unificar a disciplina da cadeia de custódia das provas materiais (art. 200 a 204) e a cadeia de custódia específica da prova digital tratada na Seção VII, do Capítulo VI (art. 313 a 316);

< 3 > Inserir na Seção V, "da prova pericial e do exame de corpo de delito" (art. 236 a 256) a perícia nas provas digitais;

< 4 > Uniformizar a disciplina da "busca e da apreensão" pessoal e domiciliar, em meio físico (art. 263 a 274) com a "busca e apreensão em dispositivos eletrônicos" (art. 304);

< 5 > Englobar em um só título a "interceptação das comunicações telefônicas e da localização de aparelho móvel celular" (art. 280 a 297) e a "interceptação telemática de dados em transmissão" (art. 305 e 306).

O maior problema, porém, está na eleição de quais tipos de meio de obtenção de prova serão admissíveis no nosso sistema jurídico. Destaco, para reflexão, alguns pontos que devem ser observados na escolha dos meios de obtenção de prova:

< 1 > Observar a estrita legalidade (material e formal);

< 2 > Assegurar a reserva de jurisdição, adequação, necessidade e proporcionalidade estrita, subsidiariedade e indispensabilidade da restrição de direito fundamental;

< 3 > Trazer um catálogo fechado de tipos penais e graduar os tipos de meios de obtenção de prova admissíveis, observando o disposto na Convenção de Budapeste;

< 4 > Suprimir os meios ocultos de obtenção de prova (a coleta remota, oculta ou não, de dados em repouso acessados à distância e a coleta por acesso forçado de sistema informático ou de redes de dados);

< 5 > Disciplinar as hipóteses de uso da inteligência artificial.

Outro aspecto relevante, que não foi tratado no projeto de reforma, é dar um tratamento moderno à busca e à apreensão. A tutela do espaço físico (inviolabilidade do domicílio) não consegue abranger o espaço virtual e disciplinar os limites legais para a busca de dados digitais.

É imprescindível hoje, mais do que nunca, dar autonomia aos institutos da busca e da apreensão. Tradicionalmente, eles sempre tiveram um tratamento legislativo único. Na verdade, a apreensão nunca foi tratada, ela é o apenso do instituto da busca.

Agora, é imprescindível que a apreensão seja disciplinada de modo mais claro e objetivo. Até porque, no tocante às provas digitais, a apreensão muitas vezes ocorre de modo autônomo, independente da busca e, em outros casos, os clássicos requi-

sitos da inviolabilidade da casa, aplicáveis à busca e apreensão não são compatíveis com a obtenção de prova digital.

A clássica busca, na maioria das hipóteses, volta-se para apreender, para reter e para custodiar elementos materiais. Porém, pode ocorrer a apreensão (por exemplo de aparelho celular) para buscar, para encontrar prova ou elemento de prova contido no bem apreendido.

Assim, não é mais possível vincular a legalidade da apreensão à da busca nos moldes tradicionais. A apreensão deve ter requisitos de legalidade específicos e lhe ser assegurada uma cadeia de custódia.

Lembrem-se que estamos nos referindo à persecução penal efetiva. Não àquela busca para a segurança pública. Investiga-se, portanto, fato certo e determinado, assim, a busca, após a apreensão dos dados digitais, precisa ser certa, determinada e com requisitos muito bem definidos. Inadmissível devassa geral e ilimitada.

Imaginem a seguinte situação: Apreendido um aparelho eletrônico (computador, tablet, smartphone) inicia-se a pesquisa, a busca, de provas e elementos de prova. Quais são os limites legais dessa busca? Não há. Eu posso com palavras chaves, nesta imensidão de dados que eu tenho, criar uma história e excluir a outra, dar uma versão e tirar a outra. Então é preciso - é imprescindível - que se tenha uma disciplina específica do que é busca, o que é procura, e do que é apreensão. O que é esta efetiva retenção para a busca posterior?

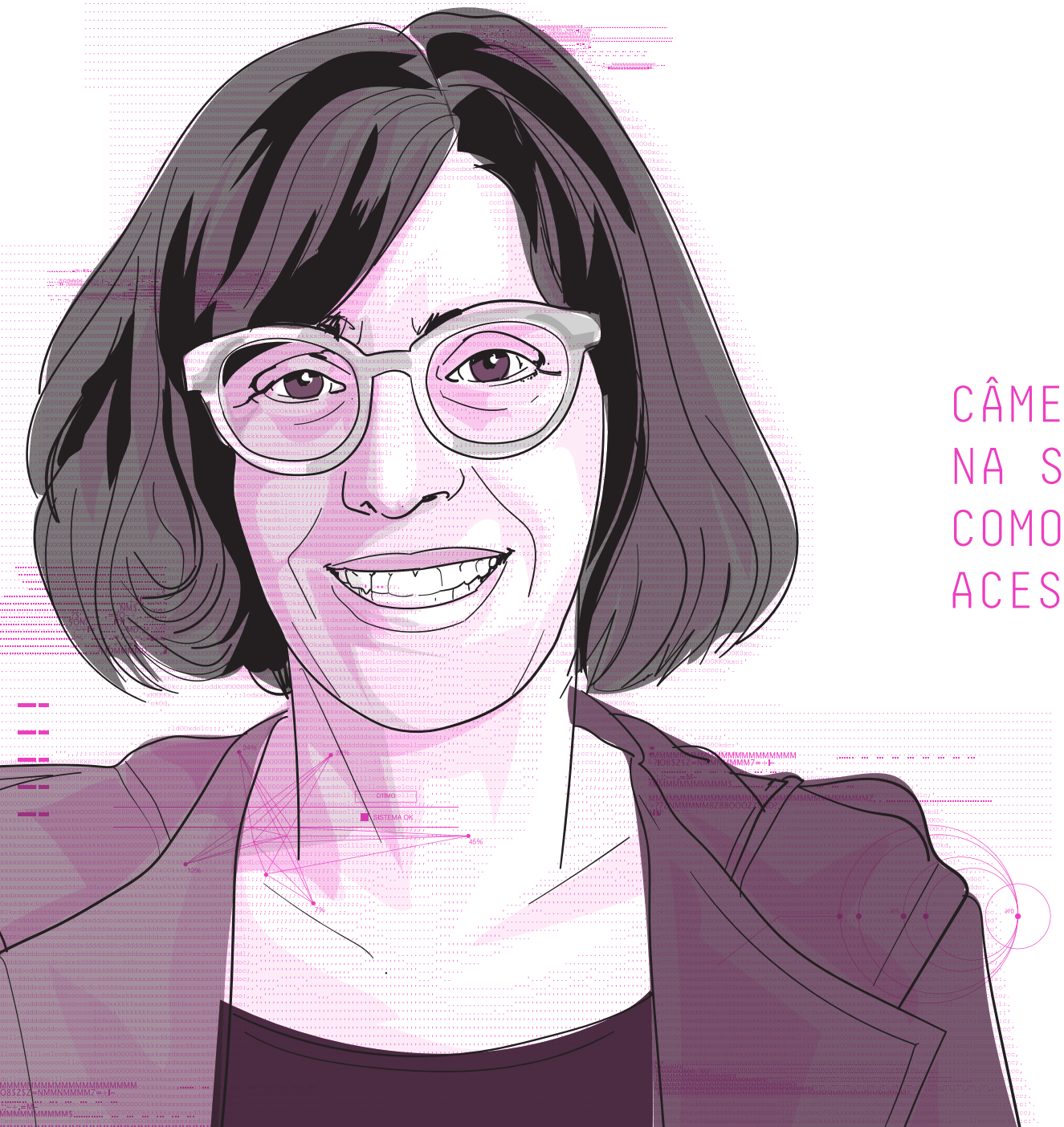
Bem, já me mandaram concluir, mas eu gostaria de deixar este alerta maior.

Não se pode tratar mais de um Código de Processo Penal analógico e um digital. Processo penal vai ser um só: digital. É preciso unificar e é preciso modificar, em particular o instituto da busca e da apreensão.

Outro importante exemplo, refere-se a apreensão do aparelho celular. Não é possível enquadrá-la na modalidade de busca pessoal ou busca domiciliar na análise da legalidade ou ilegalidade do que se apreendeu. Não é nada disso, até porque a apreensão pode decorrer da entrega voluntária. É a apreensão (instituto autônomo) de um aparelho móvel e os requisitos para obtenção dos dados contidos nesta apreensão, devem e precisam ter disciplina própria. O projeto do novo Código de Processo Penal não se preocupou com o assunto.

É urgente e necessário dar autonomia ao instituto da apreensão e disciplinar, considerando as especificidades, a Busca e a Apreensão. Me parece que daríamos um grande passo para assegurar a legalidade na obtenção das provas digitais.

Bom, acho que era isso que eu tinha, num primeiro momento, para trazer à discussão. Obrigada.



04.

CÂMERAS CORPORAIS NA SEGURANÇA PÚBLICA COMO POLÍTICA DE ACESSO À JUSTIÇA

Juliana Vieira dos Santos

A violência e o autoritarismo marcam profundamente a sociedade brasileira. O Brasil experimentou longos regimes ditatoriais, manteve traços da larga tradição colonial e conservou as marcas do escravismo e do patrimonialismo patriarcal.

Sem aprofundar as opções políticas republicanas e democráticas, e aderindo a transições incompletas e superficiais, o Brasil foi acumulando ao longo do tempo sucessivas pactuações entre as elites nacionais e afastando as opções de transformação social e de reformas significativas em suas instituições. Formou-se um país caracterizado por uma acentuada distância entre a direção política e as maiorias sociais e por uma série de obstáculos ao efetivo e pleno exercício da cidadania política e social.

O escravismo legou ao Brasil uma forte tolerância social com práticas de violência, em especial de controle físico exercido no espaço público ou privado. Há uma forte conivência com o controle dos corpos das pessoas negras. Convive-se com o racismo e com expressivas taxas de letalidade responsáveis pela morte de centenas de jovens negros do sexo masculino por disparos de arma de fogo; convive-se com a desigualdade de renda e acesso a direitos; convive-se com a violência e o autoritarismo.[1]

A ação das polícias nas cidades brasileiras, refletem e são forjadas por esse contexto, em que a gestão do espaço público se faz por meio do acionamento estrutural da violência, física e simbólica, especialmente contra pessoas negras. Como ensina Felipe Freitas, esse processo se dá em forte cooperação com o sistema de justiça criminal e é homologado em sentenças judiciais de absolvição de responsáveis por execuções, em validação de flagrantes ilegais ou no arquivamento dos autos de resistência.[2]

1. CARDOSO JR. José Celso [et al] (Org.). *Assédio institucional no Brasil: Avanço do Autoritarismo e Desconstrução do Estado*. Brasília, DF : Associação dos Funcionários do Ipea : EDUEPB, 2022. Disponível em https://laut.org.br/wp-content/uploads/2022/06/Assedio-Institucional-no-Brasil_-Avanco-do-Autoritarismo-e-Desconstrucao-do-Estado.pdf

A construção de políticas públicas na área de segurança pública passa, portanto e necessariamente, por reconhecer essa realidade e pensar formas efetivas para transformá-la.

O uso das câmeras corporais é um tipo de política pública que conecta dois conceitos importantíssimos na área de segurança pública e justiça.

O primeiro deles é exatamente a compreensão de que políticas públicas de segurança pública (e as forças policiais) são parte integrante de um Sistema de Justiça que precisa ser acessado de forma justa e igualitária por todos e todas. Trata-se de políticas de acesso à justiça. E o segundo é a construção de políticas públicas baseada em evidências.

2. FREITAS, Felipe. Polícia e Racismo: uma discussão sobre mandato policial. 2020. 264 f., il. Tese (Doutorado em Direito) - Universidade de Brasília, Brasília, 2020. Disponível em http://www.realp.unb.br/jspui/handle/10482/38911?locale=en

Primeiro, portanto, vamos explorar o conceito de acesso à Justiça.

Os primeiros debates, projetos e soluções que emergem, lá por volta do final dos anos 60, relacionadas a esse tema, têm uma compreensão restritiva de acesso à justiça, adotando um viés de assistência judiciária. A necessidade de fazer com que comunidades mais vulneráveis tivessem apoio para levar as suas demandas individualmente ao Poder Judiciário, bem como exercer seu direito de defesa. Na época, essa visão sugeria uma mudança significativa da compreensão do Estado (de uma passividade opressora para garantidor do acesso, em termos de quem paga a conta). Aí surge a advocacia dativa, surgem as defensorias (em 1977 é implementada a primeira defensoria no Brasil, no Rio de Janeiro).

Uma segunda onda no movimento de acesso à justiça tinha por objetivo aperfeiçoar o acesso enquanto ferramenta para resguardar os interesses de uma forma coletiva, ou seja, aqueles direitos que tangem a todos e a grupos específicos. São feitas reformas legislativas tendentes a proporcionar representação jurídica para os interesses "difusos", especialmente nas áreas da proteção ambiental e do consumidor, no final dos anos 80. Em 1990, o código de defesa do consumidor. Em 1985, a lei da ação pública. A própria Constituição Federal, de 1988, traz elementos dessa segunda onda, com as previsões de legitimação coletiva para impetração de mandado de segurança, por exemplo.

Um terceiro movimento na ampliação da compreensão do acesso à Justiça (inicialmente proposto por Cappelletti e Garth nos anos 70[3]), é denominada simplesmente de "enfoque de acesso à justiça" porque inclui os posicionamentos anteriores, mas vai muito além deles, representando uma tentativa de atacar as barreiras ao acesso de modo mais articulado e compreensivo. O "enfoque do acesso à justiça" se referia a mudanças na forma de acesso e no próprio conteúdo da prestação jurisdicional, visando a sua efetividade, e se referiam tanto à instituição de assistência judiciária gratuita aos menos favorecidos, quanto à representação dos interesses difusos.

3. CAPPELLETTI, Mauro; GARTH, Bryant. *Acesso à justiça*. Porto Alegre: Fabris, 1988, p. 7-73.

Aqui no Brasil observamos uma série de medidas para atacar os problemas para quem acessa a Justiça (tais como as questões de morosidade, de falta de eficiência etc.). É nesse sentido que vivenciamos a Reforma do Judiciário, em 2004, a partir da Emenda Constitucional nº 45, que cria o CNJ, por exemplo, com o objetivo de aperfeiçoar o controle e a transparência administrativa do Poder Judiciário. O CNJ passa a

/ O ENFRENTAMENTO DA QUESTÃO DO ACESSO À JUSTIÇA DEVE SER ANTECEDIDO POR OUTRAS, MAIS BÁSICAS, TAIS COMO DESIGUALDADE SOCIAL /

/ AS CÂMERAS SÃO UMA TECNOLOGIA. SE BEM USADA, ELA VAI ESTAR A SERVIÇO DA CIDADANIA. SE MAL USADA, ELA VAI SER UM IMENSO DESPERDÍCIO DE RECURSO PÚBLICO /

uniformizar os procedimentos judiciais nos tribunais do País, estabelecer metas de produtividade, entre outras medidas.

A compreensão de acesso à Justiça continua evoluindo para além das ferramentas para se chegar ao sistema de justiça ou fazer com que o sistema de justiça funcione a contento.

Um novo passo nessa evolução é dado com os Objetivos de Desenvolvimento sustentável, a Agenda 2030,[4] de que o Brasil é signatário. O ODS #16 (Paz, Justiça e Instituições eficazes) é o que consagra o acesso à Justiça. E ali se define melhor e se estabelece o conceito de acesso à Justiça para compreender que o desequilíbrio na distribuição de renda tem consequências nefastas, e as barreiras de acesso à justiça acabam por contribuir com um resultado de perpetuação da desigualdade. O enfrentamento da questão do acesso à justiça deve ser antecedido por outras, mais básicas, tais como desigualdade social, acesso à educação, alívio da pobreza, dentre outras.

4. Disponível em: https://brasil.un.org/pt-br/sdgs.

É nesse ODS #16 da ONU que está prevista a redução significativa de todas as formas de violência e das taxas de mortalidade relacionada em todos os lugares. Acabar com abuso, exploração, tráfico e todas as formas de violência e tortura contra crianças. A promoção do Estado de Direito, garantindo a igualdade de acesso à justiça para todos. O fornecimento de identidade legal para todos. A redução significativa do fluxo de armas ilegais, da corrupção e o suborno em todas as suas formas, do desenvolvimento de instituições eficazes, responsáveis e transparentes em todos os níveis.

Esse é o patamar civilizatório que deve ser almejado.

Nessa mesma toada, um outro documento internacional, o Relatório da OCDE "Acesso à Justiça Equitativa para Cresci-

mento Inclusivo: colocando pessoas no centro",[5] serve para conectar a questão da Justiça com as câmeras corporais, a partir de uma compreensão de acesso à justiça ampliada.

Esse relatório de 2019, que conta com mais de cinco anos de pesquisa e colaboração de Membros da OCDE e países parceiros, com foco nos passos necessários para proporcionar acesso à justiça para todos. Esses passos começam por uma melhor compreensão de que o sistema de justiça é um serviço. E que ele precisa ser prestado de forma a atender as necessidades de quem vai usar esse sistema.

Mas para que se preste um bom serviço, é necessário: ter equipamentos adequados, ter profissionais adequados e bem treinados.

A atividade policial faz parte do sistema de acesso à Justiça, nesse conceito ampliado.

E dentro desse conceito apresentam-se dois pontos: fortalecer as instituições policiais, porque o uso da força feito de forma adequada é estruturante para a manutenção do Estado Democrático de Direito, para o combate ao crime organizado, para a pacificação dos conflitos. Mas o profissional precisa estar bem treinado (e precisa ter os equipamentos adequados para fazer o bom uso da força). E de outro lado, a prestação de contas e a transparência das atividades policiais também integram esse patamar civilizatório de ampliação do acesso à Justiça.

O projeto de implementação do uso de câmeras corporais nas fardas dos agentes de segurança pública tem o objetivo geral de aumentar a transparência das operações e abordagens policiais. E objetivos específicos de:

5. OECD, 2019. Equal Access do Justice for Inclusive Growth: Putting People at the Centre). Página 20. Disponível em https://www.oecd-ilibrary.org/governance/equal-access-to-justice-for-inclusive-growth_597f5b7f-en

- Fornecer proteção jurídica para policiais e usuários.
- Melhorar a qualidade das provas coletadas durante as abordagens policiais.
- Auxiliar no processo de treinamento e desenvolvimento.
- Auxiliar os centros de comando e controle.

Esse é um projeto que vem sendo construído com muito cuidado dentro do Ministério da Justiça e Segurança Pública, em um processo de aperfeiçoamento e profissionalização da segurança pública e de construção de uma política de segurança pública baseada em evidências.

Nesse sentido, existem mais de 100 estudos sobre efeitos das câmeras corporais ao redor do mundo. O Ministério da Justiça e Segurança Pública contratou um estudo para fazer esse levantamento.[6]

Existem evidências muito concretas de que o uso das câmeras leva a uma redução de 60% de várias formas de uso da força. Esses são estudos de 2014 e 2015 (na Califórnia e na Flórida), mas também nos estados de Santa Catarina e São Paulo os dados são similares (aqui a gente está falando do uso não justificado da força). Há uma desescalada do uso da força seja por conta da própria conduta do policial, mas também por conta do cidadão que está sendo filmado.

6. SOUZA, Pedro C. L (consultor). Câmeras Corporais: uma revisão bibliográfica e documental. Brasília: Secretaria Nacional de Segurança Pública, 2024 (Serie Diagnósticos).

Os estudos sugerem que as câmeras afetam a dinâmica da situação ao prevenir a escalada da tensão que iria se desdobrar durante operações de rotina.

O Programa Olho Vivo em SP, que está sendo descontinuado pelo atual Governo do Estado, demonstrou que houve uma redução da letalidade policial em 57,1% e lesões corporais decorrentes de intervenção policial em 62,3%.

Mas o dado mais impactante é o efeito disso sobre a população negra. Um estudo de 2023 da UNICEF em conjunto com o Fórum Brasileiro de Segurança Pública, também sobre o exemplo de São Paulo, mostrou que a adoção das câmeras reduziu em 66% a letalidade de jovens negros mortos por agentes do estado. Esse número realmente é impactante. 102 adolescentes morreram no estado de São Paulo após intervenções policiais em 2019, quando o dispositivo não era usado. Em 2022, com a tecnologia adotada por 62 dos 135 batalhões do estado, esse número caiu para 34. Pelo menos 60 jovens negros tiveram suas vidas salvas em razão dessa política.

Mas a redução do uso da força é também associada a um menor risco da atividade policial. Aí há um aspecto muito interessante sobre as evidências que demonstram que as câmeras são uma ferramenta de proteção do próprio policial. As reclamações sobre a conduta policial em alguns estudos chegam a ter uma redução de 60%, e até 90% em outros.

Aqui é identificado um impacto econômico significativo, porque o custo de um processo administrativo disciplinar é alto (seja em pessoal mobilizado para esse fim, mas também um custo psíquico daquele profissional que fica meses angustiado para ter uma solução). Com as câmeras, o número de reclamações falsas cai, e se tem evidências e qualidade de prova muito mais robustas.

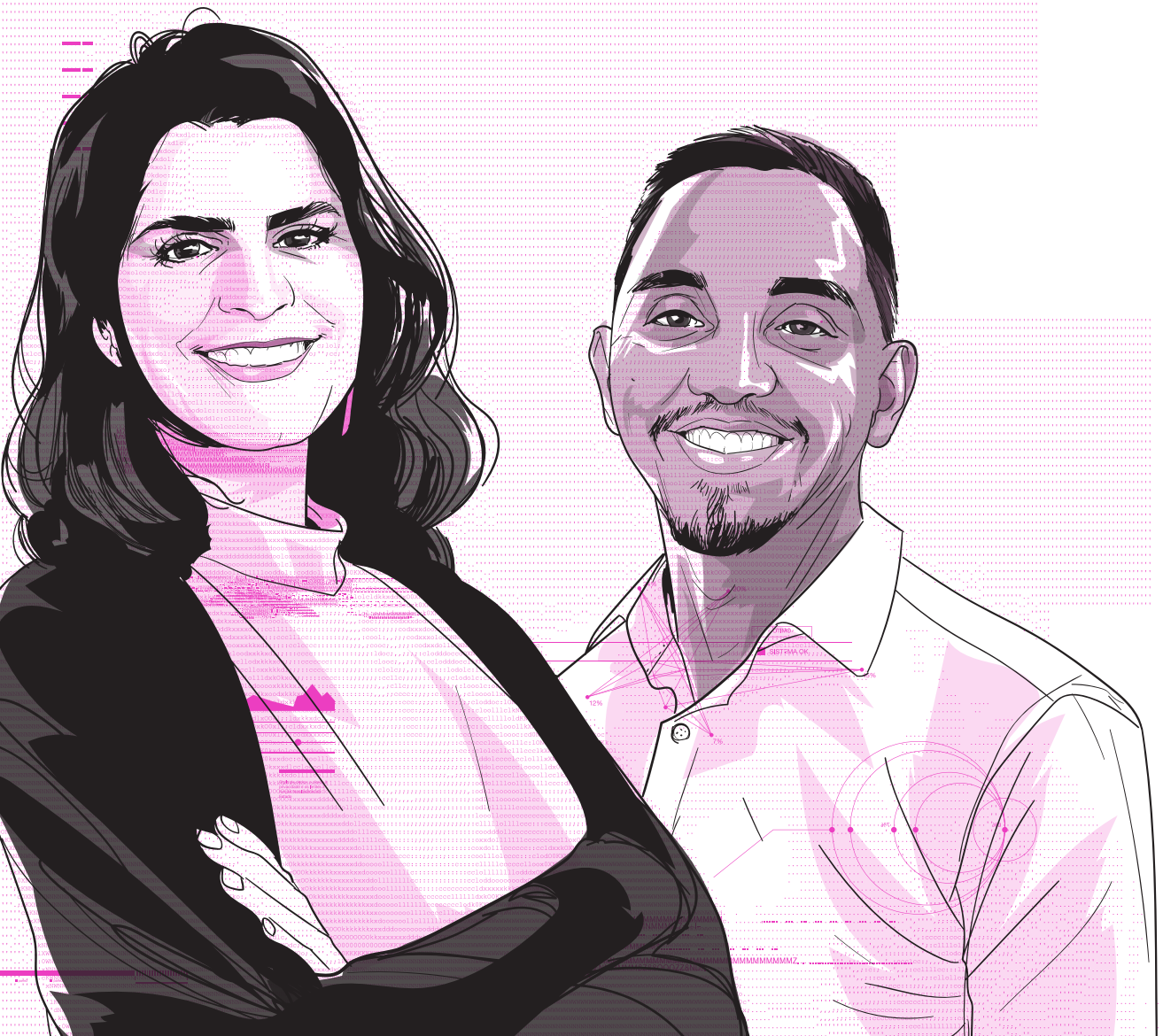
Do ponto de vista de acesso à justiça: os estudos internacionais evidenciaram aumento médio de 70% no aumento de informações de casos de violência doméstica. No estudo sobre a experiência de Santa Catarina, o efeito estimado de aumento de ocorrências de violência doméstica foi de 69,2% e em SP, o efeito foi de 102%. Aumentou a violência doméstica? Claro que não. O que aumentou foi o número de registro das ocorrências, porque os policiais passaram a usar os protocolos e passaram a registrar os casos que ocorriam e que muitas vezes eram empurrados para debaixo do tapete.

Os estudos mostram, ainda, o que não ocorre: os policiais não mudam de lugar, não passam a patrulhar lugares menos violentos, não há diferença na mancha de policiamento, não há menor número de flagrantes, não há diferença no tempo de atendimento.

É muito confortável para o gestor público implementar uma política pública com esse nível de evidência. É difícil pensar em uma outra política que tenha apresentado um impacto tão forte para a cidadania e para os agentes de segurança como o programa das câmeras corporais, nos locais em que foram implementadas com cuidado e a partir de um processo de gestão da mudança.

Mas as câmeras são uma tecnologia. Se bem usada, ela vai estar a serviço da cidadania. Se mal usada, ela vai ser um imenso desperdício de recurso público.

05.



O MERCADO DA "VIGILÂNCIA COLABORATIVA": REFLEXÕES SOBRE O USO DE TOTENS E CÂMERAS DE VIGILÂNCIA PRIVADA EM ESPAÇOS PÚBLICOS

Bárbara Simão
e Vitor Vilanova

INTRODUÇÃO

Num dia, foi um totem azul. No outro, foi um totem amarelo. Em algumas regiões da cidade de São Paulo, tem sido possível perceber a gradual expansão de câmeras instaladas em totens pelas ruas, pertencentes a empresas distintas que oferecem um mesmo tipo de proposta: monitoramento constante dos arredores de uma vizinhança. Embora a vigilância privada em áreas residenciais não seja um fenômeno novo, a proposta dessas empresas vai além do trivial. Por meio de câmeras conectadas a aplicativos, os usuários podem acessar imagens em tempo real, 24 horas por dia, com a possibilidade de compartilhar alertas e dados com órgãos públicos.

Esse modelo é frequentemente promovido pelas empresas em seus sites como uma "rede colaborativa de inteligência" ou uma "solução de segurança e zeladoria urbana", utilizando termos como "colaboração", "transparência" e "solidariedade" que sugerem uma lógica de comunidade e vizinhança. No entanto, o fácil acesso às imagens captadas e a concepção de vigilância compartilhada em rede suscita preocupações não apenas relacionadas à privacidade, mas também ao impacto sobre o uso e a apropriação do espaço público. A possibilidade de monitoramento contínuo abre margem para discussões sobre o direito à privacidade de indivíduos que podem ser monitorados, além de implicações legais relacionadas ao uso dessas imagens por terceiros, incluindo entidades públicas.

Essas questões levantam reflexões sobre os limites éticos e jurídicos da atuação dessas empresas no Brasil, em especial sobre os efeitos dessas tecnologias na organização do espaço público e no aumento das disparidades sociais em termos de segurança e controle. Diante desse cenário, o presente artigo tem como objetivo examinar o enquadramento jurídico dessas empresas de monitoramento, investigando suas consequências sobre a privacidade e o uso do espaço público.

A ATIVIDADE DE EMPRESAS DE TOTENS DE VIGILÂNCIA: O QUE FAZEM E DIZEM FAZER

A operação dessas empresas ocorre com algumas nuances em relação aos serviços oferecidos e suas capacidades.[1] Algumas das empresas desse mercado são mais recentes e surgiram neste nicho, outras já operavam anteriormente como empresas fornecedoras de serviços de segurança privada.[2] Como característica em comum, pode-se dizer que todas oferecem um serviço de assinatura, contratável por qualquer pessoa física ou jurídica, a partir do qual torres com câmeras são instaladas em um determinado local de interesse - normalmente à frente de um condomínio. A expressão "segurança colaborativa"[3] é por vezes utilizada para descrever a natureza de suas atividades, já que se amparam em um efeito de rede[4] - quanto mais pessoas ou empresas aderirem ao serviço, maior será a rede de vigilância consolidada. A CoSecurity, uma das empresas identificadas, afirma que suas "redes colaborativas permitem conectar equipamentos novos ou pré-existentes criando grupos de câmeras e usuários ilimitados".[5]

1. Consideramos, neste artigo, as seguintes empresas: Gabriel, YellowCam, CoSecurity, DeltaCity, Mantra, White e RS Serviços.

2. Este é o caso, por exemplo, das empresas RS Serviços (2006) e DeltaOmega (2007).

3. Expressão utilizada pelas empresas YellowCam, Gabriel, CoSecurity e DeltaCity.

4. O termo "efeitos de rede" se refere ao impacto que o número de usuários de uma plataforma tem sobre o valor gerado para cada usuário. Cf. PARKER, Geoffrey G.; VAN ALSTYNE, Marshall W.; CHOUDARY, Sangeet Paul. Platform revolution: How networked markets are transforming the economy--and how to make them work for you. WW Norton & Company, 2016.

5. COSECURITY. Portal do cliente. Disponível em: https://portaldocliente.cosecurity.com.br/login.

As câmeras são normalmente acessíveis em tempo real por meio de um aplicativo, além de existir a possibilidade de acesso ao histórico de gravações e de geração de alertas de ocorrências. Este é o caso das empresas YellowCam, CoSecurity, DeltaCity, White, Mantra e Gabriel. O tempo de disponibilização das imagens, por sua vez, varia. No caso da empresa Gabriel, esse histórico fica disponível por até 14 dias. A empresa também oferece acesso a um mapa de alertas, que destaca incidentes de segurança ocorridos, além de um mapa da "área de proteção",[6] que mostra as regiões monitoradas pelo sistema. Outras empresas não divulgam abertamente o tempo pelo qual é disponibilizado o acesso às gravações.

Outro ponto de variação é a existência de centrais de monitoramento em tempo real - e quem fica responsável por essa cobertura. A YellowCam chama sua central de monitoramento de "Pelotão More",[7] e afirma que o grupo é responsável pelo "apoio e acompanhamento dos alertas e ocorrências gerados no aplicativo, fazendo a interface com os órgãos públicos". A White oferece duas linhas de serviços distintas: a "linha colaborativa", em que o monitoramento é feito pelos próprios clientes, e a "linha smart", que inclui a supervisão por vigilantes virtuais profissionalmente treinados.[8] Já a Gabriel possui uma central de monitoramento própria, que opera 24 horas por dia, "analisando ocorrências e ajudando a polícia com dados e imagens".[9]

6. GABRIEL. Site da empresa. Disponível em: https://gabriel.com.br/.

7. YELLOWCAM. Site da empresa. Disponível em: https://www.yellowcam.net.br/.

8. WHITEBR. Site da empresa. Disponível em: https://whitebr.com/vigilancia-virtual-2024/

9. GABRIEL. Central 24h. Disponível em: https://gabriel.com.br/central-24h/.

Como se nota, a existência de um canal de comunicação direto ou simplificado com forças policiais e órgãos públicos é um dos chamarizes na atividade dessas empresas. A maneira como essa comunicação ocorre é, no entanto, um questionamento importante, e que chega a respostas no mínimo controversas.

Algumas matérias na imprensa já destacaram a existência de comunicação direta entre membros de empresas e forças policiais, como grupos de WhatsApp.[10] Em busca pelos sites, não há grandes informações a respeito de como os dados são compartilhados. Gabriel e Cosecurity apresentam formulários online de requisição de dados, nos quais solicitam informações básicas de quem é o responsável pela solicitação e o anexo de um ofício ou pedido formal. Não são apresentadas informações completas, porém, sobre quais são os requisitos para que esses pedidos sejam atendidos, ou mesmo critérios de controle e comprovação de veracidade. Abaixo, apresentamos uma tabela em que elencamos como as empresas abordam o assunto em seus sites, políticas de privacidade ou termos de uso.

Veja como as empresas mencionam em seus sites o compartilhamento de dados com autoridades de investigação.

10. RIBEIRO. Paulo Victor. Startup de segurança gabriel cria rede de informações clandestinas pelo whatsapp com a polícia do rio. The Intercept Brasil, 24 de abr. 2023. Disponível em: https://www.intercept.com.br/2023/04/24/startup-de-seguranca-gabriel-cria-rede-de-informacoes-clandestinas-pelo-whatsapp-com-a-policia-do-rio/.

CoSecurity

"Tratamento de Dados e Responsabilidade: Os agentes públicos concordam com o tratamento de dados fornecidos para atender às determinações das autoridades competentes e são responsáveis pela veracidade das informações fornecidas.

Procedimentos para Solicitação de Acesso: As solicitações devem ser acompanhadas por um ofício completo da autoridade competente, justificando a necessidade de acesso, com informações detalhadas sobre os eventos em questão.

Limitações de Acesso e Prazos de Atendimento: A Cosecurity pode limitar o acesso às câmeras e o tempo de visualização, conforme necessário, e os prazos de atendimento podem variar de acordo com a complexidade do caso.

Situações Emergenciais: Em casos de emergência envolvendo crimes graves, a Cosecurity pode fornecer acesso sem ordem judicial prévia, desde que haja evidências claras da necessidade e risco iminente."

COSECURITY. Autoridades. Disponível em: https://www.cosecurity.com.br/autoridades/.

DeltaCity

"Além disso, também existem outras hipóteses em que seus dados poderão ser compartilhados, que são:
A – Determinação legal, requerimento, requisição ou ordem judicial, com autoridades judiciais, administrativas ou governamentais competentes."

DELTAOMEGA. Política de privacidade. Disponível em: https://antigo.projetodeltaomega.net/portaria-virtual/politicas-de-privacidade/.

Gabriel

"ÓRGÃOS OU AUTORIDADES COMPETENTES: para cumprimento de obrigações legais ou regulatórias, para atendimento de determinações judiciais, administrativas ou arbitrais, e para colaboração com investigações conduzidas por autoridades competentes."

GABRIEL. Política de privacidade. Disponível em: https://gabriel.com.br/legal/politica-de-privacidade-da-gabriel/.

"A solicitação de fornecimento do conteúdo das câmeras da Gabriel deverá ser acompanhada de ofício expedido pela autoridade competente, a ser disponibilizado na íntegra, de forma legível e devidamente assinado, contendo, no mínimo, as seguintes informações:

- Descrição dos fatos sob apuração e da finalidade do pedido, de maneira a justificar o compartilhamento, nos termos da lei;
- Data e horário, ainda que aproximados, em que teriam ocorrido os fatos sob apuração;
- Localidade das câmeras que se necessita acesso.

A Gabriel pode se opor ao atendimento de solicitações excessivamente abrangentes ou de caráter exploratório (fishing expedition) e limitar o acesso ao conteúdo das câmeras ao período estritamente necessário para apuração do fato em questão, o que será efetuado conforme as instruções contidas na solicitação."

[. . .]

"Em situações emergenciais, envolvendo crimes graves, a Gabriel pode fornecer conteúdo das câmeras sem ordem judicial ou ofício prévio da autoridade competente, desde que a so-

licitação demonstre, de forma inequívoca, (i) a necessidade de divulgação imediata das informações; e (ii) o risco concreto e iminente de prejuízo caso a divulgação fosse condicionada a uma ordem judicial ou ofício prévio. Nessas hipóteses, a Gabriel pode demandar mais informações ou documentos para agilizar a avaliação de uma solicitação de emergência."

GABRIEL. Gabriel Autoridades. Disponível em: https://gabriel.com.br/gabriel-autoridades/.

Mantra

"Com o intuito de dar transparência ao tratamento de dados que realiza, a Mantra Monitoramento informa que alguns Dados Pessoais, limitado ao mínimo necessário à operação, podem ser compartilhados com:

Entes públicos, por motivos legais para cumprir uma ordem ou procedimento legal e/ou responder a solicitações de autoridades públicas e governamentais;"

MANTRA MONITORAMENTO. Política de privacidade. Disponível em: https://mantramonitoramento.com.br/politica-de-privacidade/.

RS Serviços

Não há menção ao compartilhamento de dados com autoridades de investigação.

White

"Não compartilhamos informações de identificação pessoal publicamente ou com terceiros, exceto quando exigido por lei."

WHITEBR. Política de privacidade. Disponível em: https://whiteseguranca.com/politica-de-privacidade/.

YellowCam

"4.2. Havendo solicitação administrativa ou decisão judicial para compartilhamento dos dados e informações, fica a Yellowcam autorizada a fornecer os dados pessoais dos usuários e terceiros que são manuseados e coletados para a execução das atividades, em consonância com o artigo 48 da Lei 13.709/2018, no qual se limitará a fornecer tão somente o que lhe for solicitado e comprometendo-se a comunicar antecipadamente, sempre que possível, o titular dos dados."

YELLOWCAM. Política de privacidade. Disponível em: https://www.yellowcam.net.br/wp-content/uploads/2021/07/Politica_de_Privacidade_V1-07-2021.pdf.

***

O uso de inteligência artificial é outro ponto relevante na operação dessas empresas e que possui variações. A CoSecurity afirma trabalhar com inteligência artificial e segurança preventiva para detectar pessoas com comportamento suspeito, gerar alertas de risco de intrusão, detectar aglomerações e identificar veículos e motos suspeitos. A DeltaCity afirma possuir módulos de inteligência artificial para reconhecimento facial, identificação de placas de veículos, registros de acidentes e identificação de aglomerações, sem detalhes a respeito de cada funcionalidade. A White Segurança afirma possuir módulo de segurança preditiva, com uso de inteligência artificial e aviso à polícia "em até 30 segundos antes do crime".[11] Outras empresas afirmam utilizar inteligência artificial, mas não mencionam o uso de ferramentas ou capacidades específicas, como Gabriel

11. WHITEBR. Site da empresa. Disponível em: https://whitebr.com/vigilancia-virtual-2024/.

- que afirma expressamente não utilizar reconhecimento facial em suas atividades - e Mantra.

Quanto ao tratamento de dados dos transeuntes que passem por ruas monitoradas, há menções vagas à possibilidade pela YellowCam e Gabriel. A primeira afirma que dados pessoais "dos usuários e de terceiros" podem ser fornecidos quando houver solicitação administrativa ou decisão judicial requisitando o compartilhamento, comprometendo-se a empresa a comunicar antecipadamente, quando possível, o titular dos dados.[12] Já a segunda reconhece a possibilidade de que titulares de dados presentes na localidade do Assinante tenham as suas imagens captadas pelo Camaleão e/ou pelas Câmeras de Proteção Exclusiva, e afirma que "processa essas informações quando necessário para o cumprimento de obrigação legal ou regulatória e fornecimento dessas imagens aos titulares ou autoridades competentes, quando cabível, bem como para o cumprimento de suas obrigações contratuais e a possibilidade de desenvolvimento de seus Serviços".[13] Não foram encontradas informações a respeito nas demais empresas.

12. YELLOWCAM. Política de privacidade. Disponível em: https://www.yellowcam.net.br/wp-content/uploads/2021/07/Politica_de_Privacidade_V1-07-2021.pdf.

13. GABRIEL. Política de privacidade. Disponível em: https://gabriel.com.br/legal/politica-de-privacidade-da-gabriel/.

O ENQUADRAMENTO JURÍDICO DA VIGILÂNCIA PRIVADA NO BRASIL

No Brasil, a regulamentação da vigilância e segurança privada é parcialmente abordada pela Lei de Segurança Bancária (Lei nº 8.863, de 1994), que define em seu artigo 10 as atividades de segurança privada:

> Art. 10. São considerados como segurança privada as atividades desenvolvidas em prestação de serviços com a finalidade de:
>
> I - proceder à vigilância patrimonial das instituições financeiras e de outros estabelecimentos, **públicos** ou privados, bem como a **segurança de pessoas físicas**.
>
> § 2º As empresas especializadas em prestação de serviços de segurança, vigilância e transporte de valores, constituídas sob a forma de empresas privadas, além das hipóteses previstas nos incisos do caput deste artigo, **poderão se prestar ao exercício das atividades de segurança privada a pessoas; a estabelecimentos comerciais, industriais, de prestação de serviços e residências; a entidades sem fins lucrativos; e órgãos e empresas públicas**. (grifamos).

A Lei, aplicável à segurança de instituições financeiras, indica uma série de regras que essas empresas devem seguir, como a vedação da propriedade e administração por estrangeiros (art. 11), vedação da contratação de empregados com antecedentes criminais (art. 12), e necessidade de autorização de funcionamento pelo Ministério da Justiça (art. 20).

Recentemente, a Portaria DG/PF nº 18.045/2023, atualizada pela Portaria nº 18.974/2024, introduziu novas regras que ampliam o escopo da regulamentação.[14] A Portaria estabelece que as atividades

14. Há outras portarias no tema da segurança privada: Portaria nº 3.233/2012 - DG/DPF; Portaria nº 34.383/2019 - CGCSP/DIREX/PF; Portaria nº 6/2021 - CGCSP/DIREX/PF; Portaria nº 11/2022 - CGCSP/DIREX/PF; Portaria nº 14/2023 - CGCSP/DPA/PF; Portaria DG/PF nº 18.504/2023; Portaria nº 18.974/2024. Todas disponíveis no site: https://www.gov.br/pf/pt-br/assuntos/seguranca-privada/legislacao-normas-e-orientacoes/portarias.

de segurança privada, exercidas tanto por empresas especializadas quanto por aquelas que possuem serviço orgânico de segurança, devem ser controladas e fiscalizadas pela Polícia Federal, funcionando como complemento às ações de segurança pública. A normativa também estabelece que a política de segurança privada deve ser orientada por princípios fundamentais, como a dignidade da pessoa humana e a proteção dos cidadãos.

No que diz respeito à vigilância patrimonial, a Portaria afirma que se trata de "atividade exercida em eventos sociais ou em estabelecimentos urbanos e rurais, públicos ou privados, com o objetivo de garantir a incolumidade física das pessoas e a integridade do patrimônio" (Art. 1º, §3º, I). Por sua vez, essa atividade deve ser exercida mediante autorização prévia da Polícia Federal, observados requisitos como capital social mínimo e instalações físicas adequadas, e deve ocorrer estritamente dentro dos limites dos imóveis vigiados (Art. 18). Em eventos sociais, como shows, eventos esportivos ou outros encontros públicos e privados, a vigilância deve se restringir ao espaço privado objeto do contrato de prestação de serviços.

A natureza de empresas de *totens* de vigilância, no entanto, é ambígua e desafia os conceitos previamente estabelecidos. São empresas que se dizem atuar como intermediárias da segurança - que é feita de forma "colaborativa" pela vizinhança. Além disso, embora se destinem à segurança privada e instalem suas câmeras em lugares, a princípio, privados e limitados a espaços condominiais ou comerciais, se direcionam ao espaço público. O monitoramento frequentemente ultrapassa os limites privados, estendendo-se a áreas públicas. A captura de imagens e sons não se limita a um espaço fechado e determinado, mas abrange ruas, calçadas e outros espaços públicos, criando uma extensa rede de monitoramento. Quanto mais moradores e associações contratam esses serviços, maior se torna essa rede.

/ A EXISTÊNCIA DE UM CANAL DE COMUNICAÇÃO DIRETO OU SIMPLIFICADO COM FORÇAS POLICIAIS E ÓRGÃOS PÚBLICOS É UM DOS CHAMARIZES NA ATIVIDADE DESSAS EMPRESAS /

A captação ambiental para investigações criminais, por sua vez, é regulamentada pelo artigo 8º-A e seguintes da Lei de Interceptações (Lei nº 9.296, de 1996), conforme atualizações introduzidas pela Lei nº 13.964, de 2019. De acordo com o artigo 8º-A, a captação ambiental pode ser autorizada pelo juiz a pedido da autoridade policial ou do Ministério Público, desde que se prove que outros meios igualmente eficazes não estão disponíveis e que existam evidências razoáveis de autoria e participação em crimes com penas superiores a quatro anos. Além disso, as regras para captação ambiental seguem, subsidiariamente, a legislação específica para interceptações telefônicas e telemáticas. Não há dúvidas, portanto, da necessidade de autorização judicial para a captação ambiental.

No que se refere à atividade das empresas com relação ao tratamento e armazenamento de dados, deve-se evidenciar a abrangência da Lei Geral de Proteção de Dados (LGPD). Essas empresas não estão abrangidas pelas exceções previstas no Art. 4º da LGPD, que se aplicam a atividades de segurança pública e investigação criminal, uma vez que não possuem autoridade ou competência para conduzir essas atividades.

Portanto, as empresas devem cumprir as exigências da LGPD, garantindo uma base legal adequada para suas atividades, além de observância aos princípios de necessidade, proporcionalidade, finalidade e adequação. No artigo 26 da LGPD, estão previstas as limitações e permissões relacionadas ao uso compartilhado de dados pessoais com o Poder Público. Este artigo estabelece que o uso compartilhado de dados pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e às atribuições legais dos órgãos e entidades públicas. Além disso, o artigo impõe restrições rigorosas ao compartilhamento com entidades privadas, permitindo-o apenas em situações específicas: (i) quando necessário para a execução descentralizada de atividades públicas; (ii) quando os dados são acessíveis publicamente; (iii) quando há previsão legal ou respaldo em contratos e convênios; e (iv) para prevenir fraudes e proteger a segurança do titular dos dados.

Como se percebe, o artigo 26 não deve ser aplicado para justificar o acesso do Poder Público a dados pessoais mantidos por empresas privadas em qualquer caso. O artigo trata especificamente do contexto de políticas públicas e atividades descentralizadas, e não do acesso a dados geridos por empresas privadas fora desse âmbito. Ou seja: ordens gerais de acesso a dados, quando não houver instrumentos normativos que deem respaldo a isso, não devem ocorrer sem observância estrita dos demais critérios elencados pela legislação, cuja regra geral é a necessidade de ordem judicial. Assim também segue o Marco Civil da Internet (MCI), ao dispor que qualquer pedido de fornecimento de registros de conexão ou de acesso a aplicações de internet deve ser feito por meio de ordem judicial, acompanhada de justificativa fundamentada quanto à utilidade dos registros para a investigação ou instrução probatória, e especificação do período dos registros solicitados.[15]

15. Artigo 22 da Lei nº 12.965/2014 (Marco Civil da Internet).

Portanto, embora existam lacunas em relação à atividade dessas empresas e sua relação com o âmbito penal, o contexto jurídico brasileiro já impõe várias camadas de proteção e requisitos para o acesso e compartilhamento de dados pessoais entre entes privados e públicos, gerando dúvidas sobre a conformidade das atividades dessas empresas com a legislação vigente.

A aprovação de uma lei aplicável à proteção de dados na esfera penal poderia ser um caminho de resolução para essas questões. Tal legislação não só proporcionaria um quadro normativo mais específico para o tratamento e compartilhamento

de dados no contexto penal, como também poderia estabelecer diretrizes rigorosas sobre as condições e limites para o acesso de autoridades a dados geridos por entidades privadas. Nesse sentido, o anteprojeto de LGPD Penal, elaborado por comissão de juristas e apresentado em 2020, inclui importantes diretrizes. Dentre elas, a proibição de tratamento de dados pessoais para atividades de segurança pública voltadas à persecução penal por entidades privadas, salvo se realizado sob a supervisão de uma pessoa jurídica de direito público, com devida comunicação ao Conselho Nacional de Justiça (CNJ).[16] Além disso, qualquer acesso de autoridades competentes a dados pessoais controlados por entidades privadas deveria ocorrer conforme previsão legal, obedecendo aos princípios de motivação concreta, adequação, necessidade e proporcionalidade. Assim, empresas privadas não poderiam conduzir atividades de segurança pública a menos que estas estivessem sob a tutela de um ente público e que fossem observadas previsões legais específicas para tanto.

16. Artigo 10 da Lei nº 12.965/2014 (Marco Civil da Internet).

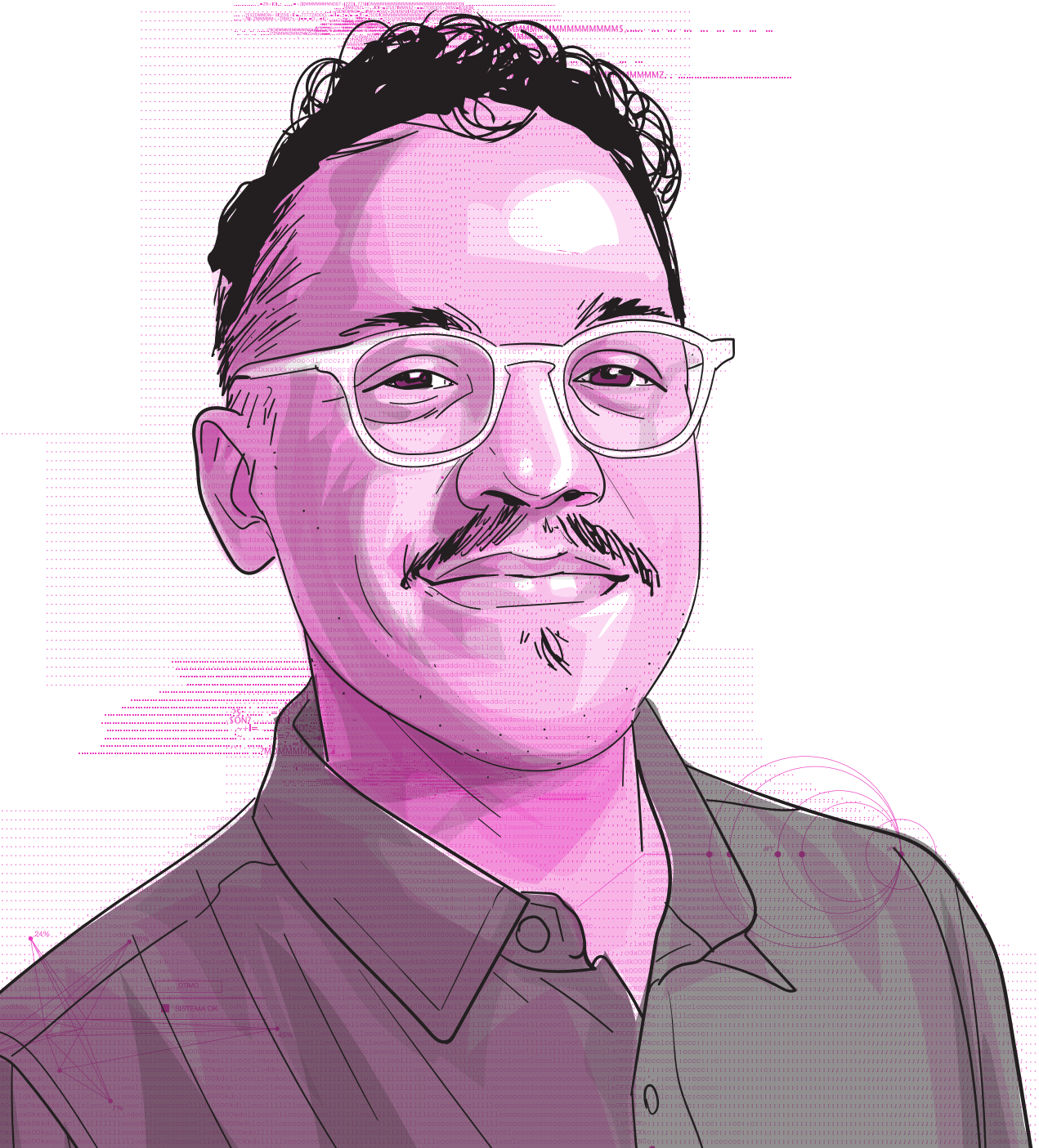
Enquanto o anteprojeto de LGPD Penal levanta potenciais limitações, ainda persistem dúvidas quanto à possibilidade e legalidade da vigilância privada que se volta aos espaços públicos. Isto é: quais seriam os limites da atuação de empresas nesse contexto e quais seriam critérios adequados de transparência, responsabilidade e exercício de direitos que deveriam ser observados. A integração entre sistemas públicos e privados, por sua vez, tem sido tema crescente de iniciativas de governos para segurança pública, como no caso do Programa Muralha Paulista em São Paulo.[17]

17. G1. Governos [sic] de SP deverá lançar programa Muralha Paulista em junho. Jun. 2024. Disponível em: https://g1.globo.com/sp/sao-paulo/sp2/video/governos-de-sp-devera-lancar-programa-muralha-paulista-em-junho-12632608.ghtml.

CONSIDERAÇÕES FINAIS

Neste artigo, abordamos o mercado da "vigilância colaborativa" no Brasil, buscando evidenciar como empresas que comercializam totens de vigilância têm se apresentado em relação ao seu público-alvo e autoridades de investigação. Diante da análise de algumas empresas em operação no Brasil e em especial na cidade de São Paulo, buscamos entender o discurso dessas empresas e, ao menos em parte, as suas práticas comuns. O que as une, além da instalação das câmeras e de um aplicativo para monitoramento pelos usuários, é de maneira geral a descrição de suas atividades a partir de uma lógica de intermediação da atividade de segurança, colaboração e solidariedade entre membros de uma mesma comunidade. O discurso lembra o da "economia de compartilhamento" - embora o compartilhado nesse caso não sejam bens ou serviços de consumo, mas a própria infraestrutura de vigilância daquele local. Sustentam-se, assim, em um efeito de rede, já que a capacidade de monitoramento consolidada aumenta conforme o crescimento de adesões ao serviço.

Contrastamos a atividade dessas empresas também em relação ao que existe de moldura jurídica sobre segurança e vigilância privada no Brasil. Conquanto já existam regras consolidadas em relação à vigilância patrimonial e ao monitoramento de ambientes privados, empresas de totens de vigilância possuem nuances que testam a aplicabilidade dessas categorias. De toda forma, mesmo que existam lacunas em relação à atividade dessas empresas e suas implicações, o cenário jurídico brasileiro já impõe camadas de proteção e requisitos para o acesso e compartilhamento de dados pessoais entre entes privados e públicos, gerando dúvidas sobre a conformidade das atividades dessas empresas com a legislação vigente.



06.

VIGILÂNCIA E SEGURANÇA PÚBLICA: RECONHECENDO A FACE DA SEGURANÇA FEITA POR TOTENS[1]

Pablo Nunes

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Vitor Vilanova.

Queria, antes de mais nada, agradecer ao Internetlab por mais uma vez me convidar para participar do Congresso Internacional. E realmente tem sido uma oportunidade fundamental para gente que discute esses temas refletir através de outras experiências e compartilhar o que temos estudado.

Eu trabalho num centro de estudos no Rio de Janeiro, o Centro de Estudos de Segurança e Cidadania (CESeC). Boa parte do que eu vou falar hoje, de experiências que eu tive em relação a esse tema, tem a ver com o cenário do Rio de Janeiro, mas acho que tem questões que a gente pode trabalhar e pensar, principalmente, como pontos de atenção que podem ser generalizados para outros cenários no Brasil como um todo.

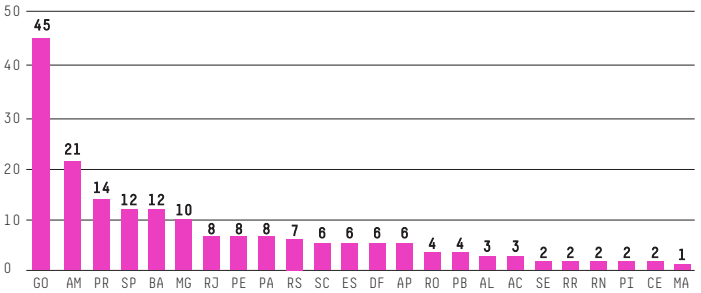
1. O PANÓPTICO

E tudo isso parte de um projeto que começamos em 2019, que é o projeto "O Panóptico",[2] que busca, de maneira muito geral, acompanhar a adoção de projetos de reconhecimento facial pelas forças de segurança do Brasil. Nós temos um foco na segurança pública, principalmente na adoção de reconhecimento facial pelas polícias militar e civil, e também por algumas guardas municipais, movimento que a gente tem acompanhado nos últimos anos. Mas o que a gente também descobriu é que existe uma participação muito profícua do setor privado, seja na cessão de tecnologias para essas forças de segurança ou também mesmo na operação desses sistemas.

2. O PANÓPTICO. Disponível em: https://www.opanoptico.com.br/. Acesso em: 20 set. 2024.

Desde 2019 até junho de 2024, nós já conseguimos monitorar 251 projetos com uso de reconhecimento facial no Brasil, focados na segurança pública. Esse monitoramento é baseado no que sai na imprensa, algumas solicitações de informação via Lei de Acesso à Informação, e também por meio dos canais oficiais da Secretaria de Segurança Pública e das Polícias Militares e Civis do Brasil. Há uma distribuição quase que uniforme nas regiões, tirando algumas concentrações que a gente consegue ver, principalmente na região Centro-Oeste, em Goiás - e depois eu falo um pouco sobre isso.

NÚMERO DE PROJETOS DE RECONHECIMENTO FACIL POR UF
MONITORAMENTO FEITO PELO PANÓPTICO (2023)



A concentração está mais evidente nesse gráfico de barra, com dados até 2023, em que Goiás segue com o maior número de projetos, 45, seguido de Amazonas, Paraná e outros estados. A gente tem, a partir disso, feito estudos de caso, entendendo que essas tecnologias, por mais que se vendam como objetivas, como isentas de subjetividades, e que também não são reativas ao contexto em que são colocadas, o que vemos na realidade é o oposto. Vemos que, a depender dos contextos, as mesmas tecnologias produzem efeitos muito distintos. Então, decidimos fazer uma parceria com o The Intercept Brasil

para aprofundar nosso entendimento sobre alguns casos de aplicação de reconhecimento facial que se destacaram no nosso monitoramento.

2. QUEM PAGA A CONTA?

A gente lançou essa série de reportagens, que até o momento são quatro, que se destinam a investigar a adoção de reconhecimento facial, mas focando basicamente em "Quem paga a conta?". [3] Ou seja, nessas relações financeiras da adoção dessa tecnologia aqui no Brasil, como que isso tem se dado em diferentes contextos. Duas dessas matérias foram baseadas em estudos de caso, produzidos por nós e a primeira delas foi em Goiás.

O que a gente encontra em Goiás[4], nessa concentração de projetos de reconhecimento facial, foi exatamente a atuação muito forte de um deputado federal - agora ex-deputado federal - Delegado Waldir, que conseguiu milhões de reais, vindos do Fundo Nacional de Segurança Pública, através de uma portaria expedida pelo ex-ministro Sérgio Moro, para municípios de Goiás adquirirem câmeras de reconhecimento facial. E o que a gente notou é que 30 milhões de reais que foram destinados, pelo Delegado Waldir, foram parar em cidades de Goiás muito rurais e muito pequenas, uma delas tinha população muito diminuta, cerca de 5.000 habitantes. Algumas das cidades tinham problemas sérios de saneamento e infraestrutura urbana básicos e que também - algo relevante - tinham pouquíssimos registros de crimes violentos e de crimes patrimoniais. Algumas das cidades que receberam as câmeras não registraram homicídios durante o período de cinco anos. Registraram um roubo a domicílio durante o período de cinco anos e outros registros semelhantes.

A partir da instalação de alguns desses projetos, a gente também conseguiu monitorar os indicadores de segurança, tentando verificar se havia algum impacto relativo à diminuição da criminalidade após a instalação dessas câmeras, e o que a gente encontrou é que não houve impacto significativo. Em algumas cidades, inclusive, os registros aumentaram depois da instalação das câmeras.

3. INTERCEPT BRASIL. Quem paga a conta? Disponível em: https://www.intercept.com.br/especiais/quem-paga-a-conta/. Acesso em: 20 set. 2024.

4. REBELLO, Aiuri. Quem paga a conta? Parte 1: delegado Waldir torrou r$ 30 milhões em reconhecimento facial para cidades que sequer têm saneamento em goiás. Intercept Brasil, abr. 2023. Disponível em: https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/. Acesso em: 20 set. 2024.

3. BANCO DE DADOS DA CLEARVIEW AI E O RECONHECIMENTO FACIAL NA BAHIA

A segunda matéria que a gente publicou foi sobre essa tentativa de entrada da Clearview AI[5] no mercado brasileiro. A empresa é muito conhecida por esse processo de captura de fotos públicas das redes sociais, e que a possibilitou reunir mais de 3 bilhões de fotografias em seus bancos de dados para cessão a forças de segurança para realização de reconhecimento facial. Então, eu, você, provavelmente todos nós aqui estamos e fazemos parte desse banco de dados que a Clearview armazenou durante esses anos. E a gente conseguiu monitorar alguns encontros da Clearview oferecendo serviços para o Ministério Público de São Paulo, para algumas polícias, também, no Brasil, mas a gente ainda não conseguiu registrar nenhum contrato assinado.

5. MARTINS, Laís. Quem paga a conta? Parte 2: exclusivo: em reuniões secretas, clearview ofereceu 3 bilhões de imagens de brasileiros para polícias e ministério da justiça. Intercept Brasil, 16 maio 2023. Disponível em: https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/. Acesso em: 20 set. 2024.

O último estudo de caso que a gente publicou foi sobre o caso da Bahia.[6] A Bahia é o estado brasileiro que tem projetos de reconhecimento facial por mais tempo no Brasil. Em 2019, foi o ano em que houve o primeiro registro de prisões com uso de reconhecimento facial, principalmente nesse segundo período da utilização dessas tecnologias. A gente sabe que as tecnologias de reconhecimento facial foram utilizadas primeiramente durante os grandes eventos, mas agora, principalmente a partir de 2019, houve investimentos sucessivos de estados, e também de municípios, na expansão desse processo como uma ferramenta das políticas públicas de segurança. E a Bahia foi pioneira nesse processo. A partir daí, o que a gente tem visto é o fortalecimento da vigilância na Região Metropolitana de Salvador, que foi a primeira região monitorada na Bahia. Mas também um processo muito acelerado de interiorização dessas câmeras de reconhecimento facial, por mais de 70 cidades do interior baiano.

Olhando os contratos, a gente conseguiu somar mais de 600 milhões de reais que já foram gastos com as câmeras de reconhecimento facial. Esses valores poderiam custear hospitais por anos a fio, além de ambulâncias e outros serviços de saúde. E a gente colocou nessa conta os hospitais, porque saúde é a principal reclamação da população baiana quando questionada sobre o que falta e quais são os principais problemas que eles enfrentam. E quando a gente olha o quanto o projeto de reconhecimento facial teve de efeito positivo, não temos nenhum dado da realidade que mostre sua eficiência, seja em termos do próprio uso da tecnologia em si, seja em

6. NASCIMENTO, Paulo. Quem paga a conta? Parte 3: dinheiro gasto por ano com reconhecimento facial na bahia custearia um hospital por 32 anos e 1,5 mil ambulâncias. Intercept Brasil, 31 jul. 2023. Disponível em: https://www.intercept.com.br/2023/07/31/reconhecimento-facial-na-bahia-custearia-um-hospital-e-mil-ambulancias-com-uti/. Acesso em: 20 set. 2024.

/ DESDE 2019 ATÉ JUNHO DE 2024, NÓS JÁ CONSEGUIMOS MONITORAR 251 PROJETOS COM USO DE RECONHECIMENTO FACIAL NO BRASIL, FOCADOS NA SEGURANÇA PÚBLICA /

/ QUEM ESTÁ GERINDO ESSAS EMPRESAS QUE GANHAM COM ESSE AUMENTO DA SENSAÇÃO DE INSEGURANÇA [É QUEM DEVERIA] GARANTIR A SEGURANÇA /

redução da sensação de insegurança da população. Além disso, a falta de transparência é uma das marcas desse projeto baiano e a Secretaria de Segurança Pública pouco tem feito na direção de divulgar dados e relatórios de impacto sobre o uso das tecnologias de reconhecimento facial no estado.

4. SMART SAMPA E OS TOTENS

E, por fim, a última matéria que a gente publicou foi exatamente sobre o Smart Sampa.[7] O que os repórteres do Intercept encontraram, analisando as tecnologias nesse projeto aqui na cidade de São Paulo, é que o consórcio que levou o edital tinha, dentro dele, uma empresa que já foi acusada por diversos casos de corrupção, mesmo assim conseguiu ganhar esse edital de mais de 580 milhões de reais.

Ou seja, ainda há uma dimensão do mercado privado que se imbrica nesse processo de expansão das tecnologias de vigilância no Brasil. Uma face de expansão da participação de empresas no setor de segurança privada é o uso de totens e outras câmeras de monitoramento urbano por meio de totens. Esse tipo de dispositivo se difere um pouco das câmeras de monitoramento urbano habituais e algumas cidades têm incluído esse tipo de dispositivo em sua infraestrutura de monitoramento. Para dar uma contribuição ao debate, filtramos o banco de dados de projetos monitorados pelo Panóptico para entender quais deles têm participação de empresas privadas nessa modalidade de emprego de totens. Foram 25 cidades encontradas utilizando

7. REBELLO, Aiuri. Quem paga a conta? Parte 4: smart sampa: denunciada por corrupção foi quem abocanhou r$ 588 mi para capturar seu rosto em sp. Intercept Brasil, 14 ago. 2023. Disponível em: https://www.intercept.com.br/2023/08/14/smart-sampa-denunciada-por-corrupcao-capturar-seu-rosto-em-sp/. Acesso em: 20 set. 2024.

Belo Horizonte

Recife

esses totens e, basicamente, cidades em que a Guarda Municipal tem operado esses dispositivos de segurança.

Ao lado vê-se um totem instalado na Savassi, em Belo Horizonte, bairro abastado da capital mineira.

No Recife, foi instalado um totem dentro do campus da Universidade Federal de Pernambuco, como se pode ver na imagem ao lado. Adicionalmente, há a questão do financiamento desses dispositivos, já que esse totem foi instalado sem custos para o poder público. Ou seja, foi cedido por uma empresa privada. Neste sentido, levantam-se muitas perguntas sobre essa relação entre público e privado, que se coloca numa zona cinzenta. E o setor privado tem crescido sua presença seja na relação com o setor público, seja no avanço de soluções de monitoramento e segurança privada.

5. AS GRANDES EMPRESAS PRIVADAS DE VIGILÂNCIA

Pesquisando sobre essas empresas que oferecem serviços de monitoramento por câmeras, encontramos, principalmente, três empresas grandes e com uma forte presença em São Paulo.

A primeira é a Yellowcam, que já tem câmeras instaladas nos locais marcados no mapa, que vocês podem ver abaixo.

A segunda empresa, com bastante entrada no mercado paulista, é a Cosecurity que já tem mais de 1.400 câmeras instaladas na cidade de São Paulo. Como se pode ver no mapa abaixo, há uma densidade grande de câmeras da Cosecurity instaladas na cidade.

E, por fim, a Bulke, que alegadamente traz a "solução definitiva para inibir crimes e tornar a sua cidade mais segura". Todas essas empresas, em maior ou menor grau, vendem essas promessas nessa linha, de garantir, novamente, o direito de ir e vir aos clientes e tornar as cidades mais seguras. Tudo isso sendo prometido pelo setor privado, transformando "cidadãos" em "clientes".

6. O PAPEL DO SETOR PRIVADO NA SEGURANÇA PÚBLICA

Para finalizar, gostaria de tratar de duas questões breves sobre o papel do setor privado na área de segurança, e também sobre a experiência do Rio de Janeiro com esse tipo de empresas de vigilância patrimonial.

Um levantamento[8] interessante realizado pelo The Intercept Brasil em 2018 mostrou que uma em cada quatro empresas de segurança privada que operavam na região metropolitana do Rio de Janeiro pertenciam a agentes de segurança. Neste sentido, coloca-se uma questão do conflito de interesses. Essas empresas privadas são mais requisitadas e ganham mais contratos a partir de um aumento da sensação de insegurança, de uma percepção de alta e ameaçadora criminalidade. Ou seja, quem está gerindo essas empresas que ganham com esse aumento da sensação de insegurança são exatamente os agentes que deveriam garantir a segurança e o combate ao crime.

E essas relações acabam sendo mais dramáticas no Rio de Janeiro, com todo o avanço de grupos paramilitares e milícias que dominam vastos territórios do estado. Das 638 empresas que o Intercept conseguiu monitorar na Receita Federal, apenas 126 possuíam autorização da Polícia Federal para funcionarem, revelando que boa parte dessas empresas estavam na clandestinidade. E, quando a gente olha para as áreas de milícia, que são um problema seríssimo do Rio de Janeiro, 90% dessas empresas privadas eram empresas clandestinas.

8. COSTA, Breno; CHAVES, Reinaldo; POTTER, Hyury. O lucrativo exército de segurança privada comandado por militares, milicianos e amigos de Eduardo Cunha no Rio. Intercept Brasil, 16 jul. 2018. Disponível em: https://www.intercept.com.br/2018/07/16/o-lucrativo-exercito-de-seguranca-privada-comandado-por-militares-milicianos-e-amigos-de-eduardo-cunha-no-rio/. Acesso em: 20 set. 2024.

7. A GABRIEL

Para finalizar, eu queria falar um pouco sobre a Gabriel, que é uma startup que nasceu no Rio de Janeiro e se vendeu como uma solução que acabaria com a criminalidade no Rio de Janeiro. Uma promessa que, para quem conhece a história do Rio, já foi feita por alguns governantes, que prometiam acabar com a criminalidade em cinco meses e foram malfadados. Essa startup iniciou seu trabalho focando na Zona Sul da capital. Se vendia exatamente como uma facilidade e uma porta de acesso a uma melhoria na sensação de segurança, nos espaços públicos dos condomínios que a contratavam.

O Intercept recebeu alguns materiais de ex-funcionários da Gabriel que fizeram alguns prints e coleta de informações produzidas dentro dos sistemas da empresa. E o que foi revelado é que existia um canal clandestino da Gabriel com as polícias Militar e Civil. Ou seja, a demanda de policiais por imagens produzidas pela Gabriel não era oficiada, e sim feita por um canal clandestino, sem controle e nem registro dessas solici-

tações. Existem pelo menos dois problemas. Quando a gente não oficia a demanda por imagens por canais oficiais, muitas dessas imagens contendo dados pessoais sensíveis, coloca-se todo esse processo, todo esse diálogo entre setor público e setor privado numa área em que nós, como cidadãos, não podemos ter acesso ou criar mecanismos para controlar essa atuação. Não há possibilidade, por exemplo, de se verificar exatamente como tem se dado essa relação entre agentes públicos e privados, a regularidade dessas conversas, levando à possibilidade de vermos o que foi encontrado no canal interno da Gabriel, que tinha a demanda por prisão de determinada pessoa que foi flagrada pelas câmeras por furtos de celular.

Além disso, o Intercept revelou que os policiais tiravam fotos das pessoas que foram detidas como suspeitos do cometimento de crimes e mandavam para a Gabriel, e a empresa circulava em grupos de WhatsApp e dentro do seu Slack.

E uma outra questão é que se há uma empresa que vende esse acesso facilitado na segurança pública, impõe-se para as polícias uma atenção, um tipo de demanda, que acaba privilegiando, de certa forma, uma atenção desproporcional para áreas mais ricas, que podem pagar a Gabriel. Há, neste sentido, o fortalecimento do que já se vê desde muito antes dessas empresas serem tão espraiadas pela cidade do Rio de Janeiro, que é essa super atenção a bairros mais abastados da cidade, enquanto que outras áreas da cidade ficam sem policiamento ou tem policiamento muito deficiente.

8. DESIGUALDADE NA SEGURANÇA PÚBLICA

É muito enganoso pensar - e aí, novamente eu falo da experiência do Rio de Janeiro - que as cidades se dividem em áreas ricas, onde ocorrem crimes patrimoniais, e em partes pobres, onde ocorrem os crimes violentos. Muito pelo contrário, no Rio de Janeiro, nos lugares onde ocorre mais homicídios, também são os lugares onde ocorre mais roubo de veículos, mais roubos de celular, mais roubos de ônibus, mostrando que não existe necessariamente essa relação. Há o registro de uma presença muito maior das polícias nas regiões mais abastadas da cidade, essas áreas onde ocorrem menos crimes, tanto patrimoniais quanto crimes violentos.

E essa construção de canais de diálogo privilegiados entre essas empresas privadas, como a Gabriel, com o setor público através das polícias colabora para que a gente tenha o aprofundamento dessa hipervigilância e esse hiperpoliciamento nas partes mais abastadas em direção à resolução de crimes patrimoniais e crimes violentos, enquanto a gente perde a possibilidade de pensar no alocamento da força policial de uma maneira mais justa dentro do que se vê no cenário de registro de crimes.

É isso. Obrigado!

07.

"E QUANDO A MÁQUINA ERRA?": A POLÍTICA DA FALHA EM TECNOLOGIAS DE SEGURANÇA[1]

Daniel Edler

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Vitor Vilanova.

Em minha apresentação vou falar um pouco sobre policiamento preditivo e sobre reconhecimento facial, mas a partir de uma perspectiva um pouco diferente da que foi debatida até aqui no painel. Faço pesquisa sobre tecnologias de segurança há vários anos, com foco principalmente no trabalho das polícias do Rio de Janeiro e de São Paulo. Nesse tempo, já pesquisei a implementação de câmeras corporais, o impacto de sistemas de reconhecimento facial, a rotina de centros de operações, processos de produção de dados criminais e o uso de aplicativos de policiamento preditivo. Fundamentalmente, o que tento entender na minha pesquisa é o processo de produção dessas tecnologias e o impacto na ação policial.

No entanto, nos últimos tempos tenho me interessado por um tema mais específico dentro do debate sobre tecnologia, vigilância e formas de controle social. Enquanto eu mapeava o uso de novas tecnologias e o debate sobre seus efeitos na segurança pública, comecei a identificar alguns padrões nas críticas a esses sistemas, principalmente, no que tange ao uso de falhas, erros e vieses como categorias mobilizadas para jogar luz sobre os efeitos problemáticos das inovações e para resistir aos investimentos nessa área. E é sobre isso que vou falar um pouco mais hoje. Para ser mais exato, vou discutir sobre a *política da crítica às falhas sociotécnicas*.

1. NOVAS TECNOLOGIAS E A CRÍTICA ACERCA DAS "FALHAS"

No Brasil, a gente tem visto desde o ciclo de megaeventos (incluindo Copa do Mundo, Olimpíadas, a visita do papa, Rio+20, etc.) grandes investimentos em tecnologias que prometem melhorar a segurança pública, tornando a polícia mais eficiente e eficaz. Dentro dessas inovações, estão os investimentos em câmeras, softwares de análise criminal e alocação de patrulhas. Em praticamente todas as grandes cidades, há centros integrados de comando e controle, está em operação algum modelo de cerco eletrônico, e a polícia já faz uso de câmeras com reconhecimento facial, *body-cams*, sistemas de mapeamento, análise e previsão de crimes.

Nesse contexto, temos um debate público em que se apresentam dois grupos antagônicos. De um lado, o gestores das polícias e as empresas que desenvolvem esses sistemas alegam que as novas tecnologias "revolucionam" a forma de combater o crime e que são inovações "imparáveis" (a gente vê discursos do tipo: "não tem outro jeito", "é o futuro", "todo mundo lá fora faz assim"). Trata-se de um discurso tecnocrático que culmina com uma retórica anti-política, muito semelhante, inclusive, aos argumentos que animam reformas econômicas. Nessa perspectiva, as tecnologias trariam eficiência, transparência, *accountability* e legitimidade, corrigindo os defeitos da sociedade ou, mais especificamente, da polícia. Se a gente for olhar o discurso que hoje cerca o reconhecimento facial, por exemplo, vamos encontrar exatamente esses pontos. Mesmo que faltem estudos robustos de avaliação de impacto, quem resiste ou critica a implementação de uma nova ferramenta é "ludista", "tecnofóbico", "não sabe do que tá falando" ou, pior, é "a galera dos direitos humanos que defende bandido".

Do outro lado, a gente vê os críticos desses sistemas alertando não só para os riscos em termos de perda de privacidade e liberdade, mas enfatizando também que as narrativas oficiais são ilusórias, pois os sistemas falham, são cheios de erros e vieses. Desse modo, os benefícios promovidos por empresas privadas e agentes de segurança raramente são atingidos porque entre a prancheta do desenvolvedor e o uso da tecnologia

pela polícia, há uma série de processos que podem impedir que o objetivo final seja cumprido. Esse argumento sobre a centralidade da falha, em geral, se desdobra em três pontos específicos que tento mapear a seguir.

2. OS TRÊS USOS DA FALHA NA CRÍTICA ÀS TECNOLOGIAS DE SEGURANÇA

Primeiro, o processo de desenvolvimento tecnológico é atravessado por escolhas dos agentes que atribuem, ou inserem, subjetividade em sistemas até então puramente objetivos. E é essa subjetividade que causa os erros. Os sistemas de predição de crimes, por exemplo, falham porque os bancos de dados usados para treinar os algoritmos são enviesados pelos padrões anteriores de atuação da polícia. Se a polícia se concentra em determinadas áreas, vai gerar mais dados sobre criminalidade ou eventos de "desordem urbana" nessas mesmas áreas e o algoritmo vai apenas reproduzir esse padrão. Para muitos, esse viés de entrada seria ainda mais significativo em países como o Brasil, onde a polícia é usada historicamente para reprimir jovens, negros e moradores das periferias urbanas. Logo, é para essas regiões que as viaturas serão deslocadas e é com especial atenção a esses perfis socais/raciais que os policiais farão o patrulhamento, o que gera um *feedback loop*. Dito de outra forma, os padrões enviesados de entrada levam a mapas de crimes enviesados e guiam o comportamento policial, de modo a reproduzir a tendência de policiamento de determinados grupos.

Mesmo os sistemas mais avançados do mercado têm esse problema. Kristian Lum e William Isaac (2016) fizeram um estudo sobre prisão por posse de drogas em Oakland, na California, e observaram o impacto de programas de policiamento preditivo. O que o estudo mostrou é que o sistema da PredPol (hoje a Geolitica), indicava mais crimes de posse de drogas em bairros com concentração de negros, mesmo que os *surveys* sobre consumo de drogas no Estados Unidos mostrem taxas muito semelhantes de usuários em diferentes grupos populacionais. Ou seja, o que Lum e Isaac (2016) apontam é que os sistemas estão reconhecendo o padrão de policiamento, não o padrão de criminalidade. Em outras palavras, a busca por uma alocação mais eficiente de patrulhas e pela identificação de perfis de suspeição tende a gerar prisões injustas porque se vale de padrões injustos de produção de dados.

A falha nesse exemplo está na relação humano-máquina. Em algum momento dessa composição de dados, algoritmos, programadores e usuários, a objetividade que viria da matemática e da estatística teria sido inundada por subjetividade humana, o que gera erros e vieses. Se olharmos a campanha recente pelo banimento de tecnologias de reconhecimento facial no Brasil, o medo dos falsos positivos, ou seja, que pessoas inocentes sejam identificadas como criminosos procurados, é constantemente mobilizado. A pergunta central da campanha "Tire meu rosto da sua mira" é "e quando a máquina erra?". Esse erro justificaria, portanto, o banimento da tecnologia.

O segundo argumento crítico sobre a "falha" é que os profissionais de segurança "corrompem" a tecnologia no dia a dia. Um exemplo disso é a dinâmica narrada na pesquisa do Bruno Cardoso (2014), professor do NECVU da UFRJ. O Bruno fez uma etnografia sobre o uso de câmeras pela polícia militar em Copacabana. Ele ficou um bom tempo acompanhando a rotina da sala de operações do batalhão e uma das coisas que ele observou é que as câmeras raramente serviam para flagrar um crime, mas que os policiais muitas vezes usavam as imagens como *voyeurs*. Apesar do discurso sobre mais segurança

e eficiência, Bruno registrou várias vezes policiais observando pessoas na orla ou simplesmente direcionando as câmeras para eventos corriqueiros do bairro. Nesses casos, a crítica aponta que o projeto de inovação passa por um desvio. Os policiais usam a tecnologia para fins não previstos originalmente. Ou, como me disse certa vez um policial carioca, a "polícia do Rio corrompe até a tecnologia".

A partir desse caso anedótico, podemos ver também muitas críticas sobre falhas que apontam que os sistemas desenvolvidos no norte global não se adaptam à realidade do sul global. Nesse caso, as falhas se dariam no processo de implementação, pois as tecnologias não são pensadas para diferentes contextos. Ou seja, não basta dizer que algoritmos preditivos estão em todos os lugares para apontar uma convergência global de práticas de policiamento. Os sistemas desempenham diferentes funções e induzem diferentes práticas em diferentes lugares. Nessa direção, temos análises que indicam que os desafios de segurança pública no Brasil são muito particulares e, fundamentalmente, que as polícias não são burocracias modernas no sentido weberiano. Como pano de fundo para esse tipo de argumento sobre a "tropicalização da tecnologia", vemos discursos do tipo: a câmera falha porque não há capacidade intelectual entre os policiais para operar, ou não há racionalidade orçamentária para garantir manutenção, não há infraestrutura necessária em cidades de países em desenvolvimento, etc. Nesse terceiro grupo de críticas, a falha é culpa de um ambiente institucional deteriorado.

Apesar de diferentes, esses três usos da falha para um projeto crítico levam, em geral, a um mesmo argumento: os sistemas não funcionam como seus desenvolvedores e as forças de segurança defendem. Não há ganhos de eficiência nas práticas de segurança e muitos dos sistemas se tornam obso-

/ A TECNOLOGIA COMO UMA REDE SOCIOTÉCNICA QUE PASSA POR ESCOLHAS POLÍTICAS, SUBJETIVIDADES, E, FUNDAMENTALMENTE, RELAÇÕES DE PODER /

letos rapidamente. Além disso, como os sistemas costumam ter vieses contrários a determinadas populações, as falhas técnicas aprofundam o problema da discriminação racial.

3. COMO A CRÍTICA A PARTIR DA FALHA CONTRIBUI PARA A ANÁLISE?

Mas o que as falhas fazem para a gente criticamente? Por que é importante falar dessas falhas? Estas críticas são, em muitos aspectos, muito importantes. Elas ajudam, por exemplo, a desmistificar o poder da tecnologia, o que Evgeny Morozov (2013) chama de "tecno-solucionismo", e apontam para as limitações do "determinismo tecnológico" que é muito presente nos debates sobre segurança pública. Ou seja, os vários estudos de caso sobre falhas tecnológicas servem como narrativas que advertem contra a ideia de que só porque um sistema preditivo foi implementado já podemos antecipar seu impacto, seja porque "traz mais segurança" ou porque "traz mais opressão".

Esse argumento corrobora o que Lee Vinsel (2021), professor da Virginia Tech, alerta sobre o "*criti-hype*", que, nas palavras dele, "pega os enunciados sensacionalistas de empreendedores e desenvolvedores, os inverte, e começa a falar sobre os riscos". Vinsel usa como exemplo os argumentos de Shoshana Zuboff (2021) sobre "capitalismo de vigilância" e "poder instrumentário". Não importam aqui os detalhes desses conceitos, mas cabe apontar que, segundo Vinsel, Zuboff constrói um argumento sobre formas de manipulação de ações e subjetividades sem ter evidências robustas que sustentem tal alegação. O livro dela é um grande ensaio sobre uma nova era do capitalismo que, como aponta o Vinsel, se pauta basicamente em uma leitura acrítica de dois relatórios internos do Facebook. Para ele, isso gera dois problemas:

< 1 > cria um ambiente informacional confuso que dá credibilidade ao que ele chama de "*industry bullshit*" – ou seja, a ideia de que o *Facebook* e o *Google* são de fato capazes de nos manipular e nos levar a votar em determinado candidato ou a comprar determinado produto;

< 2 > nos distrai dos problemas reais do mundo, tira o foco de questões mais ordinárias da tecnologia e da infraestrutura, e que têm consequências políticas profundas.

Trazer nuances para o determinismo tecnológico é, portanto, o primeiro aspecto positivo da falha enquanto dispositivo de crítica. A segunda contribuição é que esse tipo de argumento nos obriga a pensar nos efeitos desiguais das falhas. O "como" a tecnologia falha, a forma pela qual ela falha, importa. Por exemplo, o debate sobre falhas tecnológicas foi central para trazer à ordem do dia outro debate subjacente: o racismo algorítmico. Isso acontece porque, ao mostrar o descompasso entre os enunciados e as práticas, a falha abre uma fresta para vermos a composição da tecnologia em toda a sua complexidade. A tecnologia como uma rede sociotécnica que passa por escolhas políticas, subjetividades, e, fundamentalmente, relações de poder.

Quando falamos que tecnologias de policiamento preditivo automatizam as decisões sobre abordagem policial e tiram a discricionariedade do agente na rua, vemos acoplado a esse argumento um imaginário de neutralidade, como se estivéssemos falando de uma decisão pautada em "fatos" e não no mero "faro policial". Ao trazer o debate sobre as falhas de identificação que incidem mais sobre corpos negros, recuperamos então o caráter político das formas de policiamento.

Como resumem Claudia Aradau e Tobias Blanke (2021), professores do King's College de Londres e da Universidade

de Amsterdã: "como erros surgem, como eles são descobertos, a quem eles são atribuídos, e como eles devem ser resolvidos são questões profundamente políticas. Preocupações com erros, enganos e imprecisões têm moldado debates sobre o que as tecnologias fazem e onde e como determinadas tecnologias podem ser usadas e para quais propósitos". Assim, pensar na falha nos obriga a observar os deslocamentos produzidos pelas novas tecnologias e não só ler os manuais de instrução dos novos equipamentos de segurança e produzir elogios ou críticas.

4. AS LIMITAÇÕES DA CRÍTICA A PARTIR DA FALHA

Qual é o problema então de se pensar em termos de falhas? Me parece que a forma como o debate público tem apostado na crítica a partir da falha tem também algumas limitações centrais. Muitas vezes a identificação da falha não impõe barreiras ao desenvolvimento e implementação de novas tecnologias, mas o contrário: se torna o motor para a defesa de mais inovação e mais investimentos nesse campo.

No setor empresarial, nas *startups*, falhar não é um problema, mas parte normal do processo de pesquisa e inovação. Nesse contexto, a falha tem um sentido schumpeteriano de destruição criativa, no senso comum mesmo, em que apenas os resilientes (aqueles que passam por muitas falhas e persistem) fazem realmente a inovação. Nesses espaços, a gente ouve o tempo todo o discurso empreendedor de que o "sucesso é ir de um fracasso a outro sem desistir". Ou que o importante é "aprender com os erros" já que a "próxima falha será melhor".

Além disso, o central na justificativa dessas novas tecnologias de segurança não é produzir, por exemplo, algoritmos de predição de crimes que sejam 100% precisos, mas sim sistemas que tenham novas versões que permitam cada vez mais otimizar a alocação de patrulhas. Em outras palavras, a ideia não é que a falha seja eliminada, mas que ocorra um aperfeiçoamento paulatino – e é essa melhoria que justifica os investimentos. O desafio que se coloca, portanto, é que todo erro identificado no sistema revela a potencialidade de melhorias de precisão. Erros são vistos como indicativos de onde a inovação deve acontecer e, em via de regra, quando falamos de tecnologias de segurança, gera uma demanda por bases de dados mais amplas. A lógica é: se um algoritmo de identificação biométrica produz erros porque é treinado apenas a partir de rostos brancos, o que precisamos fazer é coletar e catalogar mais rostos. Ou seja, simplesmente apontar que há erros em um sistema não leva à suspensão de seu uso. A falha funciona muitas vezes para expandir e não para reduzir os sistemas.

No campo da ciência há também uma compreensão de que a falha não imobiliza ou assusta o cientista. A falha – no sentido do erro da hipótese ou do experimento – é a própria razão de ser da ciência moderna. O Robert Merton (1987), por exemplo, falava em "*specified ignorance*", aquela que os cientistas reconhecem e apontam como o espaço "vazio" a ser preenchido por suas pesquisas. Este tipo de falha está, inclusive, nos nossos pedidos de financiamento. Quando a gente escreve um projeto, um dos pontos centrais é apontar os buracos da literatura atual sobre determinado tema. Se não há falha nos nossos sistemas de explicação do mundo, não há motivo para mais pesquisas e mais investimento.

Ou seja, tanto a inovação tecnológica quanto a ciência moderna trabalham com uma noção produtiva da falha. Cientistas e empreendedores privados não veem a falha como uma crítica paralisante, mas como uma etapa natural do processo

de inovação. O progresso ocorre na medida em que identificamos e corrigimos as falhas. Além disso, criticar tecnologias de segurança a partir do erro implica em assumir que há uma forma correta de uso desses novos equipamentos que nos aguarda do outro lado da falha. Um *upgrade* no sistema de identificação, por exemplo, acabaria com a discriminação racial e legitimaria seu uso. Assim, os erros se tornam um defeito temporário, e o futuro do algoritmo passa a ser o da otimização infinita.

5. CONSIDERAÇÕES FINAIS: COMO MOBILIZAR A FALHA DE MODO CRÍTICO?

O desafio para quem quer fazer a crítica de novas tecnologias não é só observar desvios e apontar problemas técnicos, mas entender seus efeitos. Nós queremos sistemas de reconhecimento facial muito precisos? Nós queremos sistemas de policiamento preditivo muito precisos? O que eles geram em termos de técnicas de controle social? Como alteram a rotina policial? Talvez essas sejam as questões mais interessantes a serem enfrentadas.

Sistemas de policiamento preditivo, com mais ou menos falhas, aprofundam uma lógica perversa que resume as políticas de segurança pública ao trabalho repressivo da polícia. Bastaria alocar patrulhas e fazer abordagens para reduzir a mancha criminal e resolver o problema. Quando fazemos apostas em tecnologias que alimentam esse tipo de prática repressiva, perdemos de vista outras políticas preventivas voltadas para melhoria da qualidade de vida e para redução de riscos de vitimização. Focamos nas causas mais imediatas do crime e negligenciamos políticas públicas robustas e com efeito de longo prazo (Edler & Lobato, 2021).

Em resumo, o desafio é pensar como a falha pode ser problematizada de forma a produzir ruídos em espaços antes silenciosos, produzir rachaduras em consensos. Ou seja, apontar a falha não basta. Mas podemos usar a falha para mostrar que novas tecnologias são constituídas a partir de relações de poder e que operam dentro dos circuitos de acumulação de riqueza e violência.

REFERÊNCIAS

ARADAU, C., BLANKE, T. (2021) Algorithmic Surveillance and the Political Life of Error. *Journal for the History of Knowledge*, 2(1): pp. 1–13.

CARDOSO, B. (2014), *Todos os Olhos: Videovigilâncias, voyeurismos e (re) produção imagética*. Rio de Janeiro, Editora UFRJ.

EDLER, D. & LOBATO, L. (2021) A política do policiamento preditivo: Pressupostos criminológicos, técnicas algorítmicas e estratégias punitivas. *Revista Brasileira de Ciências Criminais*, 29(183), pp. 57-98.

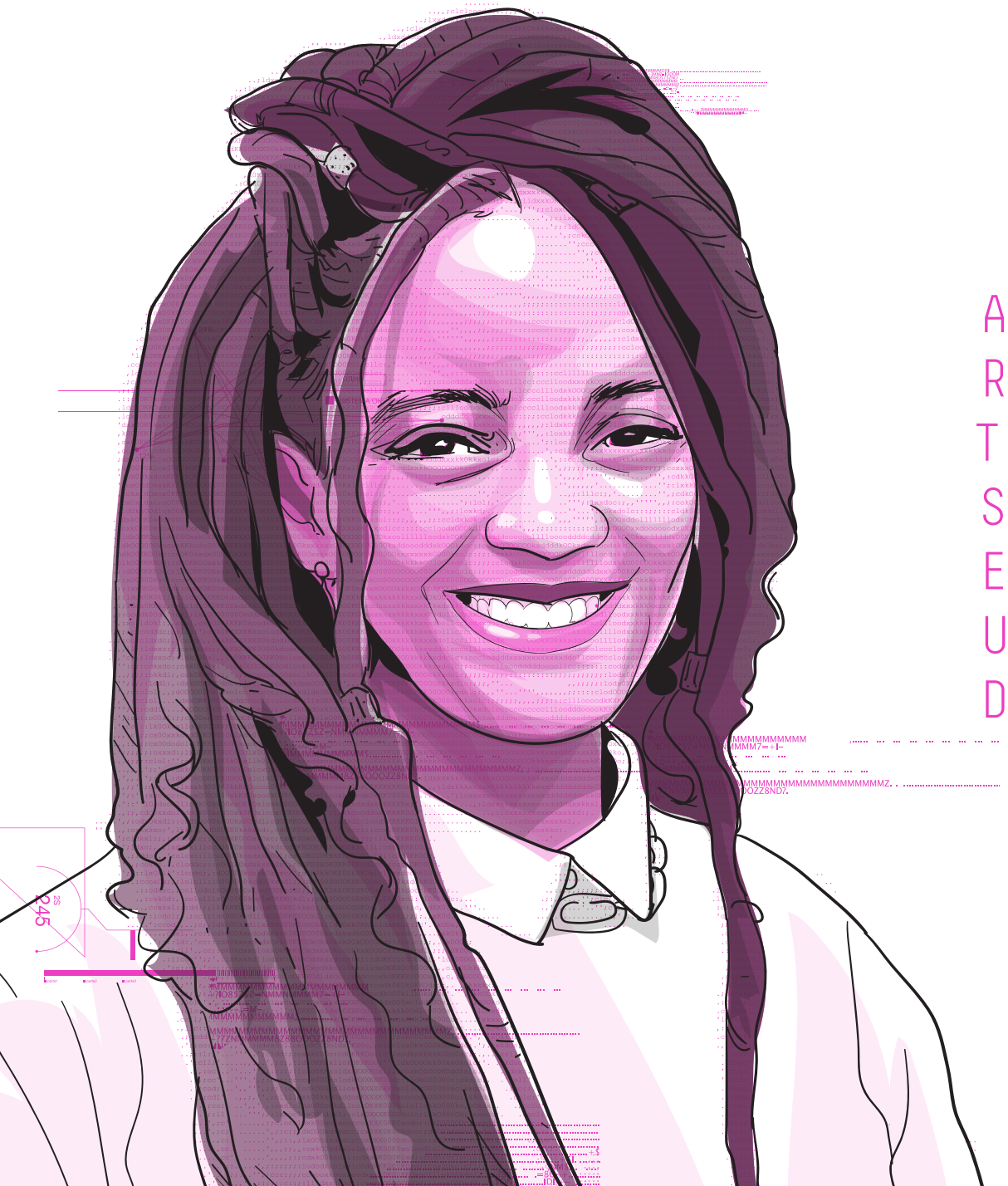
LUM, K. and ISAAC, W. (2016). To predict and serve? *Significance*, 13(5), pp. 14-19.

MERTON, R. (1987) Three Fragments from a Sociologist's Notebooks: Establishing the Phenomenon, Specified Ignorance, and Strategic Research Material. *Annual Review of Sociology*, 13: 1-29

MOROZOV, E. (2013). *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems that Don't Exist*. London: Penguin.

VINSEL, L. (2021), "You're Doing It Wrong: Notes on Criticism and Technology Hype". *Medium*, 1 fev. Disponível em: https://sts-news.medium.com/youre-doing-it-wrong-notes-on-criticism-and-technology-hype-18b08b4307e5

ZUBOFF, S. (2021) *A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder.* Rio de Janeiro: Editora Intrínseca.



08.

A ATUALIZAÇÃO DO RACISMO NAS ESCOLHAS TECNOLÓGICAS DE SEGURANÇA PÚBLICA E PREOCUPAÇÕES PARA UMA AGENDA REGULATÓRIA DA IA NO BRASIL

Fernanda dos Santos Rodrigues Silva

Auto-suficiência na criação e adoção de tecnologia, assim como no desenvolvimento científico, precisa ocorrer simultaneamente ao desenvolvimento das nações, obedecendo seu ajustamento funcional ao respectivo ambiente e realidade humana.
Abdias do Nascimento, A respeito de ciência e tecnologia (O Quilombismo, 1980).

O CONTEXTO DA SEGURANÇA PÚBLICA NO BRASIL

Segundo dados do Anuário Brasileiro de Segurança Pública,[1] o número de vítimas de letalidade policial foi de 6.393 em 2023, representando um aumento de 188,9% na última década. O perfil das vítimas é majoritariamente negro (82,7%), jovem de 12 a 29 anos (71,7%) e masculino (99,3%). Em outras palavras, o risco de uma pessoa negra morrer em virtude de intervenção policial no Brasil é 3,8 vezes maior do que para outros segmentos da população. No caso de adolescentes, o número é ainda mais alarmante. Atualmente, "a intervenção policial é (...) a causa de cerca de uma a cada sete mortes violentas intencionais de adolescentes no país",[2] representando 16,6% do total de mortes violentas na faixa etária de 12 a 17 anos e com maior impacto sobre a juventude negra, que é a mais afetada desproporcionalmente.

Quando se olha para a composição de pessoas encarceradas no país, o cenário é bastante similar. Com um aumento de 2,4% em relação a 2022, o sistema prisional brasileiro conta com 852.010 pessoas presas, sendo que 1 em cada 4 não foi sequer julgada ainda.[3] Dentre os presos, a maior parte são homens e negros. Considerando a história de cobertura das informações do Anuário, que contém dados desde 2005 até 2023, ressalta-se que a representação racial nunca se deu de forma distinta.[4] É possível afirmar, assim, que o processo criminal no Brasil tem cor, ao mesmo tempo em que "é razoável supor, a partir daí, que a decisão de quem será parado, revistado, detido e condenado é guiado pela raça".[5]

O cenário atual do país insiste em ecoar uma lógica que remete aos tempos logo após a abolição da escravatura, em que a determinação prevista em lei de prisão correcional para "mendigos aptos, vagabundos, capoeiristas e desordeiros" evidenciava a intenção de criminalizar a população negra da sociedade, que, após ser deixada à própria sorte em 1888, sem qualquer forma de reparação ou reinserção social, poderia ser vista como "desordeira" e "vagabunda".[6] Realocando a violência estatal que antes se encontrava legitimada no seio da escravização, o Estado brasileiro parece ter encontrado na política criminal e de segurança pública uma forma de manter o corpo negro e marginalizado como o principal alvo de medidas repressivas, arbitrárias e, não raro, injustas.

Segundo um levantamento feito pelo Colégio Nacional de Defensores Públicos Gerais (CONDEGE), 81% dos presos injustamente em virtude de reconhecimento fotográfico no Brasil

1. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública 2024**. São Paulo: FBSP, 2024.

2. MARTINS, Cauê. O rosto familiar da violência contra crianças e adolescentes. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública 2024**. São Paulo: FBSP, 2024, p. 211.

3. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Op. cit.

4. BRANDÃO, Juliana. Sistema prisional brasileiro e o permanente mercado das carnes mais baratas. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública 2024**. São Paulo: FBSP, 2024.

5. *Ibidem*, p. 360.

6. FLAUZINA, Ana Luiza Pinheiro. **Corpo negro caído no chão**: o sistema penal e projeto genocida do estado penal brasileiro. 2006. 145 p. Dissertação (Mestrado em Direito). Universidade de Brasília, Brasília, DF, 2006. Disponível em: http://www.cddh.org.br/assets/docs/2006_AnaLuizaPinheiroFlauzina.pdf. Acesso em: 19 ago. 2024.

são negros.[7] Para especialistas, o estudo apontou que autoridades não continuavam a investigação criminal após a vítima indicar o reconhecimento do suposto criminoso por meio de fotos, mesmo quando havia provas de que a pessoa indicada não poderia ter cometido o crime - como por estar em outro país na data do fato, por exemplo.[8] Ainda que seja uma prova frágil, o reconhecimento fotográfico tem sido utilizado como principal fundamento para algumas prisões, resultando em detenções equivocadas de pessoas inocentes[9] e o estereótipo de quem é criminoso no país contribui para isso.

Um estudo realizado pelo Centro de Estudos de Segurança e Cidadania (CESeC),[10] de 2022, que buscou compreender quais as experiências da população no Rio de Janeiro em relação a abordagens policiais, reforça essa percepção. Os dados obtidos demonstraram uma evidente discrepância: mesmo sendo apenas 48% da população carioca, as pessoas negras constituíam 63% daquelas paradas/abordadas pela polícia e 66% daquelas paradas/abordadas mais de 10 vezes.

> Aqueles que responderam terem sido "parados mais de 10 vezes" (e muitos desse grupo já foram parados centenas de vezes) compõem um setor da sociedade que representa quase um quinto dos já abordados (17%), que são alvo reiterado do olhar de incriminação prévia por agentes da lei. Sentem-se vistos como criminosos, sentem medo quando avistam policiais, pressentem e, de alguma forma, vivenciam as abordagens mesmo quando elas não acontecem.[11]

Assim, embora para alguns possa representar segurança, a experiência de pessoas negras com a polícia faz com que essa relação se estabeleça de forma tensa e frequentemente violenta - violência essa que não se encerra na abordagem e acompanha também aqueles que ingressam no sistema penal, ainda que de maneira injusta. No âmbito da Arguição de Descumprimento de Preceito Fundamental (ADPF) 347-DF, o Supremo Tribunal Federal reconheceu publicamente e de forma unânime o estado de coisas inconstitucional em que se encontra o sistema prisional brasileiro.[12] Segundo a decisão, essa desconformidade se dá em razão da (i) superlotação e baixa qualidade de vagas existentes, com déficit no fornecimento de bens e serviços essenciais; (ii) "entradas de novos presos no sistema de forma indevida e desproporcional, envolvendo autores primários e delitos de baixa periculosidade, que apenas contribuem para o agravamento da criminalidade"; e (iii) "da permanência dos presos por tempo superior àquele previsto na condenação ou em regime mais gravoso do que o devido".[13]

Para Ana Flauzina e Thula Pires,[14] entretanto, que analisaram o julgamento

7. DIRETORIA DE ESTUDOS E PESQUISAS DE ACESSO À JUSTIÇA. Relatório consolidado sobre reconhecimento fotográfico em sede policial. Disponível em: https://sistemas.rj.def.br/publico/sarova.ashx/Portal/sarova/imagem-dpge/public/arquivos/consolida%C3%A7%C3%A3o_relat%C3%B3rio_CONDEGE_e_DPERJ_reconhecimento_fotogr%C3%A1fico.pdf. Acesso em: 19 ago. 2024.

8. SANTANA, Igor. Relatórios apontam falhas em prisões após reconhecimento fotográfico. **Defensoria Pública do Estado do Rio de Janeiro**, Notícias, 24 fev. 2021. Disponível em: https://www.defensoria.rj.def.br/noticia/detalhes/11088-Relatorios-apontam-falhas-em-prisoes-apos-reconhecimento-fotografico. Acesso em: 19 ago. 2024.

9. *Ibidem.*

10. RAMOS, Silvia et al. Negro trauma: racismo e abordagem policial no Rio de Janeiro. Rio de Janeiro: CESeC, 2022, p. 14. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/02/CESEC_elemento-suspeito_final-3.pdf. Acesso em: 19 ago. 2024.

11. *Ibidem.*

12. BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Arguição de Descumprimento de Preceito Fundamental (ADPF) 347-DF**. Direitos fundamentais dos presos. ADPF. Sistema carcerário. Violação massiva de direitos. Falhas estruturais. Necessidade de reformulação de políticas públicas penais e prisionais. Procedência parcial dos pedidos. Recorrente: Partido Socialismo e Liberdade – PSOL. Recorrido: União e estados da federação. Relator: Ministro Marco Aurélio, 04 de outubro de 2023. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=773553256. Acesso em: 31 ago. 2024.

13. *Ibidem.*

da medida cautelar da referida ADPF, em 2020, apesar de reconhecer a violação estrutural de parâmetros normativos por parte de todos os poderes do Estado, em diferentes esferas federativas, a decisão da Suprema Corte, ao final, foi a de fortalecer esse mesmo sistema prisional, e não de findá-lo. Mesmo diante da repetição de uma falência do sistema prisional, elas afirmam que não há a conversão do discurso em "responsabilização dos órgãos públicos pelas violências e inconstitucionalidades que reproduzem e sustentam".[15]

As autoras recorrem ao passado para denunciar a situação do presente. Se na Constituição de 1824 ficou proibido o uso do açoite, mas se manteve o regime escravocrata, Ana Flauzina e Thula Pires defendem que o reconhecimento do "açoite que ocorre nas unidades prisionais, representado pelo estado de coisas inconstitucional" não é acompanhado do tratamento das "causas da sistemática violação de direitos que lá tomam assento de forma crua e brutal".[16] Isso as leva a concluir que "o racismo, com suas correlatas dimensões de gênero e sexualidade, é um fenômeno tão forte no Brasil que mesmo quando o órgão de cúpula do Poder Judiciário, o STF, se manifesta no sentido" contrário à arbitrariedade judicial e exclusão sistemática de grupos minoritários, a razão para "tamanha ilegalidade/inconstitucionalidade permanece em pleno funcionamento e isso não gera nem comoção popular, tampouco medidas judiciais de enfrentamento".[17]

O racismo, portanto, opera como uma engrenagem do sistema penal brasileiro, pelo menos, desde os tempos de império, servindo para a manutenção da subjugação e segregação de corpos negros do meio social. Para Ruha Benjamin, é possível afirmar que a própria construção de raça em si pode ser considerada uma tecnologia, na medida em que serve para "separar, estratificar e santificar as muitas formas de injustiça experienciadas por membros de grupos racializados", mas que "as pessoas rotineiramente re-imaginam e re-desenvolvem para os seus próprios fins".[18] Nessa senda, o racismo serve como ferramenta para conciliação entre contradições de uma sociedade que defende a liberdade para todas as pessoas ao mesmo tempo em que mantém milhões de pessoas presas.[19]

Desde o alvo mais frequente para abordagens policiais até o sofrimento em um sistema prisional que não se preocupa com a dignidade mínima de seus detentos, resultado de uma busca incessante por segurança através do encarceramento em massa, a população negra é atravessada de forma cotidiana pela discriminação e descaso do poder estatal. Em razão disso, a adição de novos aparatos digitais nesse contexto tende apenas a agravar a situação.

O USO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL PARA FINS DE PERSECUÇÃO CRIMINAL E A REPRODUÇÃO DA SELETIVIDADE DO SISTEMA PENAL

Considerando que o campo da persecução penal faz parte da segurança pública, dois exemplos do uso de tecnologias de IA auxiliam a visualizar melhor os desafios envolvidos nessa área. O primeiro deles diz respeito a sistemas de reconhecimento

14. FLAUZINA, Ana; PIRES, Thula. Supremo Tribunal Federal e a naturalização da barbárie. **Revista Direito e Práxis,** Rio de Janeiro, v. 11, n. 2, 2020, pp. 1211-1237. Disponível em: https://www.e-publicacoes.uerj.br/revistaceaju/article/view/50270/33896. Acesso em: 26 ago. 2024.

15. *Ibidem*, p. 1224.

16. *Ibidem.*

17. *Ibidem*, p. 1235.

18. BENJAMIN, Ruha. **Race after technology:** abolitionist tools for the New Jim Code. Medford, MA: Polity, 2019, p. 34.

19. *Ibidem*, p. 35.

facial, cuja utilização para fins de segurança pública no Brasil tem se intensificado. O carnaval de 2024 já é considerado o mais vigiado da história, com o uso de reconhecimento facial em oito estados do país.[20] Somente nos seis primeiros meses do ano, 39 eventos já utilizaram a tecnologia, junto a 21 municípios brasileiros que a empregaram em festas juninas.[21] A ferramenta é comumente utilizada em ações para localizar suspeitos e cumprir mandados de prisão durante investigações, como também para buscar foragidos da Justiça, dentre outras funções.

A escolha pela tecnologia, no entanto, parece ignorar diferentes avisos em torno do seu risco de vieses. Em 2018, um estudo emblemático realizado por duas pesquisadoras negras, Joy Buolamwini e Timnit Gebru,[22] denunciou o maior índice de falibilidade que esse tipo de tecnologia apresentava sobre o rosto de pessoas negras, mais especificamente mulheres (o outro do outro),[23] se comparado ao rosto de homens brancos. Com o histórico seletivo do sistema penal brasileiro, transpor esse tipo de problemática para a cena local, mesmo com as devidas precauções, significa assumir uma relevante possibilidade de potencialização dos já mencionados problemas de encarceramento em massa e criminalização da população negra.

Se em outro momento, o ideal de quem é criminoso e quem representa um perigo é alimentado por um imaginário racista impregnado na estrutura do Estado, agora o uso de novas

20. RODRIGUES, Yasmin et al. **Espetacularização da vigilância [livro eletrônico]**: suspeição policial e reconhecimento facial em grandes eventos. Rio de Janeiro: CESeC, 2024.

21. Ibidem

22. BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: **Conference on fairness, accountability and transparency**. PMLR, 2018. p. 77-91.

23. KILOMBA, Grada. **Memórias de plantação**: episódios de racismo cotidiano. Rio de Janeiro: Cobogó, 2019.

tecnologias racialmente falhas sustenta essa narrativa apoiado em uma pretensa objetividade da máquina. No caso do uso de sistemas de reconhecimento facial para fins de segurança pública, "não há hiato entre abordagem (para averiguação ou revista, por exemplo) e prisão".[24] Isto se dá, pois "a combinação feita pela tecnologia entre a identificação do indivíduo e o banco de dados passa a ser informação incontestável, produzindo, mesmo antes do processo judicial, a verdade jurídica".[25]

A esse respeito, Tarcízio Silva chama atenção para o fato de que a junção entre a opacidade em torno de sistemas algorítmicos - comumente lidos como "neutros" – e a opacidade em torno do racismo no Brasil - apoiada em uma dissipação das discussões raciais e sobre supremacismo branco no Ocidente - resultam na convergência de "tradições de ocultação e exploração, tanto nas relações raciais quanto nas decisões ideológicas que definem o que é tecnologia e o que é inovação desejável".[26] No entanto, é preciso reconhecer que "(...) previsões guiadas por dados não necessariamente fornecem decisões neutras".[27] Em seu lugar, o que se vê "é justamente o oposto: a tecnologia não apenas é capaz de propagar preconceitos e discriminações, como também lhes conferir alta escalabilidade, já que seu alcance é potencializado".[28]

O segundo exemplo de uso de IA para persecução penal ajuda a compreender melhor esse cenário. Sistemas de policiamento preditivo, como o próprio

24. RODRIGUES, Yasmin et al. **Espetacularização da vigilância [livro eletrônico]:** suspeição policial e reconhecimento facial em grandes eventos. Rio de Janeiro: CESeC, 2024.

25. *Ibidem.*

26. SILVA, Tarcízio. **Racismo algorítmico:** inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc São Paulo, 2022, p. 14.

27. KREMER, Bianca. **Direito e tecnologia em perspectiva amefricana**: autonomia, algoritmos e vieses raciais. 2021. Tese (Doutorado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2021, p. 132.

28. *Ibidem*

nome já diz, trata-se de tecnologias construídas para buscar prever a ocorrência de crimes e, assim, contribuir para um direcionamento supostamente mais apropriado de efetivo policial para áreas consideradas mais perigosas. Entretanto, no lugar de melhorar os índices de violência e criminalidade, o que se tem visto é a piora de problemas já existentes - e independentemente das bases de dados utilizadas para o seu funcionamento.

No Estados Unidos, os tipos de policiamento preditivo mais utilizados costumam ser: a) algoritmos baseados em localização, que tentam prever onde e quando crimes poderão ocorrer com base em conexões feitas entre histórico de taxas de crime, eventos e lugares (o PredPol, que é um dos modelos mais conhecidos, atua dessa forma); e b) algoritmos focados em compreender quem tem mais chances de se envolver em um crime futuramente, com base em dados pessoais, como idade, gênero, estado civil, histórico criminal e de abuso de substâncias, dentre outros (o COMPAS, também utilizado nos EUA, é um dos exemplos mais conhecidos).[29] Para os fins deste texto, o primeiro caso merece especial atenção.

29. HEAVEN, Will Douglas. Predictive policing algorithms are racist. They need to be dismantled. **MIT Technology Review**, 17 jul. 2020. Disponível em: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/. Acesso em: 28 ago. 2024.

Em relação àquele, há, pelo menos, duas formas pelas quais os dados policiais utilizados em sistemas como o PredPol podem ser enviesados. A primeira é pelo fato de que, ao passo em que reflete práticas e políticas da polícia, "se um grupo ou área geográfica for desproporcionalmente alvo de contatos e ações policiais injustificadas, este grupo ou área será sobrerrepresentado nos dados, de formas que frequentemente sugerem maior criminalidade".[30] A segunda razão é que esses mesmos dados podem ocultar práticas policiais seletivas, que fazem com que certos tipos de crime e possíveis criminosos sejam mais investigados do que outros.[31] Veja-se que em nenhum momento o tratamento de dados sobre raça é utilizado para o funcionamento do sistema. Ainda assim, a partir do cruzamento de informações, o que se verifica é que a IA acaba penalizando novamente comunidades que já são historicamente mais vigiadas pela polícia, como é o caso de comunidades negras.

30. RICHARDSON, Rashida; SCHULTZ, Jason; CRAWFORD, Kate. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. **New York University Law Review**, v. 94, n. 192, maio/2019, pp. 192-233, p. 218. Disponível em: https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf. Acesso em: 28 ago. 2024.

31. *Ibidem*.

32. *Ibidem*, p. 223.

Em virtude disso,

> Os ciclos de retroalimentação de confirmação também influenciam as políticas públicas ao impulsionar ou fornecer justificativa para que autoridades governamentais apoiem políticas que tentam micromanipular ou expulsar comunidades que são erroneamente percebidas como produtoras de problemas ou como aumentadoras da desordem.[32]

Dessa forma, uma vez que a realidade sobre a qual os sistemas são tanto treinados como pretendem atuar é racista, mesmo a mudança da fonte dos dados pode acabar gerando o mesmo tipo de estereotipização. Um estudo realizado com dados coletados ao nível distrital de Bogotá, na Colômbia, buscou analisar se a utilização de dados sobre relatos de crime, e não sobre prisões, para fins de policiamento preditivo

poderia reduzir os vieses discriminatórios da máquina. A pesquisa apontou que mesmo com a mudança na origem dos dados, os resultados ainda eram "espacialmente enviesados devido à heterogeneidade geográfica nas taxas de notificação de crimes", o que "pode resultar em policiamento excessivo de certas comunidades, enquanto outras permanecem subatendidas pela polícia".[33]

Segundo as pesquisadoras, os resultados indicam que "distritos com baixas taxas de notificação de crimes têm menos de seus pontos quentes de crimes detectados pelo algoritmo", enquanto "distritos com altas taxas de notificação de crimes apresentam uma concentração maior de pontos quentes previstos do que os níveis reais de crime justificariam".[34] Assim, concluem pela necessidade de consideração da "variação nas taxas de notificação ao avaliar os sistemas de policiamento preditivo em relação a potenciais danos e impactos discriminatórios".[35]

A importância deste estudo está justamente em apontar que não há saída fácil para evitar vieses em um sistema que visa operar na área de persecução penal e segurança pública de modo geral. Mesmo não utilizando dados que podem reproduzir eventuais práticas enviesadas da polícia, "as taxas diferenciais de notificação de crimes pelas vítimas podem levar a resultados de predição geograficamente enviesados",[36] considerando que esses dados podem ser impactados por fatores socioeconômicos, demográficos e culturais.

33. AKPINAR, Nil-Jana; DE-ARTEAGA, Maria; CHOULDECHOVA, Alexandra. The effect of differential victim crime reporting on predictive policing systems. In: ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, 2021,Canada (Virtual Event). **Proceedings [...]**. Canada: Association for Computing Machinery, 2021. Disponível em: https://nakpinar.github.io/diff_victim_crime_rep.pdf. Acesso em: 24 ago. 2024

34. *Ibidem.*

35. *Ibidem.*

36. *Ibidem.*

/ A IA ACABA PENALIZANDO NOVAMENTE COMUNIDADES QUE JÁ SÃO HISTORICAMENTE MAIS VIGIADAS PELA POLÍCIA, COMO É O CASO DE COMUNIDADES NEGRAS /

/ A REGULAÇÃO PODE APOIAR ESSE OBJETIVO AO CLASSIFICAR TECNOLOGIAS FALHAS E RACISTAS COMO DE RISCO INACEITÁVEL E AO ADOTAR O ANTIRRACISMO COMO EIXO CENTRAL /

Em termos econômicos mais objetivos, investir em tecnologias como essas, reconhecidamente falhas, inclusive com dados de diferentes origens, não se traduz sequer em uma escolha eficiente. Todavia, o que se tem visto é exatamente o oposto, com o crescimento do interesse em torno de reconhecimento facial e policiamento preditivo no Brasil, o que leva a algumas preocupações em torno de uma regulação para IA no país.[37]

37. MELO, Paulo Victor. A serviço do punitivismo, do policiamento preditivo e do racismo estrutural. **Le Monde Diplomatique Brasil**, 18 mar. 2021. Disponível em: https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/. Acesso em: 31 ago. 2024.

PREOCUPAÇÕES PARA UMA AGENDA REGULATÓRIA EM TORNO DE SISTEMAS INTELIGÊNCIA ARTIFICIAL

Desde 2020, pelo menos, o Brasil tem tido discussões mais intensas acerca da construção de uma regulação para IA. Inicialmente, com o Projeto de Lei 21/2020,[38] o debate estava mais baseado em estabelecer princípios e valores para o uso e desenvolvimento da tecnologia. A partir de 2022, com a ida do PL ao Senado e a criação de uma Comissão de Juristas para a elaboração de um substitutivo, um novo texto foi criado, passando a ser numerado como o Projeto de Lei 2.338 em 2023.[39] Diferentemente da versão anterior, a nova redação trouxe uma regulação baseada em riscos e direitos, isto é, com uma série de garantias e proteções para pessoas afetadas pela IA e a previsão de uma gradação de riscos para a classificação da tecnologia, considerando riscos inaceitáveis e altos, com a adoção de medidas de governança mais rígidas,

38. BRASIL. Câmara dos Deputados. **Projeto de Lei nº 21, de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9063365 Acesso em: 05 jul. 2023.

inspirado nos moldes do *AI Act*, na União Europeia. Apesar de ainda estar em discussão na Comissão Temporária Interna sobre IA (CTIA) no Senado, o que significa que poderá sofrer novas alterações até a aprovação de uma versão final, o cenário atual de segurança pública no Brasil e os exemplos de uso de inteligência artificial para fins de investigação criminal mencionados no capítulo anterior lançam luz sobre algumas preocupações para uma agenda regulatória desses sistemas.

A primeira delas diz respeito ao papel da definição de tecnologias classificadas como de risco inaceitável ou, como o texto do PL 2338/2023 apresenta, de risco excessivo. Tarcízio Silva destaca que a adoção pelo segundo termo, em contraposição ao termo "inaceitável", que é utilizado na regulação da União Europeia, evoca, "pelo léxico, uma suavização da proteção contra os danos algorítmicos que se desdobrou em minúcias do PL",[40] como com a criação de um rol mais restrito de IAs de risco excessivo.

Com efeito, embora coloque sistemas de identificação biométrica à distância, em tempo real e em espaços públicos como uma tecnologia de risco excessivo, a última versão do PL[41] apresenta uma série de exceções que, na prática, acabam por permitir diferentes usos desses sistemas que já vêm sendo implementados por secretarias de segurança pública em todo Brasil. Sua adoção para fins de instrução de inquérito ou processo

39. BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023.** Dispõe sobre o uso da inteligência artificial.. Brasília, DF: Senado Federal, 2023, p. 3. Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=9347622. Acesso em: 05 jul. 2023.

40. SILVA, Tarcízio. Relatórios de avaliação de impacto algorítmico. **Jota Info**, 17 out. 2023. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulando-a-inovacao/relatorios-de-avaliacao-de-impacto-algoritmico. Acesso em: 31 ago. 2024.

41. A versão analisada para fins de elaboração deste artigo foi a complementação de voto apresentada pelo relator, Senador Eduardo Gomes, ao relatório do PL 2338/2023, em 4 de julho de 2024 e que está disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulando-a-inovacao/relatorios-de-avaliacao-de-impacto-algoritmico.

criminal, com autorização judicial; nos casos de flagrante delito de crimes com pena de detenção superior a 2 anos; e para recaptura de réus fugitivos, por exemplo, são algumas das hipóteses que já ampliam sobremaneira sua possibilidade de utilização justamente para casos sensíveis.

No âmbito do policiamento preditivo, a proposta prevê que sistemas de IA criados para as finalidades de estudo analítico de crimes e para fins de investigação de informações que permitam a previsão de ocorrências ou recorrências de infrações reais ou potenciais, com base no perfil de pessoas singulares, estão classificados como sistemas de alto risco. Isto significa que não são proibidos, mas precisam seguir uma série de medidas de transparência e governança específicas, a fim de mitigar seus potenciais danos e impactos negativos. Dentre elas, estão:

> [...] **I – documentação,** no formato adequado à cada agente de IA e à tecnologia usada, do funcionamento do sistema e das decisões envolvidas em sua construção, considerando todas as etapas relevantes no ciclo de vida do sistema;
>
> [...] **V – utilizar dados de treinamento, validação e teste que sejam adequados, representativos**, contendo propriedades estatísticas apropriadas em relação às pessoas afetadas e levando em conta características e elementos específicos do contexto geográfico, comportamental ou funcional no qual o sistema de IA de alto risco será utilizado;
>
> [...] **VI – medidas para mitigar e prevenir vieses discriminatórios e incentivar diversidade nas equipes de desenvolvimento,** bem como políticas de gestão e go-

vernança para promoção da responsabilidade social e sustentável; (...) (grifo nosso).[42]

Tais obrigações são fundamentais para buscar um controle mais efetivo desse tipo de tecnologia, no entanto, em um Estado notadamente marcado pelo racismo em seu sistema penal, como já abordado, mesmo essas medidas parecem insuficientes para evitar vieses discriminatórios raciais que podem resultar, já em primeira instância, na potencialização da criminalização e encarceramento de um segmento específico da população. Segundo Silva, tão ou mais importantes do que os níveis de acurácia da IA, estão "a capacidade dos fornecedores de tecnologia de auditar seus próprios sistemas, a aceitação de taxas de erro, o modo pelo qual os instalam e vendem e, por fim, o modo como compradores governamentais avaliam ou aceitam tais erros".[43]

A implementação cada vez mais acelerada de sistemas de reconhecimento facial em diferentes estados do Brasil é um exemplo disso. Apesar dos estudos alarmantes sobre as taxas de falha da tecnologia sobre o rosto de pessoas negras, a sua operação segue a pleno vapor, como se a possibilidade de detenções equivocadas (sobre um público específico) se assemelhasse a mais um efeito colateral na busca por segurança. Ainda que resultados de sistemas de reconhecimento facial pudessem ser mais acurados, assim como os de policiamento preditivo, é imperioso destacar que se trata de ferramentas que continuarão circunscritas em uma lógica punitivista de segurança pública e policiamento que vê o corpo negro como uma ameaça a ser eliminada.

Assim, "tecnologias algorítmicas e a definição dos limites aceitáveis do que é considerado qualidade e eficiência na inteligência artificial são moldados por tal estado das relações de poder", em um mundo coordenado pela "ordenação necropolítica, que "envolve uma constante transformação dos mecanismos de violência, punição e classificação dos indivíduos pelos poderes hegemônicos herdeiros do colonialismo".[44] É nesse sentido que se esboça uma segunda preocupação regulatória, relacionada à necessidade de uma abordagem capaz de colocar a raça no centro das relações estabelecidas *com* e *através* da tecnologia, de modo a conseguir visibilizar as estruturas que servem somente para a atualização da dominação racial.

Coletivos pretos como AqualtuneLab[45] e Juristas Negras[46] enviaram contribuições para o Senado Federal, em 2022, a fim de informar a elaboração do substitutivo ao marco regulatório de IA no Brasil, contendo a necessidade de o texto trazer expressamente o antirracismo como um de seus princípios e objetivos. Uma vez que o racismo no Brasil não pode ser considerado como uma patologia social ou mero desarranjo institucional, tratando-se, antes disso, do "modo 'normal' com que se constituem as relações políticas, econômicas, jurídicas e até familiares",[47] é necessário atentar-se a ele de forma específica, sob pena de acabar contribuindo para sua perpetuação. Isto

42. BRASIL. Senado Federal. **Complementação de voto ao Relatório ao PL 2338/2023, pelo Senador Eduardo Gomes.** Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9683716&ts=1729495977237. Acesso em: 31 ago. 2024

43. SILVA, Tarcízio. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc São Paulo, 2022, p. 119.

44. *Ibidem.*

45. BARBOSA, Arthur Almeida Menesês et al. **Documento Preto I:** contribuições do AqualtuneLab para o debate sobre regulação de Inteligência Artificial no Brasil. Rio de Janeiro: AqualtuneLab, 2022. Disponível em: https://aqualtunelab.com.br/wp-content/uploads/2022/11/AQUALTUNELAB-DocumentoPreto-A5-V2-web.pdf

46. JURISTAS NEGRAS. **Contribuição JURISTAS NEGRAS**. 10 jun. 2022. Disponível em: legis.senado.leg.br/sdleg-getter/documento/download/2bf6209f-f6eb-4d49-b447-e626e7c55a77. Acesso em: 25 jun. 2023

47. ALMEIDA, Silvio. **O que é racismo estrutural?** Belo Horizonte: Letramento, 2018, p. 38.

significa olhar para os possíveis riscos e impactos negativos da inteligência artificial a partir de uma perspectiva racializada, que não descarta a sua nocividade se esta estiver restrita somente a um grupo social, e que compreende a necessidade de banimento de determinados modelos quando eles servirem apenas como empreendimentos atualizados de subjugação.

Assim como Fanon "proporá a apropriação anticolonial de outras tecnologias sociais introduzidas pelos franceses na Argélia como a medicina, o jornal impresso e, sobretudo, o rádio",[48] é importante que o uso da IA sirva para uma emancipação dos povos, e não para a manutenção da sua subjugação.[49] Nessa senda, Fanon

> analisou de modo visionário o uso de tecnologia de comunicação pelos colonialistas franceses e como revolucionários na luta anticolonial antropofagicizaram dialeticamente esses aparatos e redes eletrônicas de comunicação, no caso da Argélia, o rádio, tomando-os como seus.[50]

Dessa forma, ao invés de importar acriticamente o uso de tecnologias vigilantistas e racistas em nosso sistema penal já precário, a provocação do intelectual negro martinicano chama para uma apropriação da IA que permita a sociedades racialmente estratificadas, como a brasileira, oferecer efetiva oposição a uma abordagem tecnológica colonialista. A regulação pode ajudar para a consecução desse objetivo ao classificar tecnologias falhas e racistas como de risco inaceitável e colocando o antirracismo como eixo condutor, o que permitirá ampliar o espaço para a construção de tecnologias capazes, por exemplo, de olhar para os dados de áreas mais vulnerabilizadas em cidades e indicar a necessidade de maior destinação de recursos para assistência social, saúde e saneamento básico.

48. FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital:** por uma crítica hacker-fanoniana. São Paulo: Raízes da América, 2022, p. 220-221.

49. NASCIMENTO, Abdias. **O quilombismo:** documentos de uma militância pan-africanista. Petrópolis: Editora Vozes, 1980.

50. FAUSTINO, Deivison; LIPPOLD, Walter. *Op. cit.*

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Silvio. O que é racismo estrutural? Belo Horizonte: Letramento, 2018.

AKPINAR, Nil-Jana; DE-ARTEAGA, Maria; CHOULDECHOVA, Alexandra. The effect of differential victim crime reporting on predictive policing systems. In: ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, 2021,Canada (Virtual Event). **Proceedings [...]**. Canada: Association for Computing Machinery, 2021, p. 9. Disponível em: https://nakpinar.github.io/diff_victim_crime_rep.pdf. Acesso em: 24 ago. 2024.

BARBOSA, Arthur Almeida Menesês et al. **Documento Preto I:** contribuições do AqualtuneLab para o debate sobre regulação de Inteligência Artificial no Brasil. Rio de Janeiro: AqualtuneLab, 2022. Disponível em: https://aqualtunelab.com.br/wp-content/uploads/2022/11/AQUALTUNELAB-DocumentoPreto-A5-V2-web.pdf. Acesso em 31 ago. 2024.

BENJAMIN, Ruha. **Race after technology**: abolitionist tools for the New Jim Code. Medford, MA: Polity, 2019.

BRANDÃO, Juliana. Sistema prisional brasileiro e o permanente mercado das carnes mais baratas. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública 2024.** São Paulo: FBSP, 2024.

BRASIL. Senado Federal. **Complementação de voto ao Relatório ao PL 2338/2023, pelo Senador Eduardo Gomes.** Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9683716&ts=1723640844815&rendition_principal=S&disposition=inline. Acesso em: 31 ago. 2024.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: **Conference on fairness, accountability and transparency**. PMLR, 2018. p. 77-91.

DIRETORIA DE ESTUDOS E PESQUISAS DE ACESSO À JUSTIÇA. Relatório consolidado sobre reconhecimento fotográfico em sede policial. Disponível em: https://sistemas.rj.def.br/publico/sarova.ashx/Portal/sarova/imagem-dpge/public/arquivos/consolida%C3%A7%C3%A3o_relat%C3%B3rio_CONDEGE_e_DPERJ_reconhecimento_fotogr%C3%A1fico.pdf. Acesso em: 19 ago. 2024.

FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital:** por uma crítica hacker-fanoniana. São Paulo: Raízes da América, 2022.

FLAUZINA, Ana luiza Pinheiro. **Corpo negro caído no chão:** o sistema penal e projeto genocida do estado penal brasileiro. 2006. 145 p. Dissertação (Mestrado em Direito). Universidade de Brasília, Brasília, DF, 2006. Disponível em: http://www.cddh.org.br/assets/docs/2006_AnaLuizaPinheiroFlauzina.pdf. Acesso em: 19 ago. 2024.

FLAUZINA, Ana; PIRES, Thula. Supremo Tribunal Federal e a naturalização da barbárie. **Revista Direito e Práxis**, Rio de Janeiro, v. 11, n. 2, 2020, pp. 1211-1237. Disponível em: https://www.e-publicacoes.uerj.br/revistaceaju/article/view/50270/33896. Acesso em: 26 ago. 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 18º Anuário Brasileiro de Segurança Pública 2024. São Paulo: FBSP, 2024.

HEAVEN, Will Douglas. Predictive policing algorithms are racist. They need to be dismantled. **MIT Technology Review**, 17 jul. 2020. Disponível em: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/. Acesso em: 28 ago. 2024.

JURISTAS NEGRAS. **Contribuição JURISTAS NEGRAS**. 10 jun. 2022. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/2bf6209f-f6eb-4d49-b447-e626e7c55a77. Acesso em: 25 jun. 2023.

KILOMBA, Grada. **Memórias de plantação:** episódios de racismo cotidiano. Rio de Janeiro: Cobogó, 2019.

KREMER, Bianca. **Direito e tecnologia em perspectiva amefricana**: autonomia, algoritmos e vieses raciais. 2021. Tese (Doutorado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2021.

MARTINS, Cauê. O rosto familiar da violência contra crianças e adolescentes. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública 2024.** São Paulo: FBSP, 2024.

MELO, Paulo Victor. A serviço do punitivismo, do policiamento preditivo e do racismo estrutural. L**e Monde Diplomatique Brasil**, 18 mar. 2021. Disponível em: https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/. Acesso em: 31 ago. 2024.

RAMOS, Silvia et al. **Negro trauma:** racismo e abordagem policial no Rio de Janeiro. Rio de Janeiro: CESeC, 2022. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/02/CESEC_elemento-suspeito_final-3.pdf. Acesso em: 19 ago. 2024.

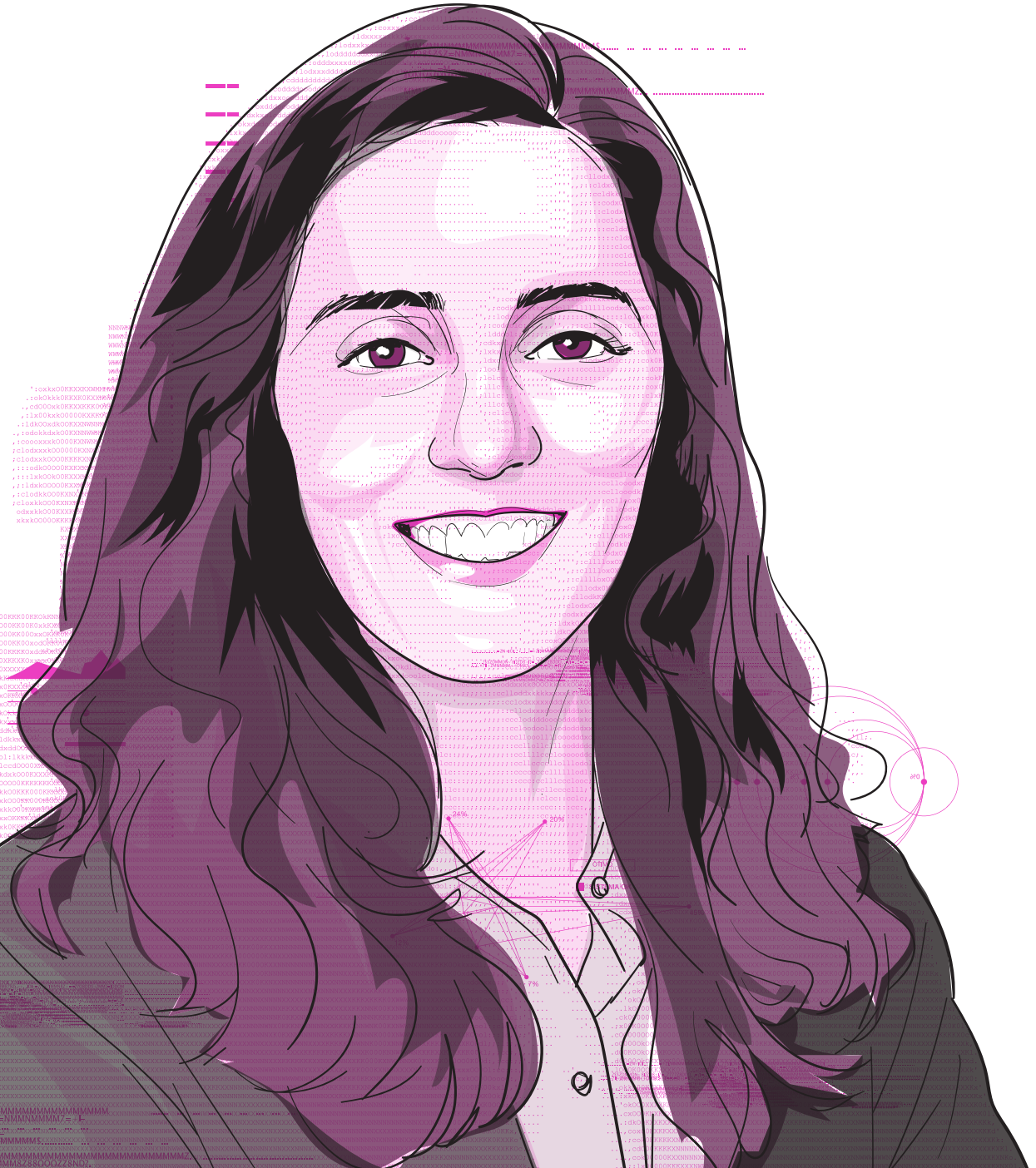
RICHARDSON, Rashida; SCHULTZ, Jason; CRAWFORD, Kate. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. **New York University Law Review**, v. 94, n. 192, maio/2019, pp. 192-233, p. 218. Disponível em: https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf. Acesso em: 28 ago. 2024.

RODRIGUES, Yasmin et al. **Espetacularização da vigilância [livro eletrônico]:** suspeição policial e reconhecimento facial em grandes eventos. Rio de Janeiro: CESeC, 2024.

SANTANA, Igor. Relatórios apontam falhas em prisões após reconhecimento fotográfico. **Defensoria Pública do Estado do Rio de Janeiro**, Notícias, 24 fev. 2021. Disponível em: https://www.defensoria.rj.def.br/noticia/detalhes/11088-Relatorios-apontam-falhas-em-prisoes-apos-reconhecimento-fotografico. Acesso em: 19 ago. 2024.

SILVA, Tarcízio. **Racismo algorítmico:** inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc São Paulo, 2022.

SILVA, Tarcízio. Relatórios de avaliação de impacto algorítmico. Jota Info, 17 out. 2023. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulando-a-inovacao/relatorios-de-avaliacao-de-impacto-algoritmico. Acesso em: 31 ago. 2024.



09.

SISTEMAS PREDITIVOS E "SUSPEITAS": DO COAF ÀS RUAS[1]

Jacqueline Abreu

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Camilly Vitória Silva.

1. INTRODUÇÃO

Dentro do tema proposto para o painel **"O uso de Inteligência Artificial em investigações criminais: do monitoramento por câmeras ao policiamento preditivo",** meu objetivo é tentar contextualizar como essa temática gira em torno da ideia de "suspeita" e "comportamentos suspeitos" – que não são categorias jurídicas formalmente, mas que, na era da inteligência artificial, são noções cujo significado dentro da prática jurídica precisará ser melhor estudado. Então, é por aí que eu vou chegar no debate sobre uso de inteligência artificial em investigações criminais. No início, vou levantar algumas considerações teóricas e, ao final, aspectos práticos que não se pode perder de vista.

2. SISTEMA PREDITIVO DO COAF

Para introduzir esse assunto, eu gostaria de começar falando do COAF, o Conselho de Controle de Atividades Financeiras. O COAF é um órgão que recebe informações de diversas instituições que atuam no mercado financeiro – bancos, corretoras, cartórios, joalherias (referidas no art. 9, Lei nº 9.613/1998) – sobre operações que possam parecer "suspeitas".[2] Suspeita porque é incompatível com a atividade econômica de uma pessoa ou, de maneira mais geral, porque passa um certo valor estabelecido em norma e envolve dinheiro em espécie. Confira-se os principais dispositivos da Lei dos Crimes de Lavagem de Dinheiro que tratam disso:

2. Vide Lei 9.613/1998 (Lei dos Crimes de Lavagem de Dinheiro), art. 11.

> Art. 10. As pessoas referidas no art. 9º: (...)
>
> < II > manterão registro de toda transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ativos virtuais, ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar limite fixado pela autoridade competente e nos termos de instruções por esta expedidas;
>
> Art. 11. As pessoas referidas no art. 9º:
>
> < I > dispensarão especial atenção às operações que, nos termos de instruções emanadas das autoridades competentes, possam constituir-se em sérios indícios dos crimes previstos nesta Lei, ou com eles relacionar-se;
>
> < II > deverão comunicar ao Coaf, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização:
>
> < A > de todas as transações referidas no inciso II do art. 10, acompanhadas da identificação de que trata o inciso I do mencionado artigo;
>
> < B > das operações referidas no inciso I;

A partir dessas incontáveis comunicações que recebe o COAF, ele pode produzir um relatório de inteligência financeira que pode ser então disponibilizado para autoridades encarregadas de fazer investigação criminal ou fiscal, como o Ministério Público e a Receita Federal.

O que esse órgão faz, então, é buscar dar visibilidade a um tipo de crime bastante específico, que poderia passar sem investigação alguma se não tivesse esse tipo de estrutura de monitoramento, como é o caso de lavagem de dinheiro, financiamento de terrorismo. Isso porque lavagem de dinheiro não

é um crime que deixa evidências expostas, que as pessoas de fora podem ver, que a polícia se depara na rua. E nisso é bastante diferente, em geral, de um roubo, de um homicídio.

Naturalmente, o COAF recebe uma quantidade enorme dessas comunicações e não necessariamente sobre todas elas vai efetivamente ter algo estranho sobre o qual eles tenham que efetivamente produzir um relatório e informar as autoridades. O que vai determinar qual operação financeira vai ser fichada no relatório e informada é uma combinação de fatores que compõem uma certa classificação de risco e prioridade que eles tenham estabelecido e que eles fazem por meio de um software de inteligência artificial.

Segundo o COAF,[3] as comunicações são submetidas inicialmente a uma "análise sistêmica", a qual é feita "a partir da identificação de fatos e fenômenos específicos que, em princípio, não apresentam riscos potenciais" de constituírem crime por meio de "regras simples de seleção previamente definidas". Com elas, faz-se diferimento automático – excluindo-se de maior análise aquilo que não apresenta "detalhamento mínimo de atipicidade". Por outro lado, a partir de modelo preditivo de análise, são emitidos alertas baseados "na probabilidade de a comunicação recebida conter elementos de risco". Um analista do COAF vai analisar por uma matriz de risco e ver se é o caso de produzir um RIF, um Relatório de Inteligência Financeira a ser disseminado para autoridades para instauração dos procedimentos cabíveis (art. 15, Lei 9.613/1998) quando concluir pela existência de crime ou fundados indícios de sua prática.

3. Confira-se exemplar de relatório de atividades do COAF, com a explicação respectiva sobre tal funcionamento à página 27: Conselho de Controle de Atividades Financeiras. Relatório Integrado de Gestão. 2023. Disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/rig-coaf-2023.pdf . As citações diretas contidas em tal parágrafo se referem a trechos de tal explicação.

Esse era o meu mote inicial dessa conversa e o ponto que eu queria chegar é que nós temos no COAF um tipo de policiamento preditivo. Ele se aplica a crimes bastante específicos (lavagem de dinheiro, financiamento ao terrorismo), que têm pouca visibilidade, e isso é a parte fundamental da justificativa pública desse tipo de monitoramento e controle. Ele gera e opera com vários tipos e níveis de alertas e suspeitas.

Primeiro, as entidades reguladas fazem o monitoramento daquilo que é "estranho"/"suspeito", a partir de certos critérios fixados em lei e aí ela manda para o COAF e lá também passa por um outro tipo de análise interna, de inteligência artificial, que gera um outro tipo de alerta. Então o analista olha, faz uma triagem e é repassado às autoridades, quando eles acham que efetivamente tem algo estranho. Claro, não necessariamente aquilo vai ser evidência e prova de um crime. Suspeitas sempre carregam consigo um nível de dúvida, uma incerteza, uma possibilidade de que aquilo não é o que está aparecendo.

3. SISTEMAS PREDITIVOS EM ESPAÇOS PÚBLICOS

Voltando a atenção para *ruas*, a gente vai para o monitoramento por câmeras de áreas públicas de uma cidade, que normalmente são implementadas para combate de furtos, roubos, tráfico de drogas e talvez também um ou outro homicídio.

O policiamento preditivo do qual a gente está falando quando a gente está pensando nesse tipo de monitoramento por câmeras em público pode servir - um pouco óbvio aqui nessa conversa - para identificar padrões de áreas, quadras, esquinas, em que pode haver mais incidência de crime, para identificar também quais tipos de comportamentos suspeitos estão envolvidos nesse tipo de crime e gerar alertas sobre eles.

Então é um software que vai prever onde pode acontecer mais crime, onde há mais oportunidade para que certos tipos de crime aconteçam e também que tipos de comportamentos são associados e antecedem esse tipo de fato criminoso. Para que isso, então, enseje um alerta nas polícias.

4. FUNDADA SUSPEITA E AÇÃO POLICIAL

Esses pontos me levam a uma observação sobre o que constituem "suspeitas" no nosso processo penal e que tipo de noção é essa. A gente se aproxima dessa noção de "suspeita" para representar um certo tipo de padrão probatório que vai permitir ao Estado mobilizar a força de maneira específica contra uma pessoa. Um elemento, então, a partir do qual você começa a gerar uma justificação, uma autorização do Estado para um tratamento distinto de certas pessoas comparada aos demais. E isso inclusive, eventualmente, vai poder gerar uma restrição da sua liberdade.

Apesar da importância desse tipo de conceito como um gatilho do processo penal, não é um conceito muito bem elaborado. No Código de Processo Penal (CPP), fala-se em "fundada suspeita", e em fundada suspeita de um certo tipo específico – de porte de material de corpo de delito (art. 240, 2º, e 244, CPP), como um requisito para que uma busca pessoal seja autorizada. Ou seja, para uma busca pessoal, para uma abordagem e como requisito também para confirmação de uma prisão em flagrante.

Por outro lado, o CPP diz muito pouco sobre o que efetivamente constitui uma "fundada suspeita". O que é que precisa ter sido verificado na prática, no mundo dos fatos, para que um comportamento configure uma fundada suspeita? Por isso mesmo, há muita discussão ainda genérica no Brasil sobre atitudes suspeitas e muita discussão na jurisprudência sobre o

/ SUSPEITAS SEMPRE CARREGAM CONSIGO UM NÍVEL DE DÚVIDA, UMA INCERTEZA, UMA POSSIBILIDADE DE QUE AQUILO NÃO É O QUE ESTÁ APARECENDO /

que isso pode significar ou não, e de como isso permite abusos e discricionariedade policial.

O Superior Tribunal de Justiça tem proferido decisões que vêm impactando a prática policial para trazer um pouco mais de parametrização sobre esse assunto. Eles já consideraram recentemente, por exemplo, que o policial simplesmente dizer que verificou um certo nervosismo na pessoa não é um gatilho suficiente para que aquilo autorize uma busca. Nem o fato de que a pessoa foi encontrada ou estava passando por uma área de venda de drogas é uma razão suficiente para parar essa pessoa e para fazer uma revista (Informativo STJ 732 de 2022, referência ao REsp 1.961.459-SP).

5. O FUTURO DOS SISTEMAS DE PREDIÇÃO

Como é que a gente transporta esses elementos para as discussões de policiamento preditivo e monitoramento por câmeras? Primeiro que sempre que alguém falar em policiamento preditivo, a gente tem que parar e olhar o que é que esse sistema está propondo e identificando como anormal. Qual é o *red flag* que ele gera? O que é que está gerando o alerta do que seria suspeito para aquele sistema?

Hoje, muitos desses alertas são baseados na experiência policial, na experiência que você conseguiria ouvir de um policial falando: "Duas pessoas andando em cima de uma moto, ou uma pessoa que para ao lado de um carro no meio de duas faixas". Elementos como esses vêm sendo embutidos em sistemas eletrônicos para ganhar escala.

Mas o futuro efetivamente do policiamento preditivo - pelo menos o que a gente vê na literatura hoje - é muito mais do que isso. É querer extrair ao máximo os benefícios de *Big Data* da inteligência artificial para extrair correlações estatísticas de comportamentos que hoje escapam completamente aos olhos humanos. É ser capaz de identificar novos tipos de suspeitas que nós, humanos, não efetivamente seremos capazes de explicar e de justificar. Um sistema, por exemplo, que vai poder adivinhar quais carros têm 80% de chance de estar carregando drogas e a gente não saber efetivamente qual a razão disso, a partir de um infinito cruzamento de dados.

O Direito admitirá isso? E a partir de que termos? É por isso que eu disse que esses sistemas vão ter que nos confrontar finalmente a refletir com profundidade sobre essa categoria jurídica do que é "suspeita", sobre o papel dela, o que autoriza efetivamente, enquanto comportamento "anormal", o Estado agir nessas situações. Neste evento também se falou de protocolos operacionais padrão. A gente vai ter que começar a pensar nisso também toda vez que tiver alguém se engajando nesse tipo de aplicação de policiamento preditivo: o que é exatamente que você está fazendo? O que é que o sistema te alerta? E o que o policial tem que verificar depois e antes daquilo efetivamente poder gerar uma ação policial? E discutir se a gente vai querer que aquilo mesmo seja suficiente para autorizar uma ação policial.

Hoje, como eu falei, o que a gente tem ainda é bastante diferente disso. É algo que dá apoio a ações policiais, que sinaliza *hotspots*, áreas quentes de tráfico de droga, sinaliza se alguém está passando por uma área. Mas a gente já tem, mesmo nesses elementos ainda básicos, alguns elementos fundamentais que a própria jurisprudência do STJ já está colocando em questão. A gente não vai poder, apenas pela existência de sistemas que nos avisem sobre isso, autorizar que a polícia aja imediatamente sobre essas ações.

6. ASPECTOS PRÁTICOS DOS SISTEMAS DE PREDIÇÃO

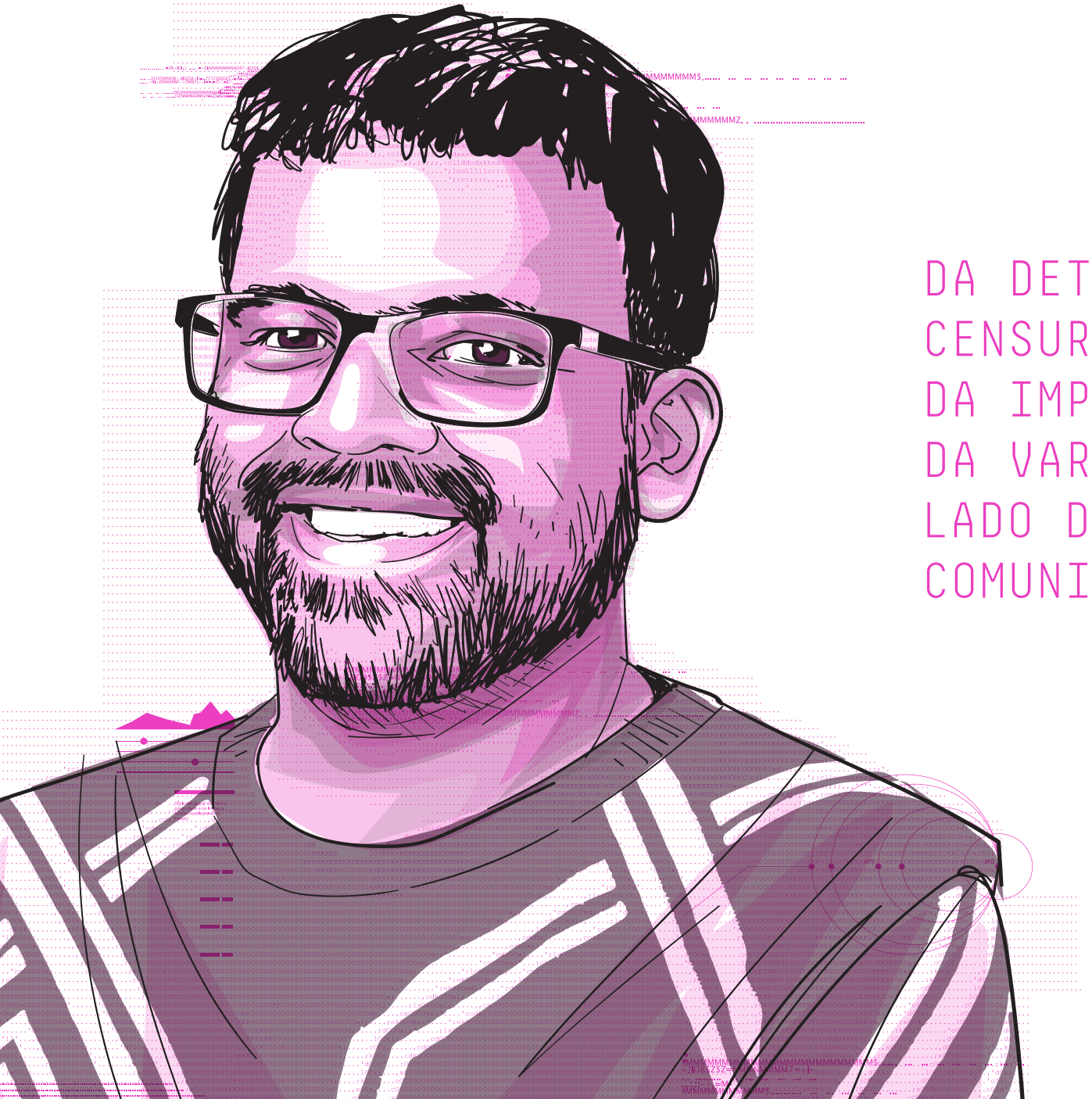
Agora que eu levantei essa discussão mais teórica e dogmática sobre essa categoria jurídica vou passar para alguns aspectos mais práticos e apontar duas diferenças do policiamento preditivo que eu comecei falando que seria do COAF, que é previsto em lei, regulado e que teve inclusive a sua constitucionalidade reconhecida pelo STF, com as propostas e debates hoje sobre policiamento preditivo atrelado a monitoramento público por câmeras nas ruas. São aspectos, como eu falei, mais de ordem prática.

Primeiro, quando se trata de câmeras nas ruas e policiamento preditivo em cima disso, não se trata de crimes que têm um problema de visibilidade, como o que o COAF monitora hoje. Sem câmeras, não significa que furtos, roubos, homicídios não serão notificados, denunciados ou ficarão sem investigação. Não existe, portanto, aqui um problema prévio que o policiamento preditivo, ou o monitoramento, vai ajudar necessariamente. Pelo contrário, são crimes que podem ser investigados por meios tradicionais de investigação.

Neste ponto, quando você vê relatos de cientistas sociais, de cientistas políticos que estudam polícia, normalmente o que se vê é que normalmente são empresas que lá atrás mais se aproximaram das polícias e venderam sistemas de policiamento preditivo e de câmeras como soluções para eles, mas não que necessariamente eles já tinham isso como pautas sobre o que precisava ser feito para aperfeiçoar o trabalho policial. É claro que também num país como o Brasil, que tem muitos problemas, um sentimento de insegurança muito forte, isso acaba tendo um apelo também, as pessoas querem que seja a resposta que gere mais sensação de segurança. No final das contas, a adoção desse tipo de tecnologia é uma escolha política, que está sendo escolhida em detrimento de outros programas sociais, de assistência social, educação, esportes que poderiam ter talvez um impacto muito maior para a redução desse tipo de crime de oportunidade que acontece nas ruas hoje.

Por fim, minha segunda preocupação prática, é a preocupação com como se dá o treinamento desses sistemas de alerta, a retroalimentação que os dados e esses sistemas geram. O COAF hoje recebe comunicações de operações suspeitas, em tese, de uma amostragem que é muito grande, do Brasil inteiro. Tudo que passa pelo sistema financeiro, vai pra lá, em tese, porque uma lei obriga todas as instituições formais, de certa maneira, que operam no mercado a fazerem isso. Como o COAF funciona realmente é um *black box*. Hoje, se você for ler um acórdão de 500 páginas do STF sobre o Coaf (referência ao RE 1.055.941, julgado em 2019) ou seu relatório de atividades, você não tem informação efetivamente de como é esse sistema de alertas, exemplos concretos do que constitui uma "suspeita" suficiente para virar um RIF. Então, há muito desenvolvimento de transparência que precisa acontecer também sobre o COAF.

Mas se você joga para as ruas e para câmeras, me parece que o problema aqui é ainda maior, e não só, é ainda um tipo de adoção que é sempre seletiva, se dá por cidade e cidade, região ou região, e sempre uma área ou outra. O que gera um problema de locais hiper vigiados, sem se levar em consideração que isso pode afetar também um problema de retroalimentação e de hipervigilância que não leva em conta a própria distribuição da população em termos de condição socioeconômica e raça na cidade, de modo que se afeta mais uma pessoa, mais um certo grupo de pessoas do que outro. Essa observação reforça a necessidade de se pensar os critérios e parâmetros de alertas e suspeitas em sistemas preditivos, que são ainda mais complexos nas ruas.



10.

DA DETECÇÃO À CENSURA: OS PERIGOS DA IMPLEMENTAÇÃO DA VARREDURA PELO LADO DO CLIENTE EM COMUNICAÇÕES PRIVADAS[1]

Udbhav Tiwari

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Anna Martha Cintra Araújo e traduzido do inglês para o português por Flora Mello Gallina.

Obrigado pelo convite. É um prazer estar aqui para discutir a varredura pelo lado do cliente (*client-side scanning*). Antes de entrar em minhas observações, gostaria de esclarecer que meus comentários se concentrarão em três áreas principais:

Primeiro, descreverei brevemente a natureza das tecnologias de varredura pelo lado do cliente e estabelecerei alguns contornos a respeito do que elas abrangem e não abrangem. Isso inclui tanto as formas com que algumas plataformas de tecnologia utilizam essas ferramentas atualmente e as distinções entre esses usos, quanto a forma com que os governos preveem que sejam implementadas. Abordarei os aspectos técnicos de como essas tecnologias funcionam, ou de como elas falham, mas tentarei manter essa discussão em um patamar mais alto, evitando uma profundidade técnica desnecessária e concentrando-me apenas no que é essencial para sua compreensão.

Em seguida, abordarei as preocupações baseadas em princípios em relação à implementação da varredura do lado do cliente. Especificamente, explorarei os riscos que ela representa para os marcos legais e para as normas democráticas, e destacarei as preocupações dela decorrentes.

Por fim, examinarei os desafios práticos da implementação de tecnologias de varredura do lado do cliente. Discutirei questões que podem surgir mesmo se assumirmos a boa-fé de todos os atores envolvidos – tanto plataformas quanto governos – e explorarei os problemas adicionais que podem emergir se os responsáveis pela implementação e regulamentação dessas tecnologias não tiverem em mente o interesse dos usuários. Tudo isso será considerado sob um guarda-chuva de considerações práticas.

A NATUREZA DA VARREDURA PELO LADO DO CLIENTE

Para iniciar, vamos discutir a natureza das tecnologias de varredura do lado do cliente. Um exemplo familiar é uma proposta da Apple feita há cerca de dois anos e meio. A Apple sugeriu uma função para dispositivos iOS que detectaria imagens de abuso sexual infantil (ASI) (*Child Sexual Abuse*, ou CSA) antes de serem carregadas em seus servidores. Muitos de vocês devem se lembrar da significativa reação pública a essa ideia, pois ela envolvia a varredura de imagens nos dispositivos dos usuários. Se um determinado limiar de conteúdo ASI fosse detectado, a Apple o denunciaria às autoridades. Essa proposta gerou uma oposição generalizada da sociedade civil e de especialistas acadêmicos em todo o mundo, resultando no abandono da função pela Apple. Atualmente, a Apple já implementa uma forma de tecnologia de varredura do lado do cliente, que discutirei em breve, mas não o denuncia às autoridades policiais, nem se concentra na detecção de imagens de ASI - dois componentes centrais da proposta original.

Desde então, vários governos em todo o mundo propuseram o uso de tecnologias de varredura do lado do cliente (VLC) em diferentes leis e regulações. O Reino Unido, por exemplo, está considerando o VLC em sua Lei de Segurança Online (*Online Safety Bill*), enquanto a União Europeia está explorando sua implementação como parte da Diretiva de Materiais de Abuso Sexual Infantil (*Child Sexual Abuse Materials Directive*). Alguns países, como a Índia, já contam com leis que, embora não exijam explicitamente a varredura do lado do cliente, impõem obrigações de rastreabilidade, o que poderia facilitar seu uso. Relatórios públicos também sugerem que os

governos solicitaram às plataformas que considerassem a implementação de tecnologias de VLC para atender a requisitos legais. Claramente, o conceito de varredura do lado do cliente está ganhando força rapidamente, com muitos governos vendo-o como uma solução para os desafios impostos pelos sistemas criptografados.

Varredura do lado do cliente significa essencialmente a varredura do conteúdo antes de ele ser criptografado e carregado nos servidores de um serviço. Na prática, por exemplo, se você enviar uma imagem para o WhatsApp ou para o Signal, que são plataformas criptografadas de ponta-a-ponta, a criptografia será realizada no seu dispositivo, e apenas o dispositivo do destinatário poderá descriptografar o conteúdo. A varredura do lado do cliente tenta analisar esse conteúdo antes da criptografia, permitindo que plataformas ou outras entidades determinem se ele está em conformidade com os padrões legais ou com as políticas da plataforma.

Já existem exemplos que se assemelham à varredura do lado do cliente. Por exemplo, se você tentar enviar um link com pequenas modificações de caracteres (como "goógle.com", em vez de "google.com") no WhatsApp, você notará que o link não é clicável. Isso sugere que o WhatsApp verifica o conteúdo antes da criptografia, para evitar *phishing*. Os governos argumentam que, se as plataformas podem verificar textos em busca de fraude ou *phishing*, elas deveriam ser capazes de escanear conteúdo ilegal, como imagens de ASI. No entanto, é essencial distinguir entre a varredura regex básica, que detecta padrões suspeitos no texto, e a varredura do lado do cliente. Quando essa varredura ocorre em um dispositivo, não há um banco de dados com o qual o conteúdo possa ser comparado. Em vez disso, o sistema procura padrões de caracteres específicos. Se esses padrões forem detectados, o sistema não sinaliza auto-

/ VARREDURA DO LADO DO CLIENTE SIGNIFICA ESSENCIALMENTE A VARREDURA DO CONTEÚDO ANTES DE ELE SER CRIPTOGRAFADO /

/ DISPOSITIVOS ELETRÔNICOS PESSOAIS SÃO ESSENCIALMENTE ESPAÇOS PRIVADOS [...] A VARREDURA [...] AMEAÇA VIOLAR ESSA PRIVACIDADE /

maticamente o conteúdo, não o denuncia a um indivíduo ou a uma agência governamental, nem impede que o usuário o envie, mas identifica se estão presentes características comumente associadas a mensagens fraudulentas. Mesmo que esses padrões sejam encontrados, o usuário consegue enviar a mensagem, embora o sistema possa fazer pequenos ajustes, como emitir um aviso de que o link pode ser suspeito, como faz o WhatsApp. Alternativamente, o sistema pode impedir que o link seja clicável, requerendo que o usuário o copie e cole em um navegador antes de prosseguir. A varredura básica de regex não envolve a comparação de conteúdos com um banco de dados de material ilegal. Antes, ele verifica se há irregularidades, como caracteres fraudulentos, sem denunciar o conteúdo ou impedir sua transmissão.

A varredura do lado do cliente é muito mais invasiva. Tomemos o exemplo anterior da Apple: o modelo contava com inteligência artificial e aprendizado de máquina para verificar imagens, vídeos e textos nos dispositivos dos usuários para detectar materiais de ASI. Organizações como o *National Center for Missing & Exploited Children* (NCMEC) mantêm bancos de dados de *hashes*, representações alfanuméricas de conteúdo ilegal conhecido. As plataformas usam esses bancos de dados para comparar conteúdos e, se uma correspondência for encontrada, denunciá-la às autoridades. Atualmente, esse processo acontece no lado do servidor, mas a varredura do lado do cliente deslocaria todo esse processo para os dispositivos dos usuários. Por exemplo – embora seja algo que ninguém deva fazer –, se você pegasse hoje uma imagem de ASI conhecida e a enviasse por Gmail, pelo bate-papo sem criptografia de ponta-a-ponta do Facebook Messenger ou por SMS, por meio de sua operadora de telefone, haveria uma grande probabilidade de você ser pego. Isso acontece porque as plataformas comparam o material

que você envia ao banco de dados de *hash* mantido por organizações como o NCMEC. Se uma correspondência for encontrada, a plataforma a relata ao governo e aos órgãos de aplicação da lei, permitindo que eles tomem as medidas cabíveis.

Resumindo essa parte da intervenção, a varredura do lado do cliente espelha o processo tradicionalmente feito em servidores, mas ocorre em dispositivos particulares, como smartphones e tablets. O problema com isso é profundo. Essencialmente, dá aos dispositivos a capacidade de monitorar e censurar os conteúdos antes de serem compartilhados, carregados ou distribuídos por meio de um canal/plataforma. Imagine um governo instalando uma câmera sobre sua caneta, monitorando tudo o que você escreve e alertando automaticamente as autoridades se o que você escrever for considerado ilegal. Essa hipótese fantástica, mas distópica, resume por que a varredura do lado do cliente é uma tecnologia tão preocupante. Ela permite que governos e plataformas monitorem pensamentos e expressões – mesmo que legais – antes de serem comunicados, levantando questões significativas sobre privacidade e liberdade de expressão. Mesmo que não seja essa a intenção atual das propostas de lei para o uso da tecnologia, uma vez que o potencial exista, será apenas uma questão de tempo e de oportunidade política até que o aumento de escopo evolua para uma polícia do pensamento permanentemente ativada.

PREOCUPAÇÕES BASEADAS EM PRINCÍPIOS NA IMPLEMENTAÇÃO DA VARREDURA DO LADO DO CLIENTE

Passando para o segundo dos meus três pontos, vamos nos concentrar na oposição baseada em princípios à implementação de tecnologias de varredura do lado do cliente. Como sugeri anteriormente, a questão fundamental que devemos nos fazer como democracias e como sociedade é: queremos conceder aos governos o poder de determinar o uso de tecnologias que escaneiem pensamentos e emoções antes que eles sejam expressos? Se essa ideia nos deixa desconfortáveis, devemos nos sentir igualmente, se não mais, desconfortáveis com a varredura do lado do cliente.

A principal preocupação é a ladeira escorregadia que isso introduz. Hoje, as tecnologias de varredura do lado do cliente são amplamente propostas para dois tipos de conteúdo: (I) materiais de abuso sexual infantil (ASI) e (II) conteúdo extremista, particularmente de indivíduos ou organizações designadas como terroristas. Essas categorias são vistas como excepcionais devido aos sólidos quadros legais que as cercam. No entanto, é importante observar que, mesmo hoje, nenhum país exige proativamente a varredura de conteúdos de ASI. Quando plataformas como a Google, a Apple ou o Facebook procuram por esse tipo de conteúdo, é por conta de um consenso social de que esses materiais não deveriam existir em seus sistemas. Fundamentalmente, essa varredura acontece em conteúdo não criptografado - conteúdo que é descriptografado pela plataforma para que ela possa processá-lo. É por isso que, por exemplo, a Google pode escanear o Gmail para veicular anúncios com base no conteúdo do e-mail, ou que o Facebook pode detectar nudez em imagens carregadas como atualizações de status.

Mas imaginem se essas mesmas tecnologias fossem estendidas por força/ordem legal para censurar discursos críticos ao governo, material protegido por direitos autorais, ou conteúdo classificado como discurso de ódio ou criminalizado por governos. Essa é a essência da ladeira escorregadia: uma

vez que a tecnologia existe e está implementada, o potencial de uso indevido se torna uma ameaça real. O princípio fundamental é que os governos não devem ser capazes de exigir tecnologias que verificam conteúdos pessoais antes de serem criados ou compartilhados. Uma vez que essa barreira é ultrapassada, torna-se um desafio impedir que os governos expandam o uso dessas tecnologias para seus próprios fins.

Considerem a diferença entre receber uma notificação do seu provedor de Internet alertando sobre o download de torrents ilegais, e a Microsoft relatar ao governo local que você pirateou conteúdo em seu disco rígido. O primeiro parece ter um equilíbrio razoável entre a garantia de direitos autorais e a privacidade individual. O último, no entanto, introduz uma realidade distópica em que os governos têm acesso aos seus arquivos privados, mesmo antes de você compartilhá-los. É comparável a ter uma câmera instalada dentro de sua casa, monitorando cada movimento e denunciando atividades suspeitas às autoridades.

Seus dispositivos eletrônicos pessoais são essencialmente espaços privados. No entanto, a varredura do lado do cliente ameaça violar essa privacidade. Uma vez que os governos tenham a capacidade de exigir a tecnologia de varredura em dispositivos pessoais, ela poderá ser usada globalmente como arma para diversos propósitos. As implicações não se limitam a apenas um país ou a alguns regimes autoritários – qualquer país poderia seguir um caminho diferente, do Brasil à Índia e ao Reino Unido.

Isso nos leva a uma das críticas mais duras contra a tecnologia de varredura do lado do cliente proposta pela Apple. Os dispositivos da Apple são amplamente usados na China, e os críticos levantaram a preocupação de que, se o governo chinês ordenasse que a Apple procurasse por termos específicos, como "Praça da Paz Celestial", a Apple enfrentaria uma intensa pressão para acatar. Embora a Apple tenha inicialmente prometido usar a tecnologia apenas para conteúdos de ASI, os críticos questionaram como a empresa resistiria a demandas do governo para ampliar a tecnologia para outros fins, como censura política. A Apple não ofereceu uma resposta convincente a esse dilema.

Esse cenário resume o problema de princípio central com a varredura do lado do cliente. Se nós, como sociedade, valorizamos os espaços privados, o pensamento privado e a distinção entre comunicação pessoal e pública, devemos nos opor à implantação de tecnologias de varredura do lado do cliente. Uma vez que esses recursos existam, eles serão difíceis de controlar e restringir, e os riscos de uso indevido se multiplicarão. Embora possa parecer que essas tecnologias ficarão restritas a dispositivos móveis, não há razão para que não possam se estender a outros dispositivos, como computadores de trabalho e laptops, ampliando ainda mais a ameaça à privacidade e à liberdade pessoal.

IMPLICAÇÕES PRÁTICAS DA IMPLANTAÇÃO DE TECNOLOGIAS DE VARREDURA DO LADO DO CLIENTE

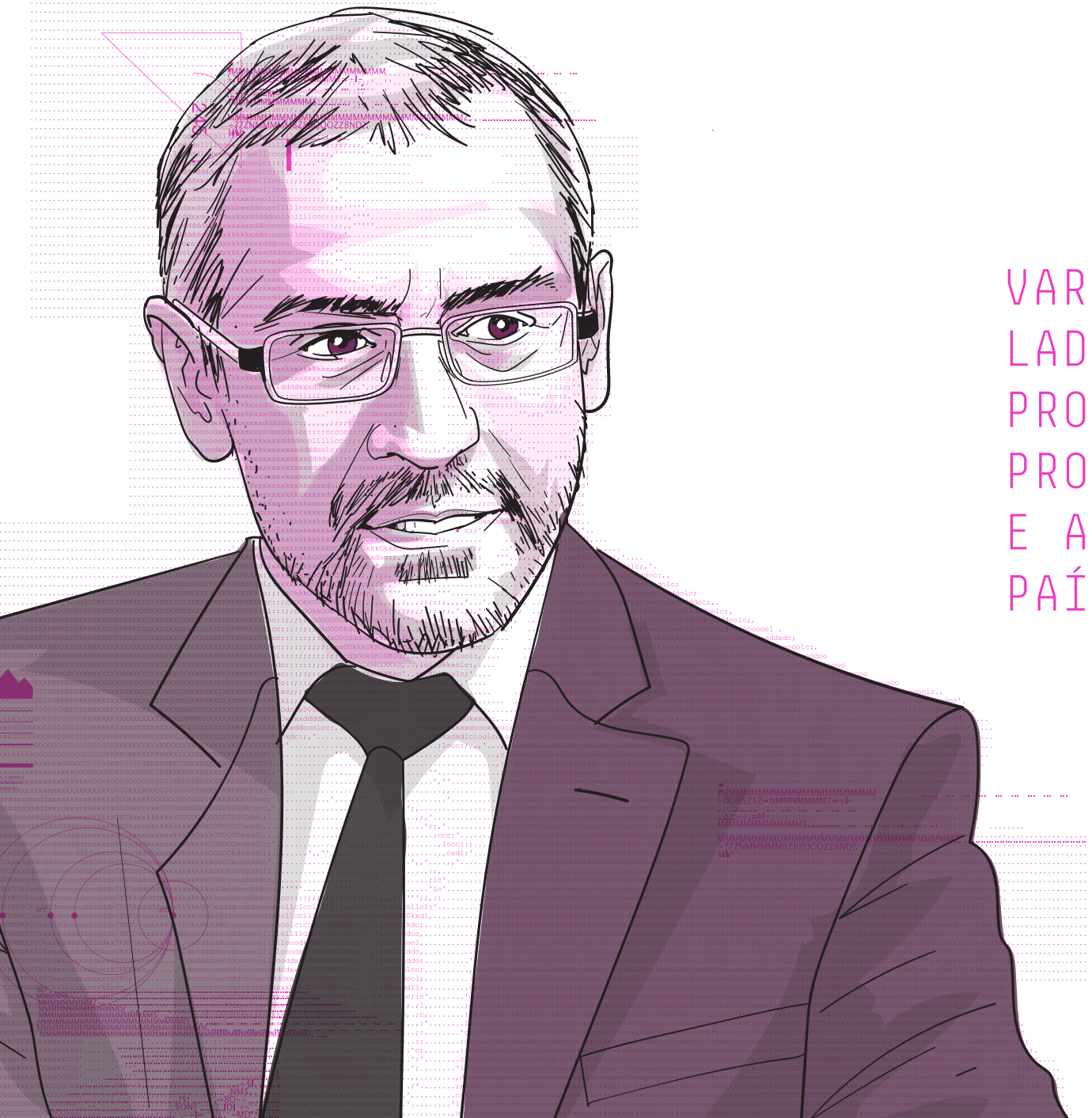
Com isso, vou agora me dirigir ao último ponto: as implicações práticas da implantação de tecnologias de varredura do lado do cliente, e por que elas são igualmente problemáticas.

A primeira, e talvez mais significativa, questão com a implantação dessas tecnologias é que a inteligência artificial e o aprendizado de máquina ainda não são capazes de realizar essa tarefa de forma confiável. Análises extensas de diversos modelos usados por plataformas como o Facebook

para detectar discurso de ódio ou por provedores que usam o PhotoDNA da Microsoft para identificar materiais de abuso sexual infantil (ASI) mostraram sérias lacunas. Esses sistemas frequentemente falham de duas formas fundamentais: eles permitem que os materiais de ASI passem despercebidos, especialmente conteúdo novo ou anteriormente desconhecido, e sinalizam erroneamente materiais legítimos como nocivos. Um caso amplamente divulgado de dois anos atrás ilustra esse problema: um homem enviou fotos de seu bebê em uma banheira para amigos, e essas imagens foram sinalizadas como conteúdo de ASI. Como resultado, a polícia o investigou e, apesar de provar que as fotos eram inocentes, sua vida virou de cabeça para baixo por mais de dois anos. Isso destaca um ponto-chave: esses sistemas estão longe de ser perfeitos e seus erros podem ter consequências devastadoras.

Diante disso, é importante reconhecer que essa tecnologia ainda não é confiável, e isso me leva à questão dos sistemas contraditórios. Imaginem uma situação em que alguém possa desencadear uma investigação contra você simplesmente enviando a você conteúdo ilegal. Tudo o que precisariam fazer seria enviar materiais extremistas ou de ASI para o seu telefone ou computador, talvez até escondê-los em uma pasta que você raramente abre. Uma vez que esse conteúdo fosse verificado pelo seu dispositivo, você poderia ser denunciado automaticamente às autoridades, completamente inconsciente dele até que fosse tarde demais. Esses sistemas não conseguem diferenciar ações maliciosas de adversários e recebimento inadvertido de materiais nocivos, tornando perigosamente fácil para que maus atores os transformem em armas.

Esses são apenas alguns dos desafios práticos com a implementação de sistemas de varredura do lado do cliente, embora muitos outros estejam bem documentados. Em resumo, expliquei o que são as tecnologias de varredura do lado do cliente, por que elas são problemáticas, as preocupações baseadas em princípios relacionados à sua existência em uma sociedade democrática e as maneiras práticas pelas quais sua implementação pode dar desastrosamente errado. É por esses motivos que, neste momento, essas tecnologias não devem ser implementadas – elas simplesmente não estão prontas para cumprir as funções que os governos estão esperando delas.



11.

VARREDURA PELO LADO DO CLIENTE, PROPORCIONALIDADE E PROTEÇÃO DE CRIANÇAS E ADOLESCENTES NO PAÍS DO ESTUPRO

Valdemar Latance Neto

A legislação dos Estados Unidos obriga empresas de tecnologia a reportar ao NCMEC[1] os usuários de seus serviços que possuam arquivos contendo abuso sexual infantojuvenil.[2] Se o reportado estiver no Brasil, o destino do relatório com os dados é a Polícia Federal, que compila as informações, analisa-as e realiza operações policiais com a finalidade de identificar e resgatar crianças e adolescentes, vítimas de abuso sexual, e de responsabilizar penalmente os abusadores.

Estudo do Instituto de Referência em Internet e Sociedade[3] utilizou método revisão da literatura, em uma análise que abarcou "22 publicações selecionadas"[4] para tratar de supostas violações à privacidade pela tecnologia de comparação de *hashes* e pela obrigatoriedade legal de reportar ao NCMEC.

Embora o texto acadêmico registre ter feito uma "revisão extensiva" de "repercussões sociais, jurídicas e políticas"[5] do uso dessa tecnologia, dele não consta uma vez sequer o nome da instituição que recebe esses relatórios no Brasil. Não há uma linha sobre as milhares operações policiais que a Polícia Federal realiza com base nessas informações, nem as suas repercussões sociais. A despeito dessa omissão, o estudo afirma peremptoriamente que a tecnologia configura "medida inadequada até mesmo para o objetivo de enfrentar a pornografia infantil".[6]

1. NCMEC. National Center for Missing & Exploited Children. Disponível em: https://www.missingkids.org/home. Acesso em: 30 maio 2024.

2. A expressão "pornografia infantil" será evitada no texto por configurar um eufemismo que suaviza exageradamente a dura ofensa às crianças e adolescentes que aparecem nos vídeos e fotos. Pornografia embute a ideia de consentimento e de entretenimento. Não há consentimento em sexo com crianças e o nome jurídico disso é estupro de vulnerável. Na Polícia Federal, prefere-se genericamente a expressão abuso sexual de crianças e adolescentes, em harmonia com recomendações internacionais.

3. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Varredura pelo lado do cliente: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/.

4. *Ibidem*, p. 5

5. *Ibidem*, p. 26

6. *Ibidem*, p. 6.

Equivoca-se absolutamente, como mostram os resultados do trabalho da Polícia Federal dos últimos anos, na apuração de crimes envolvendo abuso sexual infantojuvenil.

O estudo falhou ao não cuidar da atuação da instituição que utiliza, no Brasil, as informações advindas dessa tecnologia. Talvez essa omissão tenha surgido da falta de policiais escrevendo sobre o tema no ambiente acadêmico, possivelmente pela necessidade de manter sigilo sobre os métodos de investigação, diante da óbvia circunstância de não alertar os criminosos e ensiná-los a evitar as apurações. De todo modo, o estudo ignora diversos aspectos do complexo problema do abuso sexual de crianças e adolescentes e apresenta conclusões açodadas, baseadas em análises incompletas ou em absoluta ficção. Oferecida a oportunidade de debater os argumentos manejados, apresentar-se-ão breves considerações sobre privacidade, evolução de técnicas de investigação, varredura pelo lado de cliente, abuso sexual contra crianças e adolescentes e os resultados do trabalho da Polícia Federal nessa área, que refutam a alegada ineficiência da tecnologia na prioritária missão de proteger os mais jovens de abusadores sexuais.

Emerge de toda investigação criminal a aparente desarmonia entre os direitos individuais à privacidade e à segurança, ambos igualmente imprescindíveis, individual e coletivamente, e consagrados no artigo 5º da Constituição de 1988. Impende ao aplicador da legislação nacional encontrar equilíbrio e proporcionalidade em cada caso, baseado em parâmetros constitucionais, como os bens jurídicos envolvidos.

A privacidade tem sido objeto de grande preocupação de estudiosos, diante da captação em larga escala de dados (meramente cadastrais, profissionais, ou até personalíssimos), feito por empresas de tecnologia, como Google, Apple, Meta, dentre centenas de outras menores, nem sempre menos invasivas. Toda a atividade humana no ciberespaço gera algum

rastro digital que não evapora simplesmente. Ao contrário, em regra, enseja algum registro telemático que acaba sendo usado para individualizar melhor o usuário e, assim, apresentar-lhe sugestões várias como o próximo vídeo a assistir, qual pessoa convidar para sua rede social, qual postagem curtir, qual criticar, qual mercadoria comprar ou até mesmo em qual candidato votar, ainda que veladamente. Quanto mais informações as pessoas disponibilizam, renunciando a sua privacidade por motivos vários (fama, monetização, vaidade, necessidade profissional, vontade de utilizar um aplicativo etc.), maior o aprimoramento dos algoritmos e a precisão das sugestões. Privacidade e tecnologia andam de mãos dadas. A evolução desta gera discussões novas sobre aquela e exige atualização constante dos seus estudiosos.

Pela relevância do tema, defender a privacidade dos cidadãos brasileiros não é novidade à Polícia Federal. Dentre várias, duas operações policiais de grande repercussão mostram-no indubitavelmente. A investigação sobre a "Abin Paralela", na denominação criada pela imprensa,[7] procura esclarecer possível utilização da estrutura da agência de inteligência para fins ilícitos, durante o governo Bolsonaro, mediante uso de equipamentos que possibilitavam o acompanhamento em tempo real da localização das vítimas,[8] dentre as quais várias autoridades públicas.

A Operação Durkheim, deflagrada no fim de 2012,[9] desvendou um esquema gigantesco de venda de informações pessoais, vazadas de entes públicos (como bancos de dados da polícia, da Receita Federal, de bancos públicos) e privados (como bancos, operadoras de telefonia, provedores de internet etc.). Milhares de vítimas foram identificadas, centenas foram ouvidas durante a investigação e, surpreendentemente, poucas se importaram com o vazamento das suas informações. Em regra, apenas aquelas que experimentaram algum prejuízo financeiro mostraram interesse em ver os autores responderem criminalmente pela venda de dados sigilosos. Era um prenúncio do que os anos seguintes trariam com a cultura de hiperexposição em redes sociais, que tornou comum pessoas registrarem detalhadamente seu cotidiano em público. Fotos dos pratos das três refeições, do treino na academia, da porta da escola dos filhos, do novo lençol na cama de casa, ou até do bebê no banho inundaram as páginas pessoais na Internet. Privacidade tornou-se cada vez mais um direito que preocupa muito mais policiais, juristas e estudiosos do tema, não seus titulares.

Qualquer investigação criminal implica algum avanço na esfera da privacidade do investigado a depender da natureza do crime e da complexidade do caso. Nas mais simples, há pesquisas em bancos de dados oficiais, levantamentos no local de residência e de trabalho, intimações para comparecimento à unidade policial, por exemplo. Nas complexas, usam-se técnicas extraordinárias de investigação, que, por mais invasivas, dependem de autorização judicial como afastamentos de sigilo bancário e fiscal, interceptação telefônica e telemática, buscas domiciliares, dentre outras. A evolução da forma de comunicação entre as pessoas, pela substituição das ligações telefônicas pelo uso massivo do WhatsApp, obrigou a atualização da seleção das melhores técnicas investigativas

7. FOLHA DE S. PAULO: Investigação da 'Abin paralela' tem indícios contra suspeitos e série de lacunas. São Paulo, 03 fev. 2024. Disponível em: https://www1.folha.uol.com.br/poder/2024/02/investigacao-da-abin-paralela-tem-indicios-contra-suspeitos-e-serie-de-lacunas.shtml. Acesso em: 30 maio 2024.

8. Isso com base apenas em informações publicadas na imprensa até o momento da conclusão deste texto, em maio de 2024, como apontado na nota anterior.

9. EXAME: Operação Durkheim: senador e ex-ministro foram vítimas. São Paulo, 26 nov. 2012. Disponível em: https://exame.com/brasil/operacao-durkheim-senador-e-ex-ministro-foram-vitimas/. Acesso em: 30 maio 2024.

pela polícia, que passou a se valer mais da apreensão do dispositivo para, a partir dele, ter acesso ao seu conteúdo, com autorização judicial, e aprofundar a apuração. Eis uma forma de varredura pelo lado do cliente, que não se revela nova, mas que passou a ser mais utilizada pela mudança do meio de comunicação preferido.

Outra forma de varredura pelo lado cliente é objeto do estudo feito pelo Instituto de Referência em Internet e Sociedade que assim apresenta a questão:

> "o cenário da varredura pelo lado do cliente (em inglês client-side scanning, com as iniciais CSS, aqui abreviada como VPLC). O termo se refere a técnicas de escaneamento realizado no dispositivo de usuários ("cliente") para identificação de instâncias de compartilhamento de materiais considerados ilícitos – especialmente envolvendo conteúdo sexual de abuso de crianças e adolescentes ou CSAM (child sexual abuse material) – em ambientes protegidos por criptografia segura, ao invés de realizar esse escaneamento ao nível de servidor. Por meio de uma revisão sistemática de literatura, investigou-se um total de 22 publicações selecionadas. Os achados foram organizados em contexto, conceito, funcionamento e problemas."[10]

Explicam-se, no decorrer do texto, os acontecimentos envolvendo a Apple que ensejaram "tanta controvérsia em torno da VLPC"[11] e, aparentemente, motivaram a publicação:

> *"Em 5 de agosto de 2021, a Apple anunciou que ainda naquele ano adotaria três mudanças nos seus sistemas operacionais (iOS 15, watchOS 8, iPadOS 15 e macOS Monterey), a fim de aprimorar o enfrentamento a materiais de abuso sexual infantil, ou CSAM (sigla para o termo em inglês Child Sexual Abuse Material).*
>
> *(...)*
>
> *Com a segunda mudança, "Detecção de CSAM", antes de serem enviadas para o iCloud Photos, as imagens seriam convertidas em hashes e, no dispositivo, comparadas com os hashes de materiais de abuso sexual infantil de um banco de dados fornecido pela ONG estadunidense NCMEC – National Center for Missing and Exploited Children ("Centro Nacional para Crianças Desaparecidas e Exploradas")."*[12]

Portanto, haveria uma comparação de *hashes* antes do procedimento de criptografia. O texto registra a suspensão dessa medida pela Apple com o argumento de proteger a privacidade dos seus clientes da suposta vigilância. Argumenta-se que haveria enfraquecimento da criptografia ponta a ponta, se houvesse esse cotejo de *hashes* e relato da existência de arquivos contendo abuso sexual infantojuvenil ao NCMEC. Após alentada argumentação técnica, no fim, o trabalho apresenta algumas conclusões que merecem reflexão e refutação individual.

Na primeira, afirma-se que, quanto ao funcionamento, há "impossibilidade de se empregar essa tecnologia em qualquer hardware ao nível de cliente",[13] uma vez que a falta de atualização do sistema

10. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. Varredura pelo lado do cliente: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Acesso em: 23 ago 2023.

11. *Ibidem*, p. 13.

12. *Ibidem*, p. 13

13. *Ibidem*, p. 24.

operacional ou a obsolescência do hardware, dentre outros fatores, podem tornar-se empecilhos para o "uso da VPLC de maneira verificavelmente ampla por autoridades públicas".[14]

O primeiro argumento pressupõe que o sistema de verificação de *hashes*, pelo lado do cliente, precisaria ser perfeito e infalível para ser útil. No entanto, ainda que nem todos os usuários sejam abrangidos pela tecnologia, melhor que haja alguma forma de filtro para arquivos ilícitos. Lamentável que alguns abusadores sexuais possam não ser reportados por alguma razão tecnológica aleatória, mas, com a tecnologia, ao menos outros acabarão nos bancos de dados do NCMEC e, posteriormente, da Polícia Federal, de forma a possibilitar, após detida análise dos dados, a eventual instauração de uma investigação criminal.

14. *Ibidem*, p. 24.

Impedir o uso tecnologia porque ela pode falhar em algumas hipóteses não faz qualquer sentido, não fortalece a esfera de privacidade coletivamente e, sem dúvida, enfraquece a proteção do direito à segurança e à vida de crianças e adolescentes, ao tornar impunes pessoas que possuem arquivos contendo abuso sexual infantojuvenil. Aqui, um singelo relatório que enseje a retirada de uma criança da submissão ao seu estuprador basta para justificar a existência da tecnologia, ainda que, infelizmente, esta não seja suficiente para ajudar a polícia a salvar todas as que se encontram nessa terrível situação.

A segunda conclusão versa sobre a "eficácia" e argumenta: "observa-se que o uso de técnicas de *hash* perceptivo – propostas na vasta maioria das soluções de VPLC até o momento – necessitam de uma base de *hashes* correspondentes ao conteúdo ilegal que se quer identificar para que possam funcionar, visto que dependem de uma comparação entre o material compartilhado pelos usuários e essa base original de *hashes* ilícitos".[15]

Em seguida, mostra preocupação porque a maioria dos arquivos – "84%" – é denunciada "apenas uma vez" e há risco de "níveis mais baixos de sensibilidade do algoritmo possibilitam a adulteração de conteúdos inócuos para atribuir a eles *hashes* idênticos aos de conteúdos marcados como ilícitos, possibilitando a ativação de falsos positivos nos sistemas de comparação desses *hashes*, em especial por agentes mal-intencionados".[16]

15. *Ibidem*, p. 24.

16. *Ibidem*, p. 21.

O segundo argumento tem semelhança com o primeiro, ao supor ser necessária uma tecnologia perfeita para fazer essa verificação automatizada pela empresa que disponibiliza o serviço na internet. Parece haver a presunção de que, quando a polícia receber a informação, haverá automática instauração de inquérito policial, busca domiciliar e prisão, sem qualquer análise prévia desse relatório automático enviado pela empresa ao NCMEC.

Ainda que haja relatórios do NCMEC que tragam situações penalmente irrelevantes como piadas de mau gosto contendo crianças nuas, fotos de pais orgulhosos e inocentes a ponto de publicar a genitália dos seus bebês em redes sociais e outras situações quejandas, a polícia fará uma análise dos dados recebidos e focará suas ações apenas nos relatórios que registrem crimes dolosos, casos de abusadores e estupradores de crianças e adolescentes. Por meio de metodologia própria, aprimorada frequentemente, separam-se situações irrelevantes de outras gravíssimas que atingem os jovens, únicos cujos direitos mereceram respeito com "prioridade absoluta"[17] da Constituição de 1988.

17. Artigo 227 da Constituição Federal

A terceira conclusão versa sobre "segurança": "constata-se que as bases de *hashes* ilícitos podem ser facilmente adulteradas por agentes mal-intencionados, representando assim uma ampliação na superfície de ataque de sistemas criptográficos".[18]

O argumento revela-se meramente hipotético. As listas podem ser adulteradas, diz-se. Embora extremamente improvável, se isso acontecer, o relatório automático será encaminhado ao NCMEC, que repassará à PF e, na análise da autoridade pública brasileira, certamente ver-se-á que o arquivo reportado não é ilícito. Mais uma vez, o texto acadêmico parece presumir que a polícia brasileira não faz análise dos relatórios que recebe. Do momento do relatório automático da empresa à instauração da investigação há um considerável caminho, que passa por uma fase de análise policial, segundo metodologia própria, desenvolvida ao longo dos últimos anos na Polícia Federal e respeitada internacionalmente,[19] por apresentar excelentes resultados em ignorar os casos irrelevantes penalmente e possibilitar a responsabilização penal de abusadores sexuais e estupradores de crianças e adolescentes.

Depois, trazendo considerações sobre o "escopo" da tecnologia de verificação da existência de arquivos contendo abuso sexual infantojuvenil, a quarta conclusão alerta sobre a "possibilidade de abuso dessas ferramentas por parte de autoridades públicas ou mesmo das próprias plataformas que

18. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renáda Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente:** uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Acesso em: 23 ago 2023. p. 25.

19. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Ministério da Justiça e Polícia Judiciária de Portugal compartilharão software para combater abuso sexual infantil. Brasília, 27 fev. 2024. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-policia-judiciaria-de-portugal-compartilharao-software-para-combater-abuso-sexual-infantil. Acesso em: 20 mai. 2024.

/ A POLÍCIA FEDERAL TORNOU-SE REFERÊNCIA INTERNACIONAL NA APURAÇÃO DE CRIMES ENVOLVENDO ABUSO SEXUAL DE CRIANÇAS E ADOLESCENTES NO CIBERESPAÇO /

as administram, a fim de identificar e repreender instâncias de compartilhamento de conteúdo por motivos ideológicos, políticos, socioculturais, entre outros. A possibilidade de ampliação do escopo do conteúdo rastreado por VPLC representa um risco significativo – em especial para comunidades e populações marginalizadas e perseguidas –, o que se opõe diametralmente às expectativas de segurança da informação e liberdade de expressão que se busca proteger através do uso de algoritmos criptográficos em um primeiro momento".[20]

Mais uma vez, há um argumento meramente hipotético. Como "há possibilidade de abuso dessas ferramentas", a eventualmente representar um "risco significativo – em especial para comunidades e populações marginalizadas e perseguidas", demoniza-se a tecnologia que, no mundo real, ajuda na proteção da incolumidade sexual de crianças e adolescentes, que normalmente fazem parte desses grupos socialmente marginalizados.

Parte-se de um preconceito de que a polícia sempre pretende perseguir minorias e pessoas pobres. Ao receber o relatório automatizado do NCMEC, a Polícia Federal dispõe, em regra, apenas das informações cadastrais do usuário reportado. Nem seria possível fazer essa seleção porque a identificação do suspeito virá apenas em momento posterior, com o inquérito policial já instaurado.

Outro ponto ignorado nesse argumento baseado na possibilidade de abuso policial é que os estupradores de crianças e adolescentes, na absoluta maioria dos casos, são pessoas muito próximas socialmente das vítimas (são familiares, vizinhos, amigos próximos etc.).[21] Significa dizer que, normalmente, se o criminoso faz parte de um grupo marginalizado socialmente, suas vítimas também o fazem. Então, não faz sentido excluir a tecnologia porque há "possibilidade" de a polícia perseguir grupos marginalizados, de modo a prejudicar as crianças e adolescentes que fazem parte do mesmo grupo e são abusadas sexualmente.

Reitere-se, que se argumenta aqui apenas em hipótese, mesmo porque, em regra, os inquéritos são instaurados sem prévia identificação do suspeito, cujos dados pessoais costumam ser obtidos (ou confirmados) posteriormente, de modo que nem seria possível fazer essa escolha racista ou classista, levianamente sugerida nessa conclusão do trabalho acadêmico, sem apresentar um caso sequer em que isso aconteceu.

Persistindo nas hipóteses, também se demoniza a tecnologia de filtro de abuso sexual infantojuvenil sob o argumento fictício de que, eventualmente, ela pode ser usada "por motivos ideológicos, políticos, socioculturais (...)".[22]

Porém, como o próprio texto acadêmico registra, a comparação resume-se a cotejar uma lista de *hashes* conhecidos, categorizados como ilícitos, com os dos arquivos do usuário. Há objetividade nessa comparação, de modo a tornar difícil imaginar como poderiam motivos ideológicos, políticos ou socioculturais ser usados para perseguir cidadãos. Comparam-se expressões alfanu-

20. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente:** uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <bit.ly/3EAhEDF>. Acesso em: 23 ago 2023. p. 25.

21. CARPANEZ, Juliana. 'Fique amigo dos pais': polícia revela mensagens trocadas por abusadores de crianças. Uol. São Paulo, 27 jul. 2018. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2018/07/27/fique-amigo-dos-pais-policia-revela-mensagens-trocadas-por-abusadores-de-criancas.htm. Acesso em: 30 maio 2024.

22. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente:** uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente>. Acesso em: 23 ago 2023. p. 25.

méricas de fotos e vídeos, possivelmente ilícitos por conter abuso sexual infantojuvenil. Se houver correspondência, o usuário é reportado.

Ainda assim, na improbabilíssima hipótese de isso acontecer, a comparação tecnológica, feita no âmbito da empresa, tem o condão de apenas ensejar o envio de um relatório ao NCMEC. Eventual investigação criminal iniciar-se-ia apenas após a fase de análise preliminar na Polícia Federal, exclusivamente se realmente houvesse arquivos contendo abuso sexual infantojuvenil. Sem eles, não há possibilidade de instauração de inquérito. Se o algoritmo da tecnologia, portanto, estivesse reportando pessoas por motivos ideológicos, não haveria qualquer repercussão penal, porque facilmente a Polícia Federal verificaria o equívoco e, ainda que em má-fé quisesse, nem estaria apta a instaurar um inquérito policial sem arquivos contendo abuso sexual infantojuvenil.

A menção à "liberdade de expressão"[23] também parece mal colocada nessa conclusão. Possuir fotos e vídeos de abuso sexual infantojuvenil, compartilhar na internet, e outras condutas semelhantes configuram crimes e, portanto, não estão protegidas pelo relevantíssimo direito de liberdade de expressão, que não é afetado pelo uso de tecnologia de verificação objetiva por meio de cotejo de *hashes*.

23. *Ibidem*, p. 25.

Nas conclusões jurídicas, o trabalho argumenta que "as garantias de privacidade e sigilo da criptografia de ponta a ponta são violadas em casos em que os resultados da comparação de *hashes* sejam compartilhados com o servidor. Esse compartilhamento, contudo, é necessário para que seja possível uma verificação humana do material apontado como ilícito pelo algoritmo, para evitar a penalização de falsos positivos."[24]

24. *Ibidem*, p. 25

A verificação pela comparação (pelo cliente ou pelo servidor) de *hashes* é feita por empresas, sediadas nos Estados Unidos, que, pela legislação de lá, estão obrigadas a reportar casos de abuso sexual infantojuvenil nos seus serviços. Quando há alguma correspondência, a empresa reporta o caso ao NCMEC, que, por sua vez, encaminha o relatório ao Brasil, na hipótese de estar em território nacional o usuário reportado. A Polícia Federal recebe esse relatório apenas, não possui qualquer ingerência ou participação no momento anterior de verificação de *hashes*. Portanto, a autoridade policial brasileira recebe esse relatório como uma possível notícia de crime, que necessariamente passará por uma análise antes de ensejar a instauração de um inquérito policial.

O momento de verificação de *hashes* rege-se pela lei americana e pelo contrato firmado entre a empresa provedora do serviço na internet e o usuário reportado. Não se vislumbra qualquer violação à privacidade ou à inviolabilidade de comunicações, porque a hipótese é de obrigatoriedade de reportar um crime. O usuário está violando a lei, o contrato e os termos de uso da plataforma ao possuir ou distribuir material com abuso sexual infantojuvenil.

Alude-se também a uma suposta ofensa à "presunção da inocência"[25] no uso dessa tecnologia. Aqui também, pretende-se dar um alcance exagerado e incabível a essa fundamental garantia constitucional. Se fosse tão ampla, qualquer pessoa que procurasse a polícia para reportar um crime estaria violando a Constituição. Mais uma vez, trata-se apenas de notícias de crime elaboradas automaticamente por empresas sediadas nos EUA, conforme legislação local, e enviadas à Polícia Federal, com a intermediação do NCMEC. Todos os relatórios são tratados de modo a preservar a privacidade

25. *Ibidem*, p. 25.

dos envolvidos e o sigilo necessário para eventual inquérito policial, instaurado após análise detida e constatação da existência de arquivos ilícitos.

Por fim, o texto acadêmico afirma quanto "à **proporcionalidade** e à **necessidade**, observa-se, por todo o exposto, que técnicas de VPLC representam um risco desproporcional em comparação com os benefícios obtidos. Adicionalmente, esse risco mostra-se desnecessário em relação ao objetivo almejado, tendo em vista todas as barreiras tecnológicas apontadas ao longo deste trabalho, que tornam a VPLC uma ferramenta pouco eficaz para o combate aos ilícitos que se pretende repreender através dessa técnica."[26]

26. *Ibidem*, p. 26.

Novamente, não lhe assiste razão. O trabalho acadêmico não apresenta eventuais pontos positivos da tecnologia. Ao não os elencar, deixa a impressão de que se trata de uma ferramenta cuja finalidade é apenas fazer vigilância em massa, desrespeitar privacidade e sigilo das comunicações, com a enviesada intenção de atingir "comunidades e populações marginalizadas e perseguidas". [27]

27. *Ibidem*, p. 25.

28. Muito diferente das violações sérias à privacidade descobertas no caso da "Abin Paralela", ou da Operação Durkheim, nacionalmente, e casos Snowden e Cambridge Analytica, internacionalmente.

Na verdade, não há vigilância massiva na mera comparação objetiva de *hashes* com o fim de encontrar vídeos e imagens ilícitas.[28] Por serem objetivamente verificáveis, em um cotejo de expressões alfanuméricas, esse procedimento na empresa (seja pelo lado do cliente ou do servidor) nem arranha o direito à privacidade ou a inviolabilidade de comunicações do reportado, muito menos serve a perseguir grupos socialmente desfavorecidos.

O ponto positivo da tecnologia é incontestavelmente mais relevante que essas hipotéticas violações à privacidade. Embora imperfeita, incapaz de servir para reportar todos os arquivos ilícitos, a tecnologia atacada serve para encaminhamento de informação relevante à Polícia Federal, que a possibilita salvar crianças e adolescentes de situações de estupros frequentes e, consequentemente, levar à Justiça Criminal seus algozes. Os casos são inúmeros e estão disponíveis na imprensa, pelo Brasil inteiro, diariamente.

Sem contar a notória subnotificação nesse tipo de delito, o Fórum Brasileiro de Segurança Pública, em 2023, registrou que houve 74.930 estupros em 2022, uma média de 205 por dia e 75,8% deles tiveram como vítimas crianças, adolescentes, ou alguém com deficiência ou enfermidade.[29] Um problema social seríssimo, que faz do Brasil o país do estupro, crime extremamente difícil de ser apurado. Como normalmente ocorrem na esfera íntima, apenas vítima e criminoso testemunham os fatos. O primeiro grande obstáculo é o silêncio, uma vez que as vítimas não costumam reportá-los à polícia, por variadas razões.

29. MENON, Isabella. Brasil registra 75 mil estupros em 2022 e bate recorde. Folha de S. Paulo. São Paulo, 20 jul. 2023. Disponível em: https://www1.folha.uol.com.br/cotidiano/2023/07/brasil-registra-75-mil-estupros-em-2022-e-crime-bate-recorde-no-pais.shtml. Acesso em: 30 maio 2024.

Embora não sejam competência da Polícia Federal, esta possui um caminho, dentro de suas restritivas atribuições constitucionais, para contribuir nessa delicada situação social. Em alguns casos, vence-se esse silêncio da vítima e identifica-se o estuprador, em investigações de produção, posse ou compartilhamento de arquivos contendo abuso sexual infantojuvenil no ciberespaço. Na grande maioria, relatórios do NCMEC, obtidos pela varredura de *hashes*, ou deram início

à investigação ou foram usados para a instruir em algum momento. Por isso, ainda que imperfeita a tecnologia, seja pelo servidor ou pelo lado do cliente, o fato é que essas informações são preciosas para tirar centenas de jovens dessa situação de estupros frequentes.

Nesse ponto, cumpre ressaltar que, nas conclusões do trabalho, lê-se também que "as técnicas aqui analisadas representam mecanismos de combate à disseminação de conteúdo ilícito, mas não eliminam a fonte criadora de materiais dessa natureza".[30] Verdade, infelizmente, na enorme maioria dos casos.

Mas não usar a técnica também não elimina a "fonte criadora de materiais dessa natureza". Então, melhor usar uma ferramenta imperfeita que permite desvendar centenas de casos em que há a prisão do abusador sexual, eliminando a fonte. Infelizmente, não será mesmo possível acabar de vez com todos os abusos sexuais, mas as vítimas que a Polícia Federal salva por ano importam. Uma bastaria para justificar todo esforço.

E o último ponto da conclusão versa sobre os "**prejuízos econômicos** que podem ser causados em decorrência da obrigação legal de filtragem massiva de conteúdos por parte das plataformas, o que poderia resultar na impossibilidade de plataformas de pequeno porte atuarem nesse mercado e, assim, resultar em uma concentração de mercado ainda mais intensa por grandes provedores de aplicação."[31]

30. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente:** uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Acesso em: 23 ago 2023. p. 26.

31. *Ibidem*, p. 26.

Aqui, sugere-se ser mais importante manter o mercado funcionando que proteger a incolumidade sexual de crianças e adolescentes. Realmente, nenhuma empresa quer fazer essa "filtragem massiva" porque custa dinheiro e reduz lucros. Se elas não o fizerem, tornar-se-ão portos seguros para abusadores sexuais e estupradores de crianças e adolescentes. Parece contraditório um texto preocupado com perseguição policial a grupos marginalizados, defender um mercado trilionário como o de tecnologia argumentando que as empresas têm prejuízos econômicos com a obrigação legal de reportar abuso sexual de crianças e adolescentes nas suas plataformas.

Aos interessados em uma amostra grátis de um ambiente totalmente anônimo na Internet, sem filtros e no qual a privacidade atinge níveis altíssimos, sugere-se uma breve navegação na Dark Web. Mais ousados pela promessa de anonimato, investigados pela Polícia Federal, nesse ambiente, já discutiram, entre compartilhamentos de materiais ilícitos, qual pomada é a melhor para a genitália de bebês estuprados diariamente,[32] qual anestésico usar para a criança não chorar tanto de dor mas também não ficar totalmente desfalecida enquanto é penetrada, qual seria a tortura sexual seguinte contra uma menina de apenas nove anos que figurava como vítima em vídeos que prometiam partir do fim de sua inocência (estupros sucessivos) até sua morte ao vivo e em cores, entre outras barbaridades semelhantes.[33] Se não houver objeção para que esse tipo

32. METRÓPOLIS: Ciência ajuda PF a decifrar rede de pornografia infantil na web. São Paulo, 16 jan. 2020. Disponível em: https://www.metropoles.com/brasil/policia-br/ciencia-ajuda-pf-a-decifrar-rede-de-pornografia-infantil-na-web. Acesso em: 30 maio 2024.

33. ROCHA, Alex; IDALÓ, Eduardo. Médico de Uberaba admite pedofilia e se diz doente, segundo PF. G1: Triângulo Mineiro. Uberaba, 22 dez. 2015. Disponível em: https://g1.globo.com/minas-gerais/triangulo-mineiro/noticia/2015/12/medico-de-uberaba-admite-relacao-com-pedofilia-e-se-diz-doente-diz-pf.html. Acesso em: 30 maio 2024.

de conteúdo emerja à superfície da Internet, parece bem adequado acabar com a exigência da obrigação de reportar abuso sexual infantil ao NCMEC, em nome da higidez econômica das empresas.

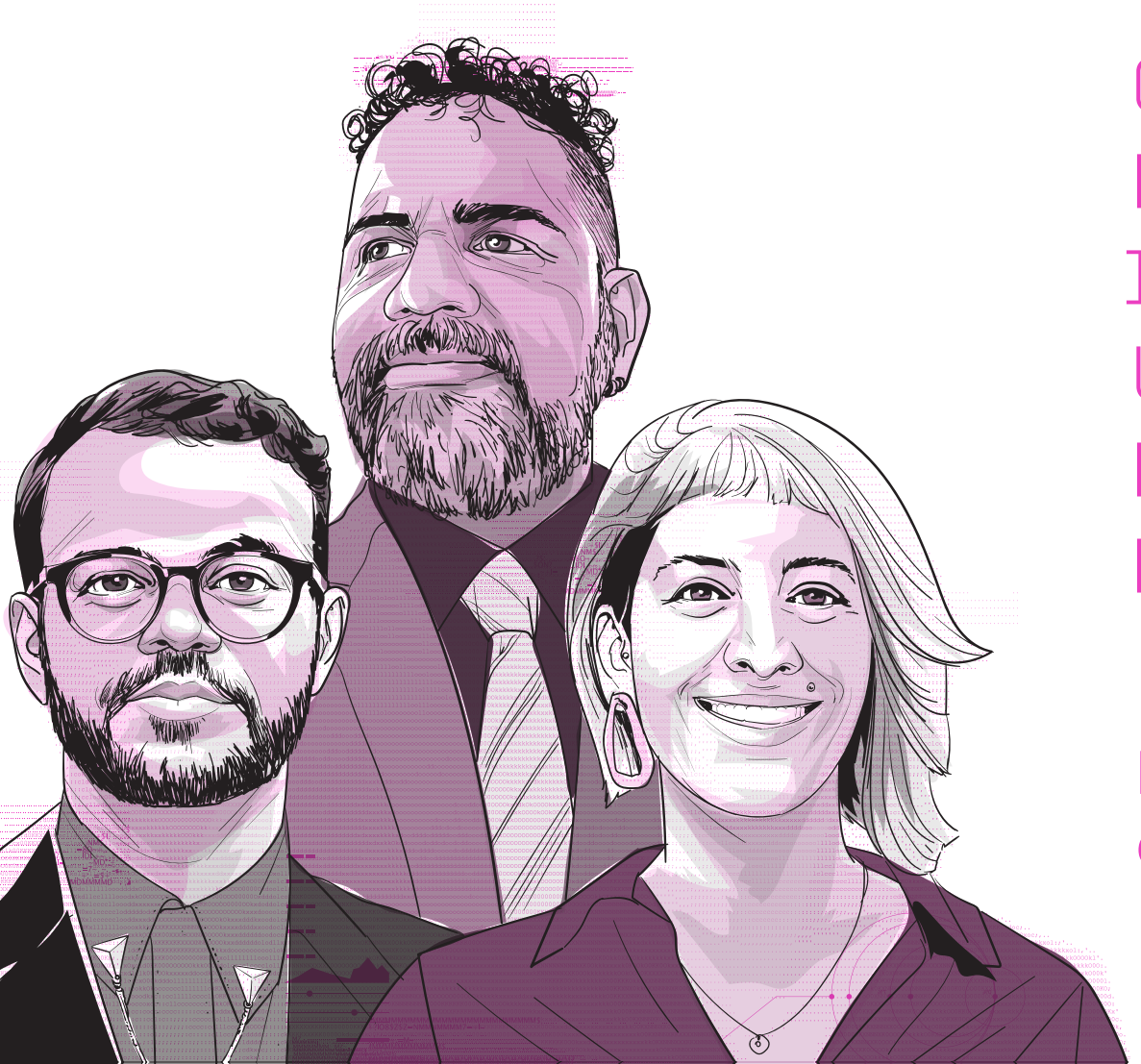
Em 2023, a Polícia Federal criou a Diretoria de Combate a Crimes Cibernéticos e, dentre as unidades subordinadas, nasceu uma Coordenação cuja missão é gerenciar e orientar todas as operações policiais, nas apurações de abuso sexual infantojuvenil online. Os resultados foram melhores que os esperados. Em 2022, houve 454 operações policiais nessa temática e 294 prisões. Em 2023, 1017 e 534, respectivamente, aumentos de 124% e 81,63%[34] nos números. Ademais, 164 vítimas de estupro foram identificadas e retiradas da situação de abuso sexual, de modo que a cada 2 dias aproximadamente, uma criança foi retirada pela PF dessa situação torturante.

34. DINO, Flávio. Atendendo à diretriz que estabelecemos, a Polícia Federal ampliou o combate a crimes cibernéticos relativos a abusos contra crianças e adolescentes. Cumprimento a direção da PF e as equipes participantes >> . 4 de jan de 2024. Disponível em: https://x.com/flaviodino/status/1742973378137329870.

Cumpre repetir que crianças e adolescentes foram os únicos a serem contemplados com absoluta prioridade na proteção de seus direitos pela Constituição de 1988. Na aparente antinomia entre privacidade, pelo uso da tecnologia de comparação de *hashes* ao reportar casos ao NCMEC, e o direito à segurança e à vida (aqui incluída a incolumidade física) de crianças e adolescentes, o artigo 227 da Lei Maior não deixa dúvida do que deve prevalecer. O uso dessa tecnologia respeita confortavelmente parâmetros de proporcionalidade e segurança, sobretudo ao levar em conta que possibilita o salvamento de crianças de situações de abuso sexual.

A Polícia Federal tornou-se referência internacional na apuração de crimes envolvendo abuso sexual de crianças e adolescentes no ciberespaço. Não se limita, atualmente, a desenvolver trabalhos decorrentes de operações anteriores ou de informações vindas de alguma polícia estrangeira. Por dispor das informações do NCMEC, além de alcançar os distribuidores desse tipo de material, prioriza a identificação e responsabilização penal de estupradores de crianças, bem como o resgate das vítimas. Fá-lo em um esforço para, dentro de suas restritivas competências, contribuir na melhoria de um problema social gravíssimo, o vergonhoso número de estupros registrados no Brasil.

12.



CRIPTOGRAFIA E DIREITOS INFANTOJUVENIS: UM DIÁLOGO PARA ALÉM DAS POLARIZAÇÕES

Luiza Correa, Paulo Renã e Wilson Guilherme

A polarização, conforme definida nos dicionários, é um substantivo feminino que designa a "ação de polarizar, ou seja, de atribuir potenciais eletrônicos a dois eletrodos distintos; o que resulta dessa atribuição."[1] Quando aplicada ao contexto político e social, a polarização refere-se à divisão de dois grupos posicionados de maneira oposta, gerando uma impossibilidade de diálogo entre eles, o que resulta em uma acentuada ênfase na prevalência de um grupo em detrimento do outro.

A partir do desejo de assegurar uma internet segura, com acesso para todas as pessoas, em consonância com os direitos humanos, o Instituto de Referência em Internet e Sociedade (IRIS), ao longo dos últimos quase dez anos, tem orientado a construção de suas investigações a partir de preceitos fundamentais, tais como: independência e autonomia científica, consistência metodológica e localização dos saberes. Esses atributos são essenciais para o posicionamento da ciência, particularmente em áreas interligadas às humanidades.

Os resultados que detalhamos a seguir são, portanto, mais um dos muitos aprofundamentos científicos do instituto e das nossas equipes de pesquisa. Neste contexto, apresentamos algumas reflexões que vão entrecruzar nossas análises científicas com as experiências profissionais e acadêmicas das pessoas dedicadas à pesquisa que, juntas, acumulam mais de 20 anos no campo de produção e investigação científica nas áreas de direitos humanos, direitos de crianças e adolescentes, segurança pública e direitos digitais. Situar estes conhecimentos é, inclusive, parte da epistemologia de localização de saberes;[2] afinal, nenhum saber surge no vácuo.

Em particular, este texto, trata-se de uma apresentação de nossos acúmulos na intersecção dos campos de criptografia e dos direitos de crianças e adolescentes, especialmente do enfrentamento as violências sexuais, a partir de duas grandes pesquisas. A primeira, o relatório publicado em outubro de 2022, sob o título "*Comunicações privadas, investigações e direitos: varredura pelo lado do cliente*", compõe nossos esforços em torno da análise de meios de investigação que são propostos como supostas alternativas à quebra da criptografia.[3] Este trabalho teve como foco a revisão de obras acadêmicas sobre o tema do *client-side scanning*, que traduzimos para o português como "varredura pelo lado do cliente", com a sigla VPLC.[4]

E o segundo advém de nossa pesquisa mais recente, intitulada "*Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no MERCOSUL*".[5] Esta investigação foi desenvolvida a partir da inquietação em compreender como garantir a proteção dos direitos de crianças e adolescentes em espaços criptografados, refletindo nosso compromisso

1. DICIO. **Polarização**. Disponível em: https://www.dicio.com.br/polarizacao/. Acesso em: 4 dez. 2024.

2. HARAWAY, Donna. Saberes localizados: a questão da ciência para o feminismo e o privilégio da perspectiva parcial. **Cadernos Pagu**, Campinas, SP, n. 5, p. 7–41, 2009. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/cadpagu/article/view/1773. Acesso em: 4 dez. 2024.

3. O primeiro relatório, sobre o panorama da rastreabilidade de mensagens instantâneas, foi publicado em 18 de maio daquele ano, sob o título "*Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas*". O terceiro foi publicado em dezembro de 2022, sob o título "*Hacking governamental: uma revisão sistemática*".

4. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. Varredura pelo lado do cliente: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-varredura-pelo-lado-do-cliente/>. Acesso em: 04 dez.2024.

5. IRIS BH. **Segurança da Informação e Proteção de Crianças e Adolescentes: discursos e propostas regulatórias no Mercosul**. Disponível em: https://irisbh.com.br/projetos/seguranca-da-informacao-e-protecao-de-criancas-e-adolescentes-discursos-e-propostas-regulatorias-no-mercosul/. Acesso em: 4 dez. 2024.

ético com a ciência e com os direitos humanos, especialmente no que se refere ao enfrentamento das violências sexuais contra este grupo social em ambientes digitais, com foco na região do MERCOSUL.

Mas, antes de seguirmos com a apresentação das reflexões de nossas pesquisas, gostaríamos de abrir este texto com uma espécie de prefácio, ou *"aviso de conteúdo sensível"*. Este aviso se mostra oportuno não apenas pelo fato de ser uma análise sobre violências sexuais contra crianças e adolescentes, o que, por si só, já justificaria a sensibilidade do tema; mas também porque a produção científica que fazemos no IRIS nos convoca a refletir sobre a compatibilização de direitos no contexto das tecnologias digitais.

Assim, fazemos o convite para ler este material com as lentes da compatibilização, entendendo que os direitos à privacidade, liberdade de expressão, presunção de inocência, proteção de dados pessoais e outras garantias asseguradas pela criptografia não são opositores aos direitos sexuais e proteção de crianças e adolescentes, em especial no espaço digital. Pelo contrário, em nosso entendimento, trata-se de direitos humanos os quais devem também ser garantidos para crianças e adolescentes, guardando relação de complementaridade, de modo que os mecanismos do Estado para sua salvaguarda, em conjunto, devem ser estabelecidos com cautelas, inclusive para garantir que crianças e adolescentes cujos direitos já foram violados não sejam revitimizadas.

É preciso compreender este debate a partir das lentes interpretativas da libertação coletiva, como nos ensina Audre Lorde: "Não serei livre enquanto alguma mulher for prisioneira, mesmo que as correntes dela sejam diferentes das minhas".[6] Assim, não há libertação real enquanto crianças sofrem violência online (e offline), e tampouco existe uma garantia de efetividade de seus direitos enquanto toda a sociedade, incluindo elas, forem vigiadas de modo desenfreado.

6. LORDE, Audre. Sister outsider. Freedom, CA: The Crossing Press, 1984. [Tradução de Tatiana Nascimento, revisada em fevereiro de 2012, do artigo The Master's Tools Will Never Dismantle the Master's House, in: Lorde, Audre. Sister outsider: essays and speeches. New York: The Crossing Press Feminist Series, 1984. 110-113.]

METODOLOGIA DE PESQUISA - OU DE ONDE PARTIMOS PARA PESQUISAR CIENTIFICAMENTE

A pesquisa científica e a construção da ciência pressupõem discussões teóricas e metodológicas de base para o desenvolvimento de um campo do saber específico. Contudo, esse campo não é estático, rígido ou imutável. No campo das humanidades, mais especificamente no campo das ciências sociais, podemos arriscar dizer que a ciência é feita a partir da investigação das dinâmicas sociais, culturais, econômicas e políticas, e de como estas se inter-relacionam e constituem as instituições e os atores sociais, os quais, por sua vez, também as moldam.[7] Ou seja, quase uma análise das estruturas sociais e dos agentes sociais com o intuito de obter teorias e explicações que contribuam para a compreensão profunda das interações sociais e da organização da sociedade em diferentes contextos.

Para produzir um conhecimento cientificamente válido não seria suficiente o mero uso de reportagens jornalísticas enquanto base bibliográfica para sustentar um argumento, por exemplo. A pesquisa científica não se faz com ilusões persecutórias, escritas antiéticas ou polarizações dogmáticas, nem tampouco sobre opinião pessoal: as metodo-

7. OSTERNE, M. do S. F.; BRASIL, G. M.; ALMEIDA, R. de O. A produção do conhecimento nas Ciências Sociais e a provisoriedade da realidade material e simbólica. **Serviço Social & Sociedade**, São Paulo, n. 113, p. 152–170, 2013. Disponível em: https://doi.org/10.1590/S0101-66282013000100007. Acesso em: 5 dez. 2024.

logias das ciências sociais são fundamentais para garantir a ética, o rigor, a validade e a relevância dos resultados de pesquisa. Elas orientam os pesquisadores na organização, coleta, análise e interpretação de dados de maneira ética e responsável, promovendo uma contribuição significativa e consistente para o desenvolvimento do conhecimento nas áreas sociais.

Neste texto, o nosso objetivo é apresentar os insights advindos de nossos estudos, inseridos no IRIS, nos campos de criptografia e proteção de crianças e adolescentes em ambientes digitais. Em razão disso, pensamos ser necessário adentrarmos nas metodologias adotadas tanto no estudo de varredura pelo lado do cliente, quanto no estudo sobre os discursos normativos e tecnológicos no MERCOSUL para proteção infantojuvenil em ambientes criptografados.

Assim, nossa metodologia para a pesquisa "*varredura pelo lado do cliente"* buscou dar atenção aos riscos e impactos do acesso excepcional à criptografia, com enfoque às implicações políticas e jurídicas associadas à segurança da informação e à proteção dos direitos humanos. Isso significa que, para atingir um nível de profundidade e confiabilidade científica, realizamos uma revisão sistemática da literatura, com o objetivo de investigar o estado da arte sobre o tema. A revisão incluiu uma seleção empírica de obras, avaliadas com base em critérios e procedimentos organizados.

A metodologia envolveu uma busca inicial pela palavra-chave "client-side scanning" na plataforma Google Acadêmico. Embora o termo tenha sido traduzido como "varredura pelo lado do cliente" no relatório, a pesquisa foi realizada em inglês devido à escassez de literatura relevante em português e à predominância dos debates nesse idioma, impulsionados pelas ferramentas anunciadas pela Apple. Foram encontradas 38 referências, das quais 3 foram excluídas por duplicação e 2 por acesso restrito.

Além disso, dois subconjuntos de obras foram obtidos a partir das referências bibliográficas de dois textos selecionados de forma discricionária: "Bugs in our Pockets: The Risks of Client-Side Scanning", de Abelson et al.[8], e "Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta", do Center For Democracy & Technology[9]. Esses textos foram escolhidos pela sua relevância no debate sobre alternativas à quebra de criptografia e pelas controvérsias relacionadas à varredura pelo lado do cliente. Todas as 68 referências citadas no primeiro texto foram selecionadas; e, dos trechos do segundo texto que abordavam especificamente a VPLC, foram eliminadas 2 referências, por repetição, somando-se 9 obras ao corpus: um subtotal de 77.

Ao total, 110 referências foram consideradas a partir dos critérios de pertinência temática e pertinência formal. Na seleção de quais delas seriam analisadas, primeiramente, dois pesquisadores decidiram, com mascaramento da opinião do colega, quais obras deveriam ser incluídas no estudo. Na sequência, um terceiro pesquisador deliberou somente no caso de discordâncias entre os pareceres dos dois primeiros, também sem saber quem havia emitido qual opinião. Foram excluídas referências não acadêmicas, como apresentações, artigos de opinião e notícias, por não constituírem material de validade científica. Ao final, 22 obras foram selecionadas, categorizadas e analisadas, com foco em

8. ABELSON, Hal e outros. Bugs in our Pockets: The Risks of Client-Side Scanning. arXiv preprint arXiv:2110.07450, 15/10/2021. https://arxiv.org/abs/2110.07450 . Acesso em: 4 dez. 2024.

9. CENTER FOR DEMOCRACY & TECHNOLOGY – CDT. **Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta**. Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 fev. 2022. Disponível em https://irisbh.com.br/publicacoes/abordagens-para-a-moderacao-de-conteudo-em-sistemas-com-criptografia-de-ponta-a-ponta/. Acesso em: 4 dez. 2024.

sua proposta, metodologia e abordagem sobre a varredura pelo lado do cliente.

Assim como em toda pesquisa científica, escolhas metodológicas resultam em limitações ao alcance do estudo. Neste caso, a principal se deve à escassez de literatura sobre o tema em português, ainda que o esforço de reunir e organizar as referências tenham superado essas limitações. O resultado final foi publicado em um relatório de pesquisa que permite uma análise aprofundada sobre o tema, considerando as principais abordagens acadêmicas e as implicações da varredura pelo lado do cliente, trazendo uma contribuição inédita para o campo.

Em relação ao estudo da pesquisa intitulada "*Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no* MERCOSUL"[10] a nossa metodologia focou na relação entre criptografia e proteção de crianças e adolescentes. A pesquisa envolveu a coleta das percepções de especialistas de cinco países: Argentina, Brasil, Paraguai, Uruguai e Venezuela. Também buscamos entender o estado atual da legislação, ou do debate legislativo, sobre criptografia e proteção infantojuvenil, além de investigar a existência de ferramentas digitais ou ações específicas para combater ou investigar a violência sexual contra crianças e adolescentes em ambientes criptografados. A análise se baseou em um marco teórico, 17 entrevistas semiestruturadas com especialistas e a identificação de normas jurídicas, vigentes ou em discussão, relacionadas aos temas centrais da pesquisa e suas intersecções.

Por fim, destacamos que a construção da ciência exige a superação do dogmatismo. Essa máxima, amplamente reconhecida por pesquisadores, reflete o próprio cerne do fazer científico: a constante busca por conhecimento embasado em procedimentos e metodologias rigorosas, sempre abertas a questionamentos. Contudo, tais questionamentos devem ser conduzidos com atenção às lacunas existentes e apresentar possibilidades de aprimoramento de forma estruturada e respeitosa.

Esse entendimento é parte integral da prática científica, que inclui o exame crítico de trabalhos preexistentes para identificar lacunas e explorar novos caminhos. Foi nesse espírito que desenvolvemos o projeto "Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no MERCOSUL"[10] e conduzimos a pesquisa sobre VPLC.[11]

RESULTADOS DA PESQUISA SOBRE VPLC

No relatório "Comunicações privadas, investigações e direitos: varredura pelo lado do cliente", revisitamos o cenário da varredura pelo lado do cliente, definida como grupo de técnicas para, em vez de realizar o escaneamento em servidores das empresas, escanear os dispositivos dos usuários, ou clientes, com o objetivo de identificar (por meio da análise de correspondência por semelhança entre identificadores, ou *hashes* do tipo perceptivo) o compartilhamento de materiais ilícitos (em especial conteúdo de violência sexual contra crianças e adolescentes) em ambientes criptografados.

Destacamos que VPLC consiste numa proposta tecnológica para reconhecer conteúdos que as plataformas pretendem adotar, e não numa funcionalidade já existente nos dispositi-

10. IRIS BH. **Segurança da Informação e Proteção de Crianças e Adolescentes: discursos e propostas regulatórias no Mercosul**. Disponível em: https://irisbh.com.br/projetos/seguranca-da-informacao-e-protecao-de-criancas-e-adolescentes-discursos-e-propostas-regulatorias-no-mercosul/. Acesso em: 4 dez. 2024.

11. PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente:** uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <bit.ly/3EAhEDF>. Acesso em: 04 dez.2024.

vos de comunicação. O que há hoje é a varredura pelo lado do servidor, analisando conteúdo na transmissão ou armazenado pelo intermediário do sistema de comunicação. O diferencial da VPLC seria a possibilidade de combate a conteúdos ilegais, em específico de violência sexual contra crianças e adolescentes, respeitando a privacidade do usuário e a criptografia de ponta a ponta.

A pergunta central da investigação foi: **como a literatura acadêmica vê a adequação da VPLC como meio investigativo em sistemas com criptografia forte sem mecanismos de acesso excepcional?** O estudo explorou riscos e desafios tecnológicos e jurídicos, organizou os principais pontos de defesa e crítica à proposta, e avaliou sua viabilidade.

Por meio de uma revisão sistemática, foram examinadas as críticas e controvérsias que cercam essa tecnologia, organizadas em duas dimensões: tecnológica e jurídica. Na primeira dimensão, os achados foram estruturados em quatro campos: funcionamento, eficácia, segurança e escopo. Já a segunda dimensão observou as repercussões da VPLC para quatro grupos de garantias jurídicas: privacidade e sigilo das comunicações; a presunção de inocência; segurança pública; e, por fim, proporcionalidade e necessidade.

No que diz respeito ao funcionamento da VPLC, observou-se que a tecnologia enfrenta barreiras significativas em razão das limitações de hardware dos dispositivos dos usuários finais. Por deslocar a atividade de comparação entre hashes – dos servidores das empresas provedoras para os aparelhos dos usuários finais – questões como capacidade de armazenamento e processamento, a desatualização do sistema, e mesmo a obsolescência do hardware comprometem a viabilidade da tecnologia.

/ TENTATIVAS TECNO-SOLUCIONISTAS NÃO PODEM SER SUFICIENTES PARA RESPONDER A DEMANDAS SOCIAIS TÃO COMPLEXAS COMO AS VIOLÊNCIAS SEXUAIS CONTRA CRIANÇAS E ADOLESCENTES /

/ OBSERVAMOS NA LITERATURA O RECEIO DE QUE AS TÉCNICAS DE VPLC REPRESENTEM UM RISCO DESPROPORCIONAL EM COMPARAÇÃO COM OS BENEFÍCIOS OBTIDOS /

Em termos de eficácia, dois pontos. Primeiro, conforme a literatura pesquisada, o uso de técnicas de *hash* perceptivo – propostas na vasta maioria das soluções de VPLC até então – necessita de uma base de hashes correspondentes ao conteúdo ilegal que se quer identificar para que possam funcionar, visto que dependem de uma comparação entre o material compartilhado pelos usuários e essa base original de hashes ilícitos. A composição dessas bases de hashes depende de denúncias iniciais e da subsequente constatação da ilicitude do conteúdo veiculado. Isto, por sua vez, gera preocupações dada a constatação de que conteúdos de violência sexual infantil – alvo de parcela significativa das soluções propostas de VPLC – são, na vasta maioria das vezes (84%), denunciados uma única vez.

Segundo, apontou-se que as preocupações na definição da sensibilidade das técnicas de VPLC a diferenças no conteúdo analisado independentemente do grau de sensibilidade definido no algoritmo. Níveis mais altos de sensibilidade fazem com que singelas alterações no conteúdo (recortes, ajustes de saturação, cor, entre outros) resultem na atribuição de hashes diferentes a conteúdos essencialmente idênticos. Por outro lado, níveis mais baixos de sensibilidade permitem que agentes mal-intencionados gerem falsos positivos de propósito, adulterando conteúdos inócuos de modo a alcançar hashes idênticos aos de conteúdos marcados como ilícitos, possibilitando a sobrecarga do sistema de comparação, ou a denunciação de pessoas inocentes com base em processos digitais.

Sobre a segurança, a literatura pesquisada apontou que as bases de hashes ilícitos podem ser manipuladas, ampliando os riscos de vulnerabilidades, uma crítica similar à feita contra a implementação de portas clandestinas (ou *backdoors*) em sistemas com criptografia. O risco é essas brechas serem usurpadas por terceiros não autorizados.

E em termos de escopo, das técnicas de VPLC, considerando a possibilidade de se ampliar conjunto dos tipos conteúdos rastreados, identificamos a possibilidade de abuso motivado por questões ideológicas, políticas, socioculturais, etc., tanto por parte de autoridades públicas quanto das próprias plataformas que as administram. Eventual interesse ilegítimo em localizar e repreender instâncias legítimas de circulação de conteúdo foi visto como um risco significativo, em especial para grupos já marginalizados e perseguidos. Assim, haveria uma quebra das expectativas de segurança da informação e liberdade de expressão afeitas ao uso da criptografia de ponta a ponta.

Na dimensão jurídica, o estudo ressaltou que a VPLC pode violar a privacidade e o sigilo das comunicações quando os resultados da comparação entre hashes pelo lado do cliente são compartilhados com o servidor. O procedimento é necessário para a verificação humana do material apontado como ilícito pelo algoritmo, a fim de evitar a punição de falsos positivos.

Também identificamos na literatura a preocupação de que o uso de técnicas de VPLC afete a prerrogativa constitucional e processual da presunção de inocência. A sua aplicação é direcionada a todos os usuários de uma dada plataforma, mal-intencionados ou não, o que resulta na filtragem de todo o conteúdo compartilhado por todas as pessoas, por padrão.

E no que se refere à proporcionalidade e à necessidade, observamos na literatura o receio de que as técnicas de VPLC representem um risco desproporcional em comparação com os benefícios obtidos, e desnecessário em relação ao objetivo almejado. Todas as barreiras tecnológicas apontadas ao longo da investigação fragilizam o argumento a favor da eficácia da VPLC no combate aos ilícitos que seu uso pretende repreender.

Além das dimensões tecnológicas e jurídicas, houve preocupações adicionais em termos sociológicos, pois a VPLC combate a disseminação de conteúdo ilícito, mas não elimina a fonte criadora dos materiais e econômicos, pelos custos necessários para cumprir com a obrigação legal de filtragem em massa de conteúdos por parte das plataformas impedirem a atuação de plataformas de pequeno porte, gerando mais concentração em favor dos grandes provedores de aplicação de Internet.

Assim, a partir da análise empreendida por meio da revisão sistemática da literatura, foi possível entendermos que as técnicas de VPLC para o combate à disseminação de conteúdos ilícitos em ambientes criptografados se mostram uma medida inadequada por diferentes motivos. Não apenas as soluções de VPLC descritas até o momento apresentam diversas falhas e brechas de um ponto de vista tecnológico, como também representam um enfraquecimento de diversas garantias jurídicas consagradas como direitos fundamentais – tais quais o direito à privacidade, à liberdade de expressão, à presunção de inocência, entre outros. Nesse sentido, a VPLC consiste em ferramentas potencialmente tão danosas quanto à própria quebra da criptografia forte ou a inserção de portas clandestinas para o chamado acesso excepcional.

PROTEÇÃO DE CRIANÇAS E ADOLESCENTES ONLINE E A VPLC

Como já aqui mencionado, no campo político e jurídico, a proteção de crianças e adolescentes em ambientes digitais frequentemente entra em conflito com a defesa da segurança tecnológica, especialmente no que diz respeito à criptografia. Embora a criptografia possa ser identificada, a partir

de alguns discursos oficiais, enquanto dificultadora nas investigações criminais, ela também é crucial para garantir a segurança, a privacidade e os direitos fundamentais das crianças e adolescentes, como a liberdade de expressão e o desenvolvimento da personalidade. O projeto *"Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no MERCOSUL"*, do IRIS, analisou como essa disputa se manifesta nos países dessa região, investigando a relação entre a criptografia e a violência sexual online, por meio de entrevistas com especialistas e da análise de normas jurídicas e artefatos tecnológicos voltados para a proteção desses jovens.

Os resultados indicam que há lacunas significativas nas abordagens normativas e tecnológicas para a proteção de crianças e adolescentes no ambiente digital, especialmente contra a violência sexual online. Embora os países do MERCOSUL sigam as diretrizes da Convenção Sobre os Direitos da Criança da ONU, a implementação prática dessas normas é desigual, com o Brasil sendo o país com mais debates identificados sobre os temas. Além disso, as discussões legislativas são limitadas e há pouca participação ativa de crianças e adolescentes nesses espaços, o que impede o pleno reconhecimento de seus direitos como sujeitos de direito.

Ainda, entre os principais achados, destacamos:

< A > ausência de legislação específica sobre proteção de crianças e adolescentes em ambientes digitais, incluindo a violência sexual online;

< B > debates legislativos escassos e sem a participação dos afetados pelas políticas públicas nessa área;

< C > falta de normas sobre criptografia, com o Brasil realizando discussões no campo, mas sem resultados concretos;

< D > inexistência de ferramentas tecnológicas específicas ou falta de conhecimento sobre elas.

Além disso, a falta de uma regulação específica acarreta riscos variados, que vão desde a criação de normas protetivas que podem exigir vulnerabilidades tecnológicas, resultando em uma atuação maior dos atores do sistema de justiça criminal e de uma aposta maior na criminalização enquanto única forma de enfrentamento a essas violências, até o risco de regulamentações que, de forma desnecessária e desproporcional, restrinjam os direitos de cidadania, privacidade e liberdade de expressão de crianças e adolescentes no ambiente digital. Existe também a ameaça de sobreexposição a conteúdos inadequados, devido à ausência de medidas adequadas de segurança tecnológica.

Aproximando nossos dois estudos, podemos identificar alguns pontos de risco que merecem atenção e que afastam o debate de uma mera polarização:

< A > o uso de VPLC pode fragilizar significativamente o desenvolvimento contínuo de políticas de privacidade que afetam os direitos de crianças e adolescentes;

< B > os softwares que permitem o rastreio de conteúdo, podem ser utilizados para identificar e perseguir pessoas LGBTQIA+;

< C > a existência de risco aos pais e responsáveis, uma vez que a tecnologia não identifica propósito de imagem. As-

sim, responsáveis que registram, armazenem ou encaminhem fotos que contenham nudez infantil, poderiam ser penalizados.

REFLEXÕES SOBRE AS LACUNAS NA PESQUISA DE VPLC

Dois anos após a realização do relatório de VPLC, é possível identificar novas dinâmicas no campo. O aumento da produção científica sobre o tema sugere que uma nova investigação, mesmo utilizando a mesma base metodológica, como a revisão sistemática, poderia trazer novos *insights* ou reflexões críticas a conclusões anteriores.

Outra perspectiva a ser explorada é a utilização de técnicas metodológicas complementares para análise das tecnologias e seus impactos político-sociais. A revisão sistemática, apesar de ser uma das técnicas mais rigorosas para revisões e análises qualitativas, apresenta limitações relacionadas ao escopo do material analisado. Caso não haja produção científica suficiente sobre o tema por pesquisadores, organizações ou órgãos nacionais, suas contribuições acabam não sendo consideradas, restringindo o alcance da análise.

Além disso, a revisão sistemática possui uma característica distintiva: seus resultados são obtidos exclusivamente a partir do material revisado. Isso implica que as conclusões apresentadas refletem uma leitura sobre a literatura analisada sobre o objeto de estudo, buscando se distanciar dos vieses e narrativas externas ao processo metodológico. No caso de nossa investigação, as conclusões sobre o VPLC são delimitadas pelo que a literatura coletada abordou sobre o tema, sem espaço para interpretações que extrapolem os dados analisados. Assim, a lacuna da literatura acadêmica em português se revela uma limitação. Ademais, é importante destacar que a revisão sistemática, diferentemente de outras técnicas de revisão, apresenta resultados exclusivamente, ou em maioria absoluta, baseados nos insumos provenientes de sua aplicação. Isso implica fundamentar as análises e conclusões nos dados extraídos desse método. Portanto, as conclusões da nossa investigação apresentam um recorte bem definido: o que a literatura científica analisada aborda sobre o VPLC.

Além disso, somente foi possível analisar as obras acadêmicas que tratavam das técnicas de VPLC que já foram descritas publicamente. Escapa à capacidade da pesquisa qualquer eventual existência de implementações secretas ou de propostas teóricas em teste, mas ainda não divulgadas, seja pelas autoridades públicas, ou pelas plataformas digitais.

Conquanto a metodologia adotada ofereça sistematização e consistência aos argumentos analisados, notou-se que a limitação a obras de caráter acadêmico não consegue abarcar os debates mais intensos, no calor do momento, que acontecem inevitavelmente fora do universo de artigos científicos e estudos investigativos. Essa restrição inerente acaba exigindo fontes adicionais sobre a cronologia dos acontecimentos, reações pela imprensa e eventuais pronunciamentos oficiais.

Ao longo do estudo realizamos revisão bibliográfica extensiva sobre os debates em torno da proposta de varredura pelo lado do cliente e de suas repercussões sociais, jurídicas e políticas. Desejamos que nossos resultados sirvam como base para o aprofundamento das discussões em trabalhos futuros. Por exemplo, pode-se indagar sobre a implementação exclusiva em favor do interesse do cliente, considerando a distinção a ambientes adversariais, quando a ferramenta deveria operar contra o interesse do proprietário do dispositivo. Outras propostas concretas de VPLC podem ser consideradas, desde

que haja compromisso com medidas que cuidem das questões apontadas em abordagem ampla, por exemplo, por meio de sistemas com código fonte integralmente aberto.

Por fim, reconhecemos, ainda, que uma possibilidade promissora para dar continuidade ao projeto seria incorporar ao debate as perspectivas do multissetorialismo (característico do ecossistema da governança da Internet) e do Sistema de Garantia de Direitos de Crianças e Adolescentes (SGDCA). Essa abordagem poderia enriquecer a compreensão dos impactos das tecnologias digitais no contexto da proteção de crianças e adolescentes, ampliando o diálogo com atores de diferentes setores e promovendo análises mais abrangentes.

CONCLUINDO

Neste breve artigo, buscamos apresentar o andamento e resultados da pesquisa intitulada "Varredura pelo lado do cliente: uma revisão sistemática", publicada no ano de 2022 pelo IRIS, e da nossa pesquisa "Segurança da Informação e Proteção de Crianças e Adolescentes: Discursos e Propostas Regulatórias no MERCOSUL". Prezando pela cientificidade das pesquisas que realizamos, apontamos a metodologia que seguimos para chegarmos nos pontos e insights apresentados e, ademais, pontuamos as lacunas existentes em nosso relatório de VPLC - naturais à pesquisa acadêmica, já que a completude dos debates não se esgota em apenas um trabalho.

Ainda, pontuamos fortemente nosso posicionamento, enquanto um instituto inserido e defensor de uma sociedade democrática e apoiadora do debate multissetorial, de que criamos e nos colocamos favoráveis a existência de espaços de pensamentos científicos divergentes e com diferentes atores sociais: a escuta ativa nos campos de governança da internet nos demonstra, constantemente, sua eficácia na formulação de caminhos possíveis. Contudo, os debates necessitam ser estabelecidos com diálogo ético, com narrativas embasadas em ideias, teorias e vivências que vão além de convicções pessoais.

Cabe ainda destacar que tentativas tecno-solucionistas não podem ser suficientes para responder a demandas sociais tão complexas como as violências sexuais contra crianças e adolescentes; apostar unicamente em tais ferramentas é inclusive um caminho de risco aos direitos humanos infanto juvenis, uma vez que podem representar esquivos de responsabilizações sociais, de agentes e atores.

As conclusões acima, além de poderem ser debatidas e cientificamente questionadas, em nada se aproximam da ideia polarizada de que, ou se defende, por um lado, a criptografia forte, ou se defende, por outro, a proteção de crianças e adolescentes. Pelo contrário, ela estimula o pensamento crítico e incita ações concretas e transparentes por parte das instituições de segurança pública, em conjunto com o setor acadêmico e demais setores, em prol da proteção deste grupo social. A proteção de crianças e adolescentes em ambientes digitais é tema central e, assim, merece ser tratada com base em conhecimento cientificamente embasado e ações transparentes.

13.

O USO DE *SPYWARE* PELO ESTADO: LIMITES E POSSIBILIDADES[1]

Yuri Corrêa da Luz

1. Este artigo foi adaptado a partir de palestra realizada no VII Congresso Direitos Fundamentais e Processo Penal na Era Digital, promovido pelo InternetLab em agosto de 2023, com o auxílio de Camilly Vitória Silva.

1. INTRODUÇÃO

Embora pareça excessivamente técnico, o debate sobre a admissibilidade, ou não, do uso de *spywares*, por parte do Estado, tem como pano de fundo uma discussão mais ampla: a relação entre Direito Penal e tempo. É uma característica fundamental de novas tecnologias seu desenvolvimento acelerado, em um passo absolutamente mais intenso do que o desenvolvimento da legislação. A tecnologia, em outras palavras, avança sempre muito mais rápido do que o Direito, e discutir o quanto ele consegue regulá-la passa por reconhecer que, invariavelmente, toda lei que pretender abarcar um campo tecnológico terá de lidar com uma realidade cambiante e com o risco, sempre presente, de chegar tarde demais, tornando-se obsoleta diante de um contexto que já se alterou. Essa percepção é fundamental porque deve orientar as nossas exigências a respeito de quão específica deve ser uma lei para que ela seja considerada um marco regulatório legítimo de dada tecnologia: caso exijamos um alto grau de especificidade, colocando como condição de legitimidade de nosso moroso processo legislativo a entrega de normas que abordem tecnologias concretas, estaremos diante, possivelmente, de uma tarefa de Sísifo, que jamais poderá ser cumprida a contento. Para evitar isso, é necessário que olhemos menos para as particularidades de cada tecnologia regulada, e mais para os direitos que por elas podem ser afetados, pensando a partir deles o que precisa ser proibido, o que precisa ser permitido com diversas condicionantes, quais condicionantes seriam estas, e quais deveres devemos impor aos atores envolvidos em sua implementação.

Nesta sede, pretendo discutir os limites e as possibilidades do uso de *spyware*, por parte do Estado, tendo como pressuposto essa percepção. Inicio com algumas definições que me parecem fundamentais para alinhamento sobre o que são *spywares*, quais são seus usos, preparando, com isso, o terreno para discutir quais são os direitos que eles podem afetar, e em que circunstâncias. Na sequência, reconstruo brevemente as duas posições principais que tratam desse debate sobre a admissibilidade, ou não, do uso de *spywares*, no Brasil, e aponto o que me parecem ser deficiências de cada uma delas. Ao final, procuro oferecer uma posição alternativa - que, a meu ver, trata esse tema com a complexidade que ele requer.

2. DEFINIÇÕES, ESPÉCIES E USOS DE *SPYWARES*

Em linhas gerais, *spywares* nada mais são do que uma espécie de *malware* que permite a quem o usa explorar deficiências de uma dada tecnologia. Mirando em vulnerabilidades pré-existentes de programas, aplicações e dispositivos eletrônicos, quem mobiliza *spywares* tem por objetivo acessar e obter determinados dados que possam estar armazenados em um computador, em um dispositivo eletrônico, em um programa, ou mesmo monitorá-los.

Esse tipo de exploração de vulnerabilidade, quando promovida por um particular, pode mesmo configurar o crime de infiltração de dispositivo eletrônico, tipificado no art. 154-A do Código Penal. Mas nos últimos anos passou-se a discutir a possibilidade de que tal exploração seja feita pelo Estado, de forma lícita, desde que devidamente regrada. Esse chamado "*hacking* estatal",[2] de fato, ganhou defensores e vem sendo apresentado como uma alternativa menos

2. Há quem defina esses recursos como hacking governamental, o que me parece um termo ruim, pois nem todo Estado que promove investigação e persecução penal é parte do governo em sentido estrito. A noção de hacking governamental, assim, sugere um tipo de espionagem com contornos muito ligados a grupos políticos de ocasião, colocando na sombra seu uso por órgãos e instituições de Estado, com independência e expertise técnico.

intrusiva, para direitos fundamentais, do que outras formas de produzir provas em ambiente digital (como, por exemplo, como alternativa à criação de *backdoors* em aplicações de mensageria, o que cria uma série de vulnerabilidades que podem impactar todos seus usuários, e não apenas aqueles que estão sob investigação concretamente).

É importante entender, de qualquer modo, que *spywares* não são meios *uniformes* de investigação digital. Há uma grande pluralidade de *spywares*, não somente de marcas diferentes (produzidos por empresas diferentes), mas sobretudo que apresentam *funcionalidades* diferentes. Alguns *spywares* servem para acessar remotamente determinado dado *armazenado* no dispositivo, outros servem para monitorar dados *em fluxo* de um determinado dispositivo, e outros, ainda, muito mais sofisticados e de alto custo para adquirir, permitem ter acesso à câmera de um dispositivo, ao áudio que é captado por uma determinada funcionalidade, por um determinado aparelho. Hoje em dia, há até mesmo *spywares* que permitem uma "exploração sem click" ou "com click zero", autorizando quem os usa a acessar um dispositivo e praticamente operar esse dispositivo sem qualquer contribuição do seu usuário, ou seja, à revelia do seu usuário (por exemplo, entrando em determinado site dentro do aparelho, conseguindo manter contato com pessoas de um determinado dispositivo móvel sem que o possuidor desse móvel tenha conhecimento a respeito disso).

Perceber que estamos diante, portanto, de um *conjunto plural de funcionalidades*, cada qual com sua vocação é de enorme relevância, pois cada uma dessas utilidades tem impactos distintos sobre direitos fundamentais, e é determinante para a discussão sobre se e em que termos elas podem, ou não, ser exploradas pelo Estado.

3. AS DUAS PRINCIPAIS POSIÇÕES SOBRE A (IN)ADMISSIBILIDADE DO USO DE *SPYWARE*, PELO ESTADO BRASILEIRO, E SUAS DEFICIÊNCIAS

No debate sobre admissibilidade, ou não, do uso de *spyware* pelo Estado brasileiro, duas posições são defendidas com maior destaque.

A primeira sustenta que não seria admissível, ao Estado, usar de *spywares* porque não haveria uma lei específica autorizando-o especificamente a mobilizar essas tecnologias. Esse argumento, em linhas gerais, recorre a uma compreensão extremada do princípio da legalidade. Segundo seus partidários, a lei precisaria sempre prever, de forma específica, quais são os *meios* de produção de prova à disposição dos órgãos de investigação e persecução. Nessa linha, assim como a Lei nº 9.296/1996 foi especificamente pensada para autorizar o meio *interceptação telefônica*, e os arts. 240 e seguintes do Código de Processo Penal foram especificamente pensados para autorizar o meio *busca e apreensão domiciliar e pessoal*, seria necessário que uma lei específica fosse editada para autorizar o uso de tecnologias como *spyware*. E como nós não temos, hoje, essa lei, ao Estado estaria vedado mobilizá-las.

Essa posição parece ser o que está na base, por exemplo, da decisão proferida pelo Superior Tribunal de Justiça no julgamento do Habeas Corpus nº 99.735-SC, da relatoria da Min. Laurita Vaz. Na ocasião, estava em discussão a possibilidade de a polícia usar provas colhidas a partir *do "espelhamento" do WhatsApp* de um investigado. Em termos gerais, a Polícia havia apreendido o aparelho celular de um investigado e acessando sua conta de Whatsapp, promoveu um acesso espelhado, via Whatsapp Web, das mensagens por ele trocadas. Nesse caso, é verdade que sequer se era uma tecnologia

nova, mas o modo como o espelhamento foi promovido se assemelha a um uso de *spyware*: explorou-se uma vulnerabilidade (no caso, porém, emergida com a apreensão de um celular não bloqueado), para se acessar os conteúdos tanto armazenados quanto em fluxo daquela conta. O Superior Tribunal de Justiça foi chamado a apreciar a legalidade das provas obtidas por meio dessa técnica e, entre outros argumentos, entendeu que se estava diante de um meio "híbrido" de produção de prova, por não consistir nem em uma quebra telemática (já que não se estava acessando apenas os dados armazenados no aparelho), nem uma interceptação telemática (já que, naquele contexto, também se estava acessando os dados armazenados, além dos em fluxo). E diante disso, sob a percepção de que não haveria previsão legal específica para autorizar o uso desse meio "híbrido", anulou-se a prova a partir dele produzida.

Em oposição a isso, uma segunda posição diversa, sustenta que seria admissível o uso de *spyware*, pelo Estado, bastando, para tanto, que ele estivesse sujeito a um controle independente, notadamente o controle judicial. Quem advoga essa posição baseia-se, por exemplo, no art. 3º-B do Código de Processo Penal, que, ao introduzir a figura do juiz de garantias, atribuiu-lhe um papel de decidir sobre requerimentos diversos (como de quebra telemática, de interceptação telefônica, etc.), e em sua alínea "e", ao cabo, o papel de decidir sobre *"outros meios de obtenção da prova que restrinjam direitos fundamentais do investigado"*. Segundo essa posição, haveria, aqui, uma previsão geral autorizadora de uma produção de provas por quaisquer meios, bastando, para garantir sua legitimidade, que o Judiciário fizesse um crivo prévio, isso é, que um juiz imparcial avalie o cabimento, a proporcionalidade, a justa causa da obtenção visada pelos órgãos de persecução.

/ A PRÓPRIA LEI ESTÁ RECONHECENDO QUE OS MEIOS A SEREM EMPREGADOS, PARA EFETIVAÇÃO DE UMA INTERCEPTAÇÃO, ESTÃO INEVITAVELMENTE EM ABERTO /

Ambas as posições - tanto a que sustenta a plena inadmissibilidade aduzindo que "não há autorização legal específica para o uso dessa tecnologia no Brasil", quanto a que sustenta a plena admissibilidade aduzindo que "há autorização genérica no Código de Processo Penal, bastando controle judicial do uso" - parecem-me equivocadas.

De um lado, aqueles que exigem uma previsão legal específica para o uso de *spyware* pelo Estado brasileiro ignoram que o processo legislativo jamais conseguirá acompanhar a velocidade do desenvolvimento, de modo que, quando finalmente uma lei for editada para autorizar o uso de dado recurso específico, é provável que ela chegue num momento em que ele sequer se mostre mais útil. A exigência de autorização legal muito específica, ao cabo, coloca-nos em um cenário em que a produção de prova, por aquela via, pode sequer mais ser necessária, para além de ignorar que um meio de produção de prova, se afeta indevidamente direitos fundamentais, não deixa de ser ilegal por ter sido autorizado judicialmente.

De outro lado, aqueles que sustentam que *spywares* poderiam ser usados em qualquer situação, bastando que o Estado esteja previamente lastreado em uma autorização judicial concreta, ignoram que este tipo de controle, embora necessário, é ainda assim muito insuficiente, principalmente tendo em vista o tipo de intervenção em direitos fundamentais implicada nessas tecnologias.

Diante disso, na sequência pretendo estabelecer algumas linhas mestras de uma posição alternativa, que talvez ofereça um olhar mais sofisticado sobre as possibilidades e os limites que devem ser observados para o uso de *spywares*, pelo Estado, no marco normativo vigente em nosso país.

4. PROPOSTAS E PREMISSAS PARA UMA REGULAMENTAÇÃO ADEQUADA PARA O USO DE *SPYWARE*.

Uma posição adequada, nesse debate, deve se afastar desses dois extremos e tentar se construir em um balanço entre o interesse de produzir prova por meios digitais e a necessária garantia de direitos fundamentais de investigados. Nesta sede, enumero três delas.

A primeira das premissas parte da percepção de que o foco da avaliação quanto ao cabimento, ou não, de um meio de produção de prova não pode ser a *tecnologia específica* nele embutida. Muito pelo contrário, devemos olhar, antes, para *os direitos fundamentais vigentes*, sobretudo para as inviolabilidades constitucionais que estão, digamos, em tensão com o meio de prova que se pretende mobilizar. Se adotarmos esse olhar, de partida percebermos que a Constituição é em larga medida *neutra* do ponto de vista tecnológico. Em outras palavras, ela não prevê autorização para uso da tecnologia A ou B, mas sim *esferas de inviolabilidade*, concreções de direitos fundamentais que, para o constituinte, derivam de dimensões das vidas dos cidadãos consideradas importantes e, portanto, dignas de proteção. Mais ainda, ao prever quais são essas esferas de inviolabilidade, a Constituição, em alguns casos, chega mesmo a delinear quando sua relativização é admissível, e quando não o é.

Essa mudança de foco é relevante porque, se a Constituição não fala de meios tecnológicos específicos, mas sim de esferas de inviolabilidade, um debate sobre a admissibilidade, ou não, do uso de *spyware* pelo Estado passa a poder ser feito em outros termos. Não se pergunta, nessa chave, se dada tecnologia tem seu uso previsto em lei ou não, mas se seu uso

tensiona ou mesmo viola, do ponto de vista constitucional, alguma esfera de inviolabilidade ou não.

Um exemplo permite tentar concretizar essa premissa. Pensemos em um *spyware* cujo uso permite *capturar*, remotamente, dados que estão armazenados em um dispositivo eletrônico, como em um computador. Imaginemos, ainda, que, em relação a um investigado específico, o que os órgãos de persecução pretendem é usar desse *spyware* para tentar capturar dados que estão em uma pasta de seu computador, a qual está vinculada a um serviço de nuvem que funciona com sincronização automática nativa - serviço de nuvem este que, contudo, é controlado por um provedor estrangeiro que não responde a ordens judiciais brasileiras de entrega. Nesse contexto, pergunta-se não sobre se há previsão legal para o uso de *spywares* no país, mas para qual é a inviolabilidade implicada no caso, leva-nos a reconhecer que está em jogo o art. 5º, inciso XII, que prevê que o sigilo de dados é inviolável, podendo, porém, ser relativizado por ordem judicial na forma da lei para fins de investigação criminal, instrução de processo penal. Ora, se o Estado, como investigador, observa esses parâmetros do art. 5º, inciso XII, não importa se o acesso aos dados visados está sendo feito por meio de um *spyware* (ou seja, por uma funcionalidade que acessa remotamente o conteúdo desta pasta), ou se por meio de uma ordem de entrega direcionada ao provedor de aplicação que tem uma cópia desses dados em nuvem. Do ponto de vista jurídico-constitucional, é indiferente qual a tecnologia utilizada: observados os parâmetros de relativização legítima da inviolabilidade implicada, deve-se admitir o acesso pretendido, independentemente do meio tecnológico que o viabiliza.

Imaginemos, agora, um outro exemplo, envolvendo o famigerado *spyware* Pégasus. O Pégasus é uma funcionalidade produzida por uma empresa israelense, a NSO Group, que permite a quem o usa ingressos absolutamente graves na esfera dos cidadãos. Para além do acesso a dados armazenados, essa tecnologia franqueia acesso à câmera e ao microfone de dispositivos eletrônicos do alvo, e mesmo permite monitorá-lo ao vivo, coletando dados de localização, analisar *pari passu* as páginas que ele consulta e as conversas que trava etc. Se formos pensar esse exemplo à luz do marco constitucional implicado, teremos, aqui, uma enorme dificuldade de, na Constituição, encontrar respaldo para esse tipo de intervenção. Porque esse tipo específico de *spyware* não está somente acessando dados (em providência típica de quebra de sigilo de dados armazenados), ou mesmo monitorando dados em fluxo daquele dispositivo (em providência típica de interceptação telemática de dados em fluxo), algo que poderia estar autorizado, observados os parâmetros do art. 5º, inciso XII, da Constituição. Muito além, está até mesmo monitorando conversas que estão acontecendo *inclusive fora do ambiente digital* (pense-se, aqui, na capacidade de se captar o áudio do ambiente off-line em que está o aparelho alvo do Pegasus), incidindo, assim, sobre esferas muito mais íntimas da pessoa, não amparadas pelo espectro de relativização legítima da referida inviolabilidade constitucional.

Alguém poderia alegar que esse tipo de monitoramento off-line, se não pode se legitimar pela inviolabilidade de sigilo de dados, talvez pudesse se legitimar pela inviolabilidade de domicílio, prevista no art. 5º, inciso XI, da Constituição. É verdade que esse dispositivo normativo prevê que o domicílio é inviolável, mas também prevê que essa inviolabilidade pode ser relativizada, sendo essa a base autorizadora de medidas de busca e apreensão. Ocorre que, para que tal relativização seja legítima, uma série de requisitos devem ser observados: a

polícia pode entrar em residências apenas em determinados horários (salvo em caso de flagrante delito), e mais do que isso não pode, a princípio, fazer isso em segredo (trata-se de uma percepção de que a casa é uma espécie de santuário da pessoa, e que o Estado, quando presente, precisa estar acompanhado de quem domina aquele espaço). Analisada à luz da inviolabilidade domiciliar, o que o Pegasus faz é algo absolutamente desproporcional, porque envolve um ingresso do Estado, na vida privada do cidadão, em qualquer horário, e em segredo, sem que dono da casa sequer saiba que está sendo alvo de uma medida intrusiva. Medidas que jamais estariam legitimadas por uma busca residencial, como a captação de imagens de uma pessoa nua ao sair do banho, ou em qualquer outro contexto íntimo, está no escopo de providências tecnicamente possíveis para esse *spyware* específico. É por isso não encontrar respaldo no marco constitucional das inviolabilidades que estão sendo implicadas ali, e não por não haver lei prevendo o uso específico dessa tecnologia, que o uso do Pegasus deve ser entendido como inadmissível.

A segunda premissa que considero fundamental nesse debate sobre admissibilidade, ou não, do uso do *spyware* pelo Estado brasileiro envolve reconhecer que, embora tais tecnologias sejam diferentes entre si, todas elas implicam uma interferência razoável em direitos fundamentais, e por isso, uma prévia autorização judicial é necessária, mas insuficiente como forma de controle.

É evidente que, no manejo de tecnologias que permitem acessar dados, imagens e mesmo vídeos pertinentes à nossa vida privada, um controle judicial é importante. Afinal, é por meio dele que se torna possível avaliar se a qualidade da prova que está sendo apresentada pela Polícia ou pelo Ministério Público atende parâmetros razoáveis a justificar a afetação de direitos do alvo. Contudo, não se pode perder de vista que, ao lado desse crivo judicial, a própria legislação *vigente* prevê uma série de outras balizas objetivas, que devem nortear a todos, e inclusive o juiz ou a juíza da causa, nessa avaliação.

A título de exemplo, para a medida de interceptação telefônica, a Constituição indica que, além de prévia autorização judicial, ela precisa ser mobilizada exclusivamente em favor de investigações criminais (vedando, portanto, seu uso para apurações cíveis). Não bastasse, o art. 2º da Lei nº 9296/1996 prevê que apenas poderá haver interceptação para investigação de crime sancionado com reclusão. Desses e outros dispositivos, hoje em vigor, é possível, portanto, derivar parâmetros que, ao lado do mero controle *judicial* de standard probatório, garantem um controle *democrático* a esse tipo de atuação dos órgãos de persecução penal, uma vez que definidos pelo legislador legitimado e eleito pelo povo.

Disso deflui que, se focamos nos direitos fundamentais potencialmente implicados por um meio de produção de prova, e analisamos os marcos normativos que delineiam hipóteses de sua relativização legítima, existem, já hoje, balizas objetivas, previstas na legislação, para analisar a admissibilidade, em cada caso concreto, do uso de *spyware* por parte do Estado. Isso não significa, frise-se, que um diploma legal que tratasse exclusivamente de *spyware*, como vem sendo elaborado em outros países, seja indesejável, sobretudo se pensado como marcos amplos, principiológicos, e não comprometido com um regramento de tecnologias específicas, que rapidamente podem se tornar obsoletas. Significa, porém, que um tal diploma legal parece dispensável, se formos capazes de observar que o que importa, sempre, é partir dos direitos implicados em cada caso, e analisarmos quais são os marcos normativos já vigentes que devem balizar a análise de cabimento,

ou não, do uso de *spyware* concretamente pretendido em uma investigação.

Para concretizar esse raciocínio, imaginemos que a Polícia pretende se valer de um *spyware* que permite monitorar dados em fluxo em um determinado aplicativo de mensagens. Esse tipo de tecnologia, ao fim e ao cabo, nada mais faz que tensionar uma inviolabilidade de sigilo de dados, de forma análoga à operada por uma interceptação telemática. Nesse passo, observando-se o art. 5º, inciso II, e os parâmetros legais previstos na Lei nº 9296/1996, o juiz ou a juíza, ao analisar uma representação de uso de *spyware* para essa finalidade específica, deverá crivar não apenas o standard probatório dos elementos apresentados, mas também se balizar pelos parâmetros dos citados diplomas normativos que regem a interceptação telemática, e, se todos estiverem forem atendidos, não parece haver razão para considerar a medida inadmissível.

A reforçar essa percepção, vale notar que o art. 4º da Lei nº 9296/1996 denota sua pretensão de ser tecnologicamente neutro, ao prever que "o pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, *com indicação dos meios a serem empregados*". Aqui, a própria lei está reconhecendo que os meios a serem empregados, para efetivação de uma interceptação, estão inevitavelmente em aberto, e que precisam ser, claro, explicados, para o juiz ou a juíza, em seus contornos concretos e em suas capacidades de tensionamento de direitos fundamentais, mas não precisam ser parte vinculados a uma tecnologia A ou B.

Em uma outra frente, a mesma lógica pode ser aplicada à análise de admissibilidade do uso de um *spyware* que permite invadir um aplicativo e garantir, aos investigadores, uma interação com os contatos de seu titular. Nessa hipótese, estamos diante de uma situação em que há uma interação *ativa*, por parte dos investigadores, com alguns contatos do alvo, de modo que se mostra inviável sua legitimação à luz das balizas próprias da interceptação telefônica ou de dados. Contudo, tal situação encontra similitude patente com a de i*nfiltração*, em organização criminosa, regrada pelos arts. 10 e seguintes da Lei nº 12.850/2013. Assim, apresentado pleito de autorização de uso de tal tecnologia, deve ser possível, ao juiz ou à juíza, avaliar sua admissibilidade à luz dos parâmetros objetivos da Lei nº 12.850/2013, atendendo, com isso, a essa segunda premissa, de controle judicial e democrático necessário à legitimação destes meios de produção de prova.

Uma terceira e última premissa passa por reconhecermos que deve haver não apenas um controle *ex ante*, por parte do Judiciário (de avaliar a justa causa, de observar parâmetros legais pertinentes, ainda que por analogia etc.), mas também alguma forma controle *ex post*, sobre a autorização e a implementação dessas medidas. Ou seja, é preciso discutirmos e construirmos - em cada caso concreto, por indução do juiz ou da juíza que autorizou a medida, mas também via regramentos como resoluções do Conselho Nacional de Justiça, que envolvam outros atores e a sociedade civil – protocolos para garantir que o uso de *spyware* específico foi implementado de maneira legítima, isso é, se depois de autorizado ele não foi objeto de abuso. Isso repercute, concretamente, em um necessário detalhamento do *caminho da implementação dessas medidas*, que deixe registrado, para análise posterior, o que foi guardado, em que termos foi guardado, se houve descarte de produção de dados que não eram úteis à investigação, em que termos que esse descarte se deu, se houve preocupação com a higidez da cadeia de custódia etc. Em suma, há de se criar formas de garantir também um controle ex *post*.

Essas três premissas, que poderiam ser detalhadas em outra sede, permitem construir, a meu ver, uma posição mais sofisticada no debate sobre a admissibilidade, ou não, do uso de *spyware* por parte do Estado, que garanta, de um lado, a preservação de direitos fundamentais que podem ser implicados por esse tipo de tecnologia, mas, de outro, que não impede o Estado de acompanhar o desenvolvimento tecnológico e produzir investigação consentânea com o estágio de desenvolvimento de seu tempo.

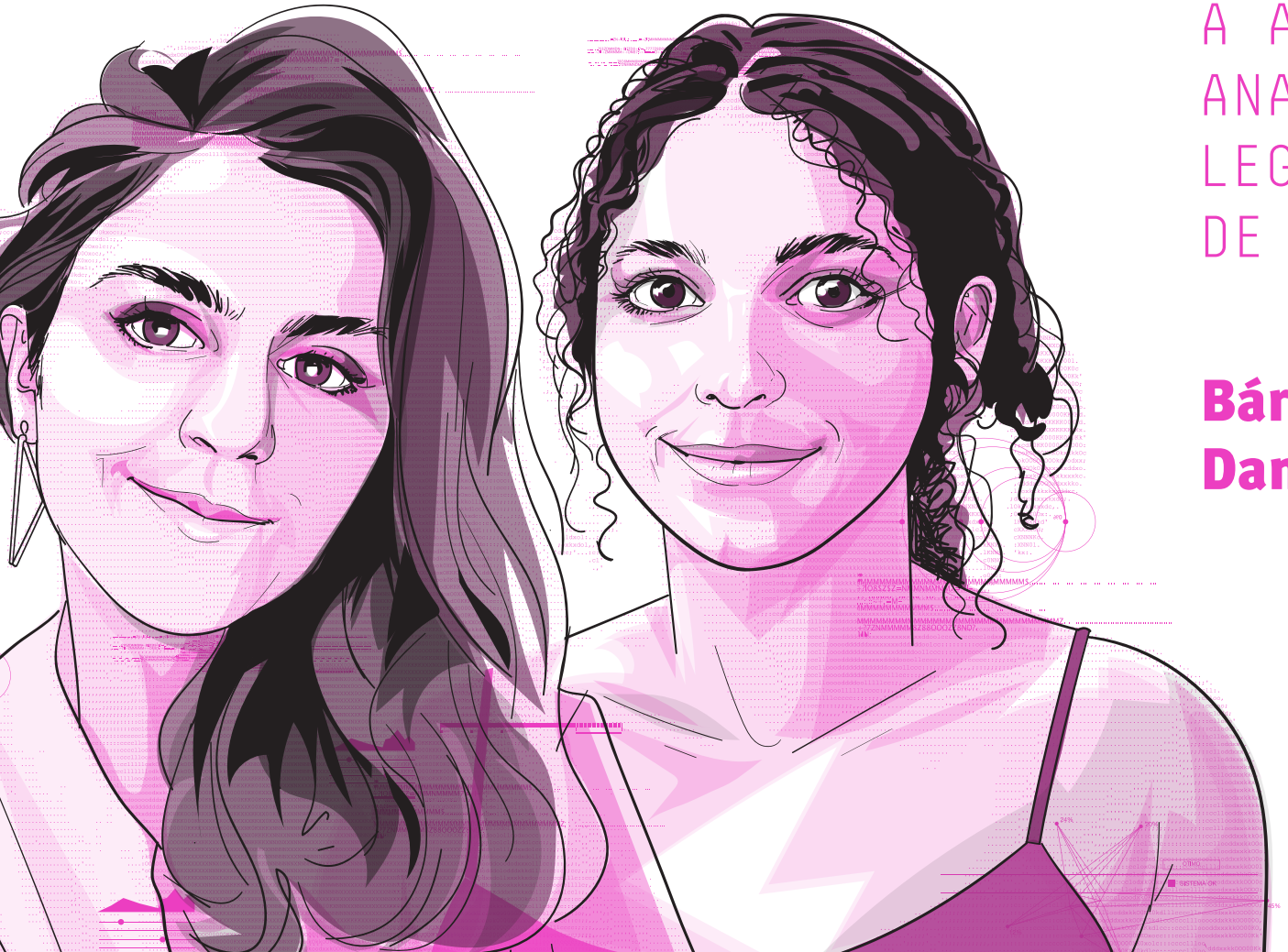
5. CONCLUSÃO

Uma última observação, de qualquer forma, faz-se necessária: todo o aqui defendido, essas três premissas que consubstanciam uma série de controles sucessivos, *ex post* e *ex ante*, a cargo de diversos atores, deixam claro que o uso de s*pyware* apenas pode ser legítimo, no marco normativo vigente, se for objeto de muitos crivos e de muitos cuidados em sua aplicação.

Neste marco vigente, portanto, esse tipo de tecnologia apenas pode ser legitimamente utilizado como *alternativa a outros meios de investigação criminal*, plano no qual incidem todas as balizas constitucionais e legais citadas acima como lastro de relativização de inviolabilidades de que somos titulares como cidadãos e cidadãs. Fica, no entanto, absolutamente vedado o uso de *spyware*, hoje, p*ara fins de inteligência e da atuação de órgãos de defesa nacional*, considerada a opacidade e a falta de regras claras, envolvendo sucessivos controles, a que está submetido o Sistema de Inteligência Nacional (Sisbin) e em especial a Abin.

Recentemente, o Supremo Tribunal Federal deu um passo importante a reforçar essa ideia, ao decidir, no âmbito da ADI nº 6529, que os órgãos do Sisbin não podem colher e tratar dados sujeitos a reserva de jurisdição. Afinal, considerando que os dados obtidos por meio de *spyware* são, em larga medida, dados cujo acesso envolve alguma das inviolabilidades sujeitas à autorização judicial, a Corte, com isso, praticamente fechou a porta para mobilização destas tecnologias neste plano específico de atuação do Estado. Disso tudo se extrai, portanto, que o uso de *spyware* para atividades de inteligência está absolutamente descartado no marco legal vigente, e sua autorização, aí sim, invariavelmente dependeria de uma lei específica, e ainda assim com enormes limitações, capazes de garantir que sua implementação se desse com controle ainda maior do que o já previsto para as investigações criminais.

14.



A ADPF Nº 1143: ANALISANDO A LEGALIDADE DO USO DE *SPYWARES*

Bárbara Simão e Danyelle Reis Carvalho

INTRODUÇÃO

Como a Constituição brasileira deve se posicionar em relação à adoção de tecnologias de monitoramento secreto (*spywares*) pelo Estado? Será que esses softwares de espionagem podem ser legitimamente utilizados em investigações criminais? Quais direitos fundamentais estão em potencial risco ou em proteção neste contexto? Considerando o aumento do uso de *spywares* pelas autoridades brasileiras e os recentes escândalos nacionais e globais que expuseram sua aplicação indevida no monitoramento de ativistas, jornalistas e até de outras autoridades, essas questões tornam-se não apenas prementes, mas também fundamentais no debate acerca dos limites da ação estatal e a salvaguarda dos direitos constitucionais no Brasil.

Diante dessas questões, em dezembro de 2023, a Procuradoria-Geral da República (PGR) protocolou Ação Direta de Inconstitucionalidade por Omissão (ADO 84) — posteriormente convertida em uma Arguição de Descumprimento de Preceito Fundamental (ADPF 1143), questionando a ausência de uma legislação específica que regule o uso de *spywares* por agentes públicos. A PGR argumentou que a utilização desses softwares espiões, sem regulamentação adequada, representa grave ameaça aos direitos constitucionais de inviolabilidade da vida privada, intimidade, e sigilo de comunicações e dados pessoais, contidos nos artigos 5º, X, XII e LXXIX, da Constituição.[1] Então, solicitou ao Supremo Tribunal Federal (STF) que declare inconstitucional a omissão parcial do Congresso Nacional em não implementar plenamente os direitos fundamentais em disputa no caso. Também requereu que a Corte estipule um prazo adequado para o Congresso Nacional corrigir esta omissão legislativa e definir diretrizes temporárias para assegurar a proteção dos direitos fundamentais à intimidade, privacidade e inviolabilidade do sigilo das comunicações e dados pessoais, enquanto esta lacuna normativa inconstitucional não for resolvida.

Em fevereiro de 2024, o InternetLab, em parceria com a Data Privacy Brasil e com o apoio do escritório Mudrovitsch Advogados, ingressou como *amicus curiae* no caso[2] com o objetivo de fornecer argumentos relevantes à decisão judicial, baseados em sua expertise em tecnologias, processo penal e direitos fundamentais. Em síntese, argumentamos que, ao adquirir e utilizar ferramentas que invadem dispositivos pessoais, o Estado incentiva um mercado que enfraquece a segurança das comunicações e sistemas de informação. Defendemos que, além da privacidade e proteção de dados, existe um direito à integridade dos sistemas informacionais, cabendo ao Estado protegê-los. Diante disso, concluímos que o uso de *spywares* pelo Estado compromete direitos fundamentais e deve ser considerado inconstitucional.

Este artigo tem como objetivo principal sintetizar os argumentos jurídicos apresentados pelo InternetLab e pelo Data Privacy Brasil, na qualidade de amicus curiae, na ADPF 1143.

SPYWARES E O MERCADO INTERNACIONAL DE VIGILÂNCIA

Para contextualizar a nossa contribuição à Corte, é fundamental retroceder e compreender as tecnologias de vigilância remota abordadas na ação. Em resumo, *spywares* são ferramentas que

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"

2. INTERNETLAB; DATA PRIVACY BRASIL **Petição de amicus curiae na ADPF 1143**. Relator: Cristiano Zanin. 29 jul. 2024. Disponível em: https://internetlab.org.br/wp-content/uploads/2024/08/document.pdf.

invadem dispositivos e extraem dados sem o conhecimento do usuário, explorando falhas de segurança em sistemas e redes. Isso compromete a segurança das comunicações e ameaça os direitos à privacidade e à liberdade de expressão. Como afirma Fionnuala Ní Aoláin, Relatora Especial da ONU, "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".[3]

Em 2019, o relatório "Surveillance and Human Rights" da ONU,[4] destacou a vigilância estatal direcionada, mostrando que governos utilizam *spywares* sem controle ou transparência, colocando em risco direitos fundamentais. A ausência de regulamentação sobre a exportação e o uso dessas tecnologias possibilita uma vigilância em massa e intensifica a vigilância direcionada, especialmente em regimes autocráticos, David Kaye e Marietje Schaake abordam a dinâmica:

> 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.[5]

3. 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.

4. 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://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur. Acesso em 17 set 2024.

5. 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/. Acesso em: 16 set.

Para sustentar a tese principal e facilitar a análise dos softwares que extraem informações sem o conhecimento do usuário, a Data Privacy Brasil desenvolveu uma tipologia com seis categorias:

< 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.[6]

A tipologia dos *spywares* não apenas aprimora a descrição analítica dessas ferramentas, mas também destaca como elas afetam os direitos fundamentais. Ao entender melhor suas capacidades, fica evidente que certos riscos a esses direitos são amplificados, exigindo respostas institucionais mais eficazes. Os *spywares* violam múltiplos direitos simultaneamente, representando um grande desafio para a proteção das instituições democráticas e do Estado de Direito. Essa classificação ajuda a identificar e analisar essas violações com maior precisão, reforçando a necessidade de uma regulamentação rigorosa dessas tecnologias.

6. Não se trata de uma classificação rígida e excludente, pois tais softwares estão em atualização constante e muitos utilizam vários métodos de extração, o que aumenta sua eficácia na invasão dos alvos.

3. O QUADRO NORMATIVO DE USO DE ACESSO A DADOS EM INVESTIGAÇÕES CRIMINAIS

No Brasil, temos um amplo quadro jurídico que regulamenta o sigilo das comunicações e a proteção dos dados pessoais. Entendemos que tais balizas normativas devem nortear a construção da legislação e a apreciação jurisdicional de casos que

envolvam *spywares*. Em nossa contribuição ao STF, detalhamos as principais leis e decisões judiciais sobre a temática, que perpassa a Constituição Federal, o Código de Processo Penal, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei de Interceptações Telefônicas (Lei nº 9.296/1996), a Lei de Lavagem de Dinheiro (Lei nº 9.613/1998, alterada pela Lei nº 12.683/2012) e a Lei de Organizações Criminosas (Lei nº 12.850/2013).

A Constituição Federal assegura os direitos à intimidade, privacidade, sigilo e proteção de dados pessoais, delimitando espaços que exigem justificativas especiais para qualquer intrusão estatal (art. 5º, X, XII e LXXIX). O STF tem reconhecido que a proteção da privacidade é condição de possibilidade para exercício de diversos outros direitos fundamentais. A Corte também tem reafirmado a necessidade de constante reavaliação sobre a proteção desses direitos frente às transformações tecnológicas. Em decisões recentes, como nas ADI 6649, ADPF 695[7] e ADI 6387,[8] o tribunal destacou a importância da proteção à privacidade na era digital, ressaltando que o avanço tecnológico pode tanto viabilizar o exercício de direitos fundamentais quanto ameaçá-los. Além disso, a Emenda Constitucional nº 115/2022[9] sedimentou a proteção de dados como um direito fundamental autônomo, inserido nos direitos à personalidade. Nas ADIs 6387 e 6649, a Corte corretamente estabeleceu uma dimensão subjetiva para os direitos de proteção de dados pessoais, garantidos pela LGPD, e uma dimensão objetiva, que inclui salvaguardas e procedimentos administrativos para mitigar riscos às liberdades e ao desenvolvimento da personalidade.

A quebra de sigilo, embora seja uma medida excepcional permitida, encontra-se rigidamente circunscrita a parâmetros legais que visam garantir a proteção dos direitos fundamentais. O acesso a dados pessoais pelas autoridades em investigações criminais está condicionado à demonstração de indícios razoáveis de autoria ou participação em crimes, sendo, em regra, necessária autorização judicial específica para tanto. O direito à privacidade, consagrado constitucionalmente, não pode ser violado sem justificativa adequada e fundamentada, o que impõe a obrigatoriedade de o Estado demonstrar a relevância da medida antes de intrusões nas comunicações ou nos dados de um indivíduo.

Em síntese, qualquer acesso a dados pessoais que ultrapassem a qualificação pessoal, filiação e endereço do investigado, deve ser precedido de uma análise judicial criteriosa, devidamente fundamentada e limitada a casos onde haja evidências razoáveis de envolvimento do indivíduo em atividades criminosas. Em nenhuma das hipóteses previstas pela legislação brasileira é admitida a intrusão remota em dispositivos eletrônicos. Dessa forma, a necessidade de autorização judicial específica torna-se um requisito inafastável para a adoção de medidas tão intrusivas quanto a quebra de sigilo de comunicações e dados, resguardando a privacidade dos indivíduos e limitando o poder investigatório do Estado a situações excepcionais e claramente justificadas.

7. Nas ações, o STF decidiu que os órgãos e entidades da administração pública federal estão autorizados a compartilhar dados pessoais entre si, desde que atendam a determinados critérios.

8. Na ação, a Corte suspendeu os efeitos da MP 954/2020, que autorizava o compartilhamento de dados de usuários de telecomunicações com o IBGE para fins de estatísticas durante a pandemia. Em uma decisão histórica, o tribunal reconheceu a proteção de dados como um direito fundamental autônomo.

9. BRASIL. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e no rol de competências privativas da União. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 20 set. 2024.

4. ARGUMENTOS PELA INCONSTITUCIONALIDADE NO USO DE *SPYWARES*

Partimos da premissa anterior, então, para analisar a questão pendente: tecnologias de intrusão remota deveriam ser consideradas inconstitucionais ou seu uso poderia ser permitido, desde que respeitados limites e normas legais rigorosas?

Em nossa análise, a primeira alternativa se apresenta como a mais adequada. O argumento parte da premissa de que 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. Além disso, ao adquirir ou viabilizar o uso de aplicativos espiões, o Estado contribui para o fortalecimento de uma indústria que explora vulnerabilidades nas comunicações de seus cidadãos. Defendemos, nesse sentido, a existência de um direito à integridade informacional, que decorre das proteções constitucionais relativas à privacidade, ao sigilo das comunicações e à proteção de dados pessoais, e a inconstitucionalidade no uso de *spywares*.

Ferramentas de spyware figuram entre os meios de investigação mais intrusivos disponíveis para o Estado. A possibilidade de acesso remoto a um dispositivo eletrônico, sem o conhecimento do usuário, não pode ser equiparada à interceptação telefônica ou à invasão de domicílio, uma vez que o grau de intrusão na vida privada pode ser considerado ainda mais grave. Dados extraídos de um dispositivo eletrônico têm o potencial de revelar aspectos profundos da identidade de seu titular, abrangendo informações sobre sua residência, hábitos, renda e interações pessoais. Tais informações compõem um retrato abrangente e detalhado da vida privada do indivíduo, incluindo seus hábitos, interesses, preferências e associações familiares, políticas, profissionais, religiosas e sexuais, que

/ O ESTADO INCENTIVA UM MERCADO QUE ENFRAQUECE A SEGURANÇA DAS COMUNICAÇÕES E SISTEMAS DE INFORMAÇÃO /

/ A POSSIBILIDADE DE ACESSO REMOTO A UM DISPOSITIVO ELETRÔNICO [...] NÃO PODE SER EQUIPARADA À INTERCEPTAÇÃO TELEFÔNICA /

podem ser revelados ou inferidos por meio dessas tecnologias. Além disso, como também já foi dito, a premissa do desenvolvimento de *spywares* depende da exploração de vulnerabilidades na infraestrutura de comunicação dos usuários.

Isso posto, o incentivo à indústria de *spywares* é capaz de afetar a qualidade do debate público e a 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 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.

De acordo com Alan Westin, a privacidade é de fundamental importância social e política, constituindo um elemento essencial nos sistemas democráticos.[10] A ausência de privacidade, por sua vez, pode ter efeitos nocivos sobre a autonomia individual, política, decisória e de opinião. A consciência de que pode haver monitoramento pode levar os cidadãos a alterar a forma como se expressam. Práticas estatais podem causar "efeitos inibitórios" (*chilling effects*) na expressão de toda uma comunidade, incluindo aqueles que ainda não foram diretamente alvos de vigilância. As consequências desses efeitos vão desde a desconfiança em relação às instituições sociais até a deterioração da vida intelectual, criando um ambiente onde a comunicação ocorre de maneira inibida ou tímida.[11]

10. WESTIN, A. F. Privacy and freedom. New York: Ig Publishing, 2015, p. 246.

11. 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 .

Esse impacto se manifesta não apenas quando uma pessoa sabe que está sendo vigiada, mas também quando há consciência da possibilidade de vigilância, mesmo sem a certeza de quando isso possa ocorrer. Conforme observa 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.[12]

12. SOLOVE, Daniel J. A taxonomy of privacy. University of Pennsylvania Law Review, v. 154, n. 3, jan. 2006, p. 494-495.

A utilização reiterada de ferramentas de spyware por autoridades estatais, portanto, pode ter implicações negativas para o ambiente democrático, seja pelo impacto na segurança da infraestrutura de telecomunicações, pelo efeito inibidor sobre a liberdade de expressão e a confiança da população nas instituições, ou pela possibilidade de tais ferramentas serem usadas para fins antidemocráticos, contrariando os princípios da legalidade e da impessoalidade na administração pública, como demonstram diversos casos no Brasil e em outras partes do mundo.

Diante disso, é difícil pensar em casos em que o uso de *spywares* possa ser considerado *necessário e proporcional*. A expressão remete ao teste tripartite da Corte Interamericana de Direitos Humanos, que verifica a legitimidade das ingerências à privacidade no âmbito das comunicações.[13] O Estado tem o ônus de provar uma conexão direta e imediata entre uma possível ameaça e a consequente restrição a direitos, bem como de impor o instrumento menos intrusivo entre aqueles que podem alcançar a mesma função protetora. Isso significa que apenas uma situação muito excepcional, de alta gravidade e risco iminente, em que não houvesse mais meios disponíveis à disposição do Estado, seria capaz de justificar uma medida extrema como a instalação de uma ferramenta espiã. Mesmo assim, seriam essenciais mecanismos de supervisão e prestação de contas suficientemente sólidos, assegurando que o uso dessas tecnologias fosse autorizado, monitorado e revisado por instâncias independentes, de forma a prevenir abusos e resguardar os princípios do Estado Democrático de Direito.

13. O direito à liberdade de expressão e o direito à privacidade são protegidos tanto pelo Pacto Internacional de Direitos Civis e Políticos (PIDCP) quanto pela Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica). Qualquer restrição a esses direitos deve atender a três critérios essenciais: (a) estar definida de forma clara e precisa em lei, evitando ambiguidades que possam permitir interpretações arbitrárias; (b) ser necessária e proporcional, ou seja, a restrição deve ser a medida menos invasiva possível para alcançar o objetivo pretendido; e (c) visar um objetivo legítimo, como a proteção da segurança nacional, da ordem pública, da saúde pública ou dos costumes. A Corte Interamericana de Direitos Humanos reforça que essas condições são indispensáveis para evitar ingerências arbitrárias nos direitos garantidos.

Na prática, observa-se um cenário contrário à transparência e à prestação de contas. A indústria de *spywares* tem se expandido em um contexto de baixa transparência, escassa fiscalização pública e fracos mecanismos de controle. Em razão dessas fragilidades, o então Relator Especial das Nações Unidas para a Liberdade de Expressão, David Kaye, defendeu a necessidade de moratória na concessão de licenças para a exportação de tecnologias de vigilância direcionada, "até que existam evidências convincentes de que o uso dessas tecnologias pode ser tecnicamente limitado a finalidades legais, em conformidade com os padrões de direitos humanos, ou que essas tecnologias serão exportadas apenas para países onde seu uso esteja sujeito à autorização - concedida de acordo com o de-

vido processo legal e com os critérios de legalidade, necessidade e legitimidade - por uma autoridade judicial independente e imparcial".[14]

Tais consequências enfatizam a necessidade de proteção do direito à integridade dos sistemas informacionais, que decorre das garantias constitucionais relacionadas à privacidade, à proteção de dados e à autodeterminação informativa. A "garantia da confidencialidade e da integridade dos sistemas técnico-informacionais" foi declarada pelo Tribunal Constitucional Alemão em 2008,[15] chamando atenção "para a importância que a utilização dos sistemas informáticos adquiriu para o desenvolvimento da personalidade do indivíduo nas últimas décadas".[16] Conforme nota Fabiano Menke, enquanto a autodeterminação informativa se ocupa da proteção de dados individuais ou de conjuntos específicos de dados, o direito fundamental à confidencialidade e integridade dos sistemas técnico-informacionais se estende à proteção tanto dos sistemas quanto dos dados de maneira mais abrangente.[17]A existência de um dever do Estado de proteção sobre o ambiente informacional tem sido, inclusive, reconhecido pelo STF em diferentes oportunidades, condicionando as atividades do Estado ao não enfraquecimento do ambiente de informação e comunicação de seus cidadãos, assim como à garantia de uma infraestrutura democrática do debate público. Essa é a conclusão que se extrai a partir do julgamento da ADPF 722[18], ADPF 695[19], ADI 6529[20] e ADI 6387[21], casos em que se reforçaram interpretações relacionadas ao direito autônomo à proteção de dados pessoais e à autodeterminação informacional, bem como o dever de que o Estado atue em conformidade com a garantia desses direitos.

O debate sobre criptografia também oferece entendimentos relevantes ao caso. Hoje, o tema é discutido na ADPF 403 e na ADI 552, ambas previstas para julgamento conjunto no STF. Em seu voto na ADI 5527, a então Ministra Rosa Weber comparou os dispositivos móveis a "janelas luminosas para a nossa intimidade". A Ministra decidiu que o Estado não pode obrigar empresas a "prestar serviços de comunicações privadas a adotar mecanismos que garantam o acesso ao conteúdo das conversas" e, assim, enfraquecer a criptografia. Edson Fachin, relator da ADPF 403, argumentou em seu voto que é contraditório que "em nome da segurança pública, não se promova uma internet mais segura, já que uma internet mais segura é um direito de todos e um dever do Estado". O Ministro refutou o dilema entre segu-

14. **KAYE, David.** *Report on the adverse effect of the surveillance industry on freedom of expression.* A/HRC/41/35. Organização das Nações Unidas. Disponível em: https://www.ohchr.org/en/calls-for-input/report-adverse-effect-surveillance-industry-freedom-expression. Acesso em: 19 set. 2024. Tradução livre.

15. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informations-technischer Systeme.

16. 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. p. 795.

17. Ibidem, p. 795.

18. 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. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354

19. 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.

20. 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.

21. 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.

rança e privacidade, argumentando que o enfraquecimento da criptografia compromete o dever do Estado de garantir a segurança. Ambos os votos, portanto, sustentam que a proteção dos sistemas informáticos e comunicacionais é fundamental para a preservação dos direitos à privacidade e à liberdade de expressão.

A utilização de tecnologias espiãs vai de encontro à garantia da integridade desses sistemas. Por isso, defendemos a não utilização de ferramentas de intrusão remota em sistemas eletrônicos, além do reconhecimento da ilegalidade na aquisição dessas ferramentas.

5. CONSIDERAÇÕES FINAIS

No presente artigo, exploramos os argumentos jurídicos desenvolvidos ao longo da contribuição de *amicus curiae* apresentada pelo InternetLab e pela Data Privacy Brasil. Diante da crescente evidência de ilegalidades associadas ao uso de *spywares* por autoridades públicas, aumenta a expectativa em relação à decisão do STF sobre essa questão. O Tribunal tem hoje a possibilidade de moldar os limites quanto à utilização dessas tecnologias no Brasil.

Defendemos, no Amicus Curiae, que o uso de *spywares* pelo Estado seja declarado inconstitucional, uma vez que essa prática compromete direitos fundamentais, como a privacidade, a proteção de dados pessoais e a integridade dos sistemas informacionais. Os argumentos apresentados sustentam que o Estado deve, prioritariamente, garantir a segurança das comunicações de seus cidadãos, em vez de comprometer tais garantias ao incentivar a exploração de vulnerabilidades em infraestruturas e sistemas de comunicação. Considerando a elevada intrusividade e os riscos associados a essas ferramentas, torna-se questionável sua proporcionalidade em relação aos possíveis benefícios para investigações criminais, uma vez que o Estado dispõe de outras técnicas menos invasivas e mais compatíveis com os princípios democráticos.

Caso, no entanto, o STF opte por não declarar a inconstitucionalidade do uso de *spywares*, é fundamental que o emprego dessas tecnologias seja rigorosamente limitado a situações excepcionais, apenas quando não houver alternativas viáveis. Além disso, são necessários critérios estritos, em conformidade com a legislação brasileira, para mitigar os impactos sobre os direitos fundamentais. Legislações e decisões judiciais que buscam oferecer as balizas contra o uso ilegal de *spywares* devem observar, 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."[22]

22. Contribuição ao STF (*amicus curiae*) p. 48

De toda forma, é grande a expectativa em torno do julgamento deste caso no Supremo Tribunal Federal. A Corte possui a oportunidade de definir limites significativos para o uso de *spywares* no Brasil, garantindo a proteção das garantias fundamentais e dos valores democráticos.

REFERÊNCIAS

BRASIL. **Emenda Constitucional n.º 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e no rol de competências privativas da União. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** Segunda Edição. Rio de Janeiro: Revista dos Tribunais, 2001. p. 165

INTERNETLAB; DATA PRIVACY BRASIL **Petição de *amicus curiae* na ADPF 1143**. Relator: Cristiano Zanin. 29 jul. 2024. Disponível em: https://internetlab.org.br/wp-content/uploads/2024/08/document.pdf .

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/.

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.

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.

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.

PROCURADORIA-GERAL DA REPÚBLICA. **Petição inicial na ADO 84**. 13 dez. 2023. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=776054030&prcID=6900814#. Acesso em 17 set. 2024.

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://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur. Acesso em 17 set. 2024.

SUPREMO TRIBUNAL FEDERALl. Relator: Cristiano Zanin. **Decisão monocrática na ADO 84 que a converteu para a ADPF 1143.** 16 abril Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=776054030&prcID=6900814#. Acesso em 17 set. 2024.

KAYE, David. *Report on the adverse effect of the surveillance industry on freedom of expression*. A/HRC/41/35. Organização das Nações Unidas. Disponível em: https://www.ohchr.org/en/calls-for-input/report-adverse-effect-surveillance-industry-freedom-expression.

ESTE LIVRO FOI COMPOSTO COM AS FAMÍLIAS TIPOGRÁFICAS *DECIMA MONO* E *FF META*. PARA O MIOLO FOI UTILIZADO O PAPEL COUCHÊ FOSCO E PARA A CAPA O PAPEL DUO DESIGN. O PROJETO GRÁFICO É DE AUTORIA DO *ESTÚDIO CLARABOIA* E AS ILUSTRAÇÕES SÃO DA *PINGADO SOCIEDADE ILUSTRATIVA*.