DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.6 >

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / ALEXANDRE AU-YONG OLIVEIRA / ALEXANDRE SENRA / BENNETT CAPERS / CLARISSA BORGES / DANIELA EILBERG / ERIC DO VAL LACERDA SOGOCIO / EVELYN SHEEHAN / JULIANA SÁ DE MIRANDA / MAURÍCIO ZANOIDE DE MORAES / NATHÁLIA CORRÊA LEISER TAMER / PAULO RENÁ / VERIDIANA ALIMONTI / VITOR SANTOS VILANOVA

INTERNETLAB

SÃO PAULO, 2023

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(eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. V. São Paulo. InternetLab, 2023.

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 eradigital. -- 1. ed. -- São Paulo : InternetLab,2023. -- (Doutrina e prática em debate ; 6)

Vários autores.
Bibliografia.
ISBN 978-65-88385-16-6

1. Direito processual penal **2.** Direitosfundamentais **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação **I.** Série.

23-165951 **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 /

< ALEXANDRE AU-YONG OLIVEIRA >

Alexandre Au-Yong Oliveira é juiz de direito desde 1999. É docente no Centro de Estudos Judiciários (CEJ), Lisboa, desde 2016, sendo responsável pela formação de juízes e procuradores nas áreas de Direito Penal e Processo Penal, Cooperação Judiciária Internacional em Matéria Penal e Ética. Representa o CEJ no subgrupo de trabalho de Justiça Criminal da Rede Europeia de Formação Judiciária, onde organiza e participa em seminários sobre Cibercriminalidade e Prova Digital.

< ALEXANDRE SENRA >

Procurador da República. Coordenador do GT Criptoativos do MPF. Mestre em Direito. Mestrando em Digital Currencies e Blockchain. Certificado em Blockchain pelo Massachussets Institute of Technology e em Decentralized Finances pela University of Nicosia. Participou da primeira alienação de bitcoins da Justiça Federal Brasileira. Coordena o primeiro MBA em Criptoativos e Blockchain do País.

< BÁRBARA SIMÃO >

Mestre em direito e desenvolvimento pela Fundação Getúlio Vargas (FGV Direito SP). Graduada pela Faculdade de Direito da Universidade de São Paulo (FDUSP). Durante a graduação, foi aluna intercambista na universidade Paris 1 Panthéon-Sorbonne (2015-2016). Foi bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica, pelo Ministério da Educação. Atuou como pesquisadora na área de direitos digitais do Instituto Brasileiro de Defesa do Consumidor (Idec), entre 2017 e 2020.

Foi também conselheira do Projeto "Proteção de Dados em Serviços de Saúde Digital", da Fiotec/Fiocruz. Atualmente, é coordenadora de pesquisa da área de Privacidade e Vigilância do InternetLab.

< BENNETT CAPERS >

No outono de 2020, o professor Bennett Capers juntou-se à Faculdade de Direito da Fordham, onde leciona sobre Provas, Direito Penal e Processo Penal, e também é diretor do Centro de Raça, Direito e Justiça. Como ex-procurador federal, seus interesses acadêmicos incluem a relação entre raça, gênero, tecnologia e justiça criminal, e ele é um prolífico escritor sobre esses temas. Ele foi professor visitante na Faculdade de Direito da Fordham durante o ano acadêmico de 2008-09, e também foi professor visitante na Faculdade de Direito da Universidade do Texas e na Faculdade de Direito da Universidade de Boston. Na primavera de 2022, ele será professor visitante na Faculdade de Direito de Yale.

< CLARISSA BORGES >

Assessora de advocacy e litígio estratégico do IDDD, advogada, mestre em direito pelo PPGD/UFMG.

< DANIELA EILBERG >

Doutoranda e Mestra em Ciências Criminais pela PUCRS. Pós-graduanda em Ciberdelitos y Evidencia Digital pela Universidade de Buenos Aires. Realizou visita profissional na Corte Interamericana de Direitos Humanos. Graduada em Direito pela UFRGS com período sanduíche na Université Paris I Panthéon-Sorbonne. Editora-assistente da Revista Brasileira de Direito Processual Penal e da Revista de Estudos Criminais. Pesquisadora Sênior da Associação Data Privacy Brasil de Pesquisa.

< ERIC DO VAL LACERDA SOGOCIO >

Vice-Presidente do Comitê Ad Hoc das Nações Unidas para elaborar Convenção Abrangente sobre Combate ao Uso de Tecnologias da Informação e Comunicação para Fins Criminosos. Conselheiro na Missão Permanente de Brasil ante os Organismos Internacionais en Viena desde agosto de 2021. Diplomata de carreira desde 2003. Bacharel em Relações Internacionais pela Universidade de Brasília, em 2000. Mestre em Diplomacia pelo Instituto Rio Branco, em 2005. Serviu nas embaixadas do Brasil em Pretória (2014 – 2017), Buenos Aires (2011 – 2014) e Nova Delhi (2008 – 2011), onde se encarregou, principalmente, de temas relativos a segurança e defesa. Chefe da Coordenação-Geral de Combate ao Crime Transnacional, do Ministério de Relações Exteriores em Brasília de 2018 até 2021. Assessor dessa divisão, entre 2005 e 2008. Como Chefe da Coordenação-Geral de Combate ao Crime Transnacional, foi o representante do Ministério de Relações Exteriores junto: ao Conselho de Controle de Atividades Financeiras (COAF), a unidade de inteligência financeira do Brasil; ao Conselho do Sistema Brasileiro de Inteligência (SISBIN); ao Conselho Nacional de Políticas sobre Drogas (CONAD); à Comissão Nacional de Segurança Publica nos Portos, Terminais e Vias Navegáveis (CONPORTOS); à Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA). No âmbito do combate ao crime cibernético, foi panelista durante a 4ª Sessão do Grupo Intergovernamental de Peritos Encarregado de Conduzir um Estudo Integral sobre Crime Cibernético (2018), sob o tópico dedicado à criminalização, e chefe de delegações brasileiras que trataram de temas vinculados ao crime cibernético em foros bilaterais, regionais e multilaterais.

< EVELYN SHEEHAN >

Evelyn Baltodano Sheehan concentra sua prática no aconselhamento de indivíduos de alto patrimônio líquido, clientes institucionais e seus executivos em investigações transfronteiriças, ações de fiscalização do governo e questões relacionadas ao confisco de ativos. Antes de ingressar na Kobre & Kim, a Sra. Baltodano Sheehan atuou como promotora por quase dez anos no Departamento de Justiça dos EUA (DOJ), onde foi responsável por supervisionar investigações transfronteiriças complexas relacionadas à corrupção internacional, suborno estrangeiro, fraude de colarinho branco, tráfico de entorpecentes, crime organizado e violações das leis de combate à lavagem de dinheiro. Ela também palestrou extensivamente sobre a aplicação das leis de confisco de ativos e lavagem de dinheiro para o Departamento de Justiça dos EUA e várias agências federais, incluindo o Federal Bureau of Investigation, o Departamento de Defesa dos EUA, o Departamento de Saúde e Serviços Humanos dos EUA e a Drug Enforcement Agency.

< JULIANA SÁ DE MIRANDA >

Sócia das práticas de crimes de colarinho branco e compliance & investigação do Machado Meyer Advogados, Juliana é uma advogada experiente, cuja atuação se concentra na defesa de empresas e pessoas físicas em complexas investigações nacionais e internacionais. Mais de 20 anos de experiência na condução de investigações internas de alegadas violações de compliance para clientes corporativos, assessorando-os em melhorias nos programas e treinamentos de compliance. No crime de colarinho branco, a atuação de Juliana abrange as áreas de consultoria e contencioso, incluindo a avaliação de riscos criminais, due diligences criminais e anticorrupção

em operações societárias, e a defesa de casos de Direito Penal Empresarial relacionados a corrupção, fraude, meio ambiente, fiscal e outros. relacionados com a atividade empresarial. Certificação em Compliance & Ethics Professional International (CCEP-I) pela Society of Corporate Compliance and Ethics (SCCE – 2010). Graduação na Faculdade de Direito da Universidade de São Paulo (1999).

< MAURÍCIO ZANOIDE DE MORAES >

Professor Associado do Departamento de Direito Processual da Faculdade de Direito da Universidade de São Paulo, a mesma Universidade na qual se graduou (1989), tornou-se Doutor em Direito Processual (1999) e Livre-Docente (2008). Também é Pós-Graduado (2000) em Direito Penal Econômico e Europeu pelo Instituto de Direito Penal Econômico e Europeu (IDPEE) em parceria com o Instituto Brasileiro de Ciências Criminais (IBCCRIM). É na Faculdade de Direito da Universidade de São Paulo que atualmente coordena o desenvolvimento de pesquisas, trabalhos e atividades acerca de meios de solução de conflito não judiciais e a interrelação entre direito processual penal e os avanços tecnológicos. É membro de várias associações e instituições científicas e profissionais, dentre as quais estão o Instituto Brasileiro de Direito Processual (IBDP), o Instituto de Defesa do Direito de Defesa (IDDD) e a Associação dos Advogados de São Paulo (AASP), tendo sido presidente do IBCCRIM no período de 2005/2006.

< NATHÁLIA CORREA LEISER TAMER >

Nathália é advogada com formação em Direito pela Universidade Presbiteriana Mackenzie em São Paulo e possui trajetória profissional dedicada à área de Compliance e Investigações. Por meio de sua atuação na área desde 2017, possui experiên-

cia consultiva e na prevenção e solução de riscos, bem como na condução de investigações corporativas e atuação em processos administrativos de responsabilização."

< PAULO RENÁ >

Doutorando e Mestre em Direito, Estado e Constituição na Universidade de Brasília, Professor de Direito Digital na graduação e na Pós-Graduação do Centro Universitário de Brasília. Pesquisador no Instituto de Referência em Internet e Sociedade. Diretor do Aqualtune LAB: Direito, Raça e Tecnologia. Foi gestor do processo de elaboração coletiva do Marco Civil da Internet na Secretaria de Assuntos Legislativos do Ministério da Justiça.

< VERIDIANA ALIMONTI >

Advogada, diretora associada de políticas para a América Latina da Electronic Frontier Foundation e doutora em Direitos Humanos pela Faculdade de Direito da USP. Foi estudante visitante no Departamento de Proteção de Dados do Conselho da Europa em 2017, representante titular do terceiro setor no CGI entre 2011 e 2013 e representante dos consumidores no Comitê de Defesa dos Usuários de Serviços de Telecomunicações da Anatel (CDUST) até o início de 2015.

< VITOR SANTOS VILANOVA >

Estagiário do InternetLab. Graduando em Direito pela Faculdade de Direito da Universidade de São Paulo (FD-USP). É pesquisador convidado do IBCCrim. Foi aluno da Escola de Formação Pública da Sociedade Brasileira de Direito Público (SBDP), em que desenvolveu pesquisa no tema: “Princípio da Insignificância no Supremo Tribunal Federal” (2021). Foi estagiário em direito criminal em Cavalcanti, Sion e Salles

Advogados. Fez parte do Departamento Jurídico XI de Agosto e foi editor na Revista Acadêmica São Francisco (RASF), ambos da FD-USP. Tem se dedicado a pesquisas na área penal, em especial criminalização da pobreza. Atualmente, é estagiário de pesquisa no InternetLab.

SUMÁRIO /

APRESENTAÇÃO DOS EDITORES /

Em um mundo em que se expandem as possibilidades de coleta e tratamento de dados por parte de órgãos de investigação, refletir sobre garantias penais e direitos fundamentais dos cidadãos é uma tarefa essencial e complexa. Novas tecnologias amparadas em dados devem ser vistas com atenção e cautela, em debates que levem em conta o impacto, a efetividade e os potenciais riscos e controvérsias de determinadas medidas.

Com o intuito de refletir sobre as questões desse campo, o InternetLab, centro independente de pesquisa em direito e tecnologia, organiza desde 2017 o Congresso "Direitos Fundamentais e Processo Penal na Era Digital", promovido anualmente com o apoio institucional da Faculdade de Direito da Universidade de São Paulo (FDUSP), e com auxílio da Professora Doutora de Direito Processual Penal Marta Saad.

A sexta edição do Congresso, que ocorreu de forma híbrida entre os dias 23 e 25 de agosto de 2022, adotou o tema "proteção de dados pessoais e cibercrimes", abordando as controvérsias em torno de tratados internacionais sobre o assunto e a adesão brasileira a essas normas, bem como enfrentadas por legisladores, pelo judiciário e por operadores do direito diante do desenvolvimento e absorção de novas tecnologias na prevenção, repressão, processamento de delitos digitais.

As contribuições aqui compiladas abordam a persecução penal internacional, as perspectivas de negociação da Conven-

ção das Nações Unidas sobre crime cibernético, abordagens sobre os crimes de *ramsomware* e lavagem de dinheiro, análises sobre investigação defensiva e cadeia de custódia, assim como textos que abordam debates hoje correntes no supremo Tribunal Federal, como a busca reversa por dados de pessoas indefinidas no âmbito de investigações criminais. Abordamos também os poderes de vigilância estatal e os potenciais impactos sobre direitos fundamentais decorrentes dos desafios impostos por novas tecnologias.

Todas as contribuições do Congresso estão também registradas em vídeo e disponíveis para acesso online. Com isso, seguimos na intenção de construir e divulgar reflexões que atualizem e destrinchem os desafios postos pelo desenvolvimento tecnológico e o uso de dados às garantias do processo penal.

Boa leitura,

FRANCISCO BRITO CRUZ
BÁRBARA SIMÃO

São Paulo, junho de 2023.

01.

NOVAS FORMAS DE SUJEIÇÃO, VELHAS E NOVAS FORMAS DE RESISTÊNCIA[1]

Alexandre Au-Yong Oliveira

Agradeço o convite para ser *keynote* neste seminário, ao Internetlab e à Faculdade de Direito da Universidade de São Paulo - e às gentis palavras de apresentação feitas pela Doutora Heloisa Massaro. Muito obrigado.

Quanto à minha apresentação, eu represento o Centro de Estudos Judiciários de Lisboa (CEJ), na Rede de Formação Judiciária Europeia – uma rede de escolas de magistrados que visa englobar o máximo de Estados Membros da União Europeia possível e compartilhar experiências em diversas áreas. Eu estou incumbido de organizar atividades em torno do cibercrime e prova digital. Por essa razão, nos últimos cinco anos, tenho trabalhado sobre estas matérias e contatado profissionais, em especial procuradores e juízes, e também advogados que trabalham nesta área e com agentes de organizações transnacionais, tais como Eurojust e Europol.

Com esta contextualização pessoal, minha apresentação passará por fases distintas: um primeiro enquadramento, mais filosófico e social, acerca da sociedade em que vivemos, para depois passarmos a questões mais concretas do processo da investigação criminal na era digital.

DA SOCIEDADE DISCIPLINAR À SOCIEDADE DE CONTROLE

Em 1990, o filósofo Gilles Deleuze, em um pequeno texto intitulado "Post-scriptum Sobre a Sociedade de Controle"[2], falava da "modulação universal" dando o exemplo de uma pulseira eletrônica e da possibilidade da geo-localização dessa pessoa em um espaço aberto. O que o autor queria dizer por esta "modulação universal"?

1. Sociedade disciplinar (Foucault): família, escola, quartel, fábrica, hospital e prisão (séculos XVII a XX)
2. Transição do discreto (**molde**) para o contínuo (**modulação**): crise da *família* (patriarcal), *escola* (da avaliação contínua à formação contínua), *fábrica* (retribuição variável, "uberização"), *quartel* (exército voluntário), *hospital* (centros de saúde locais, centros de dia, etc.) e *prisão* (pulseira eletrónica, proibição de contactos com controlo remoto); a reformulação da propriedade (*streaming*)

SCREENSHOT DA APRESENTAÇÃO

Dando um passo atrás, a sociedade disciplinar – como designada por outro filósofo francês contemporâneo, Michel Foucault, no livro "Vigiar e Punir"[3] – era uma forma de organizar a sociedade por moldes, por espaços fechados e bem delimitados no tempo e, portanto, com um certo dinamismo espácio-temporal. A sociedade organizava-se em espaços-tempo bem delimitados. Era o caso da família e diversas outras instituições, como a escola, o quartel, a fábrica e a prisão.

No período de transição desta moldagem do indivíduo para a sociedade de controle, assistimos, naturalmente, a crises abertas dessas instituições. Desde a crise da família patriarcal como a forma de "expressão familiar" e o surgimento das famílias sem figura paterna, à reorganização ou crise da escola, a qual deixa de ser delimitada em um tempo e espaço. A educação e formação do indivíduo passa por uma avaliação contínua, não se encerrando no período escolar. Juízes e procuradores em Portugal são obrigados a assistir, por exemplo, a seis horas de formação de "reciclagem" anualmente, para atualizarem os seus conhecimentos, numa formação perpétua.

Já a instituição da fábrica, que antes se concentrava na produção em diversos níveis, classificados pelos respectivo trabalhadores, passou a ser mais vocacionada para o setor terciário e para a venda. Com isso, a retribuição passou a ser variável, modulável, digamos assim. Além disso, assiste-se a uma maior flexibilização do espaço-tempo no ambiente de trabalho – do que nasce, por exemplo, o direito a desligar-se, uma vez que o espaço do trabalho invade as nossas próprias casas. Durante as férias estamos constantemente ligados ao nosso trabalho através do e-mail, através de grupos de mensagem instantânea como o WhatsApp e, portanto, nunca nos desligamos. O contínuo do espaço e do tempo que, no passado, se fechava, hoje é difícil desligar.

O mesmo vale para hospitais. Os ambientes hospitalares foram acompanhados de uma evolução, em que são cada vez mais importantes os centros médicos. Isto é, o internamento em hospital passou a ser excepcional e a regra passou a ser o acompanhamento domiciliar.

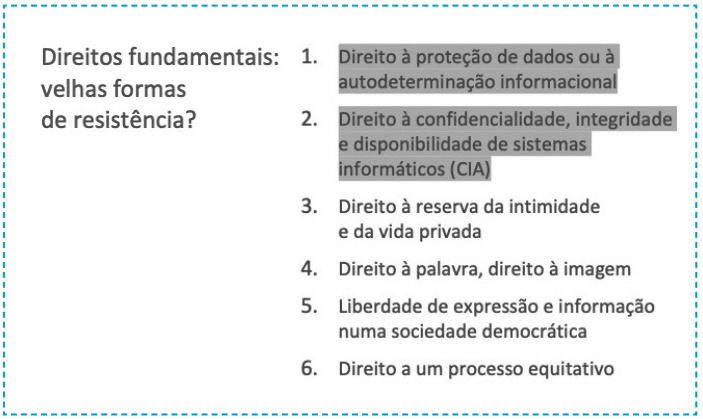
No caso da prisão, que era o espaço de fechamento por excelência, existem agora alternativas como a pulseira eletrônica e outras medidas de controle remoto. Portanto, é dentro desta nova sociedade que o processo penal se localiza, como diria Foucault.

Não vale muito a pena apontar qual é o regime mais agressivo, qual é o regime mais violento. Ambos têm as suas próprias violências. Ambos têm as suas próprias liberdades. Deixa-nos o autor com esta ideia que não vale a pena ter medo ou esperança: mais vale procurar, nos tempos do novo regime, novas armas de resistência.

DIREITOS FUNDAMENTAIS: VELHAS FORMAS DE RESISTÊNCIA?

Como sabemos, uma das formas mais tradicionais de resistência é a criação de direitos fundamentais como limite aos poderes do Estado, protegendo o indivíduo contra arbitrariedades. A sua grande expansão deu-se nas épocas liberais, entre os séculos XIX e XX, uma vez que foram instrumentos construídos de uma sociedade que levava ao fechamento do indivíduo e organizava-o dentro de um espaço-tempo muito bem delimitado.

Em bom rigor, essa não é mais a nossa sociedade disciplinar. No entanto, os direitos fundamentais ainda hoje são instrumentos importantíssimos a nível jurídico. Eu queria, portanto, destacar os direitos fundamentais principais mais importantes dentro da problemática que nos traz aqui hoje - ou seja, do cibercrime e da prova digital.



SCREENSHOT DA APRESENTAÇÃO

Começo com os dois direitos sublinhados, uma vez que são direitos da nova sociedade que foram criados há relativamente pouco tempo, já no século XXI. O direito à proteção de dados, em Portugal e na grande maioria das constituições europeias, está consagrado expressamente como direito fundamental. Também se denomina este direito, por vezes, como o direito à autodeterminação informacional.

Seguidamente, temos um direito baseado no conceito de cibersegurança, no chamado direito à confidencialidade, integridade e disponibilidade de sistemas informáticos (em inglês, *confidentiality, integrity and availability*, daí a sigla CIA). Este direito fundamental é considerado um direito não-escrito. Não está expressamente consagrado nas Constituições que eu conheço, mas foi desenvolvido pelo Tribunal Constitucional Alemão já no princípio do século XXI, quando eram discutidas questões como a utilização de novos meios intrusivos na investigação criminal, em especial, a infiltração de *malware* em sistemas informáticos de suspeitos, pelas autoridades policiais e judiciárias.

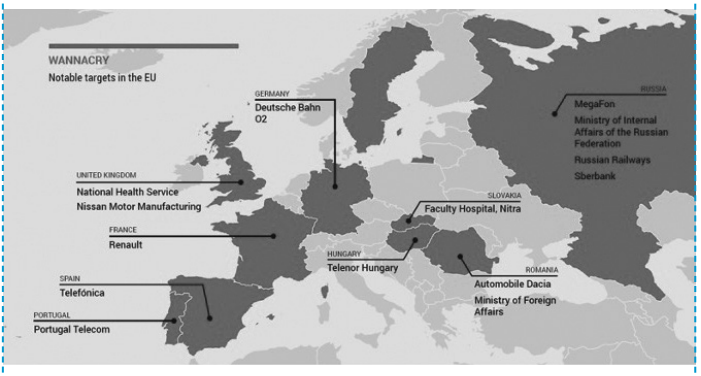
Depois, temos o direito à reserva da intimidade e da vida privada, o direito à palavra, à imagem, à liberdade de expressão e à informação na sociedade democrática – os quais são direitos tradicionais e já muito antigos.

Fazendo esta introdução dentro de um contexto mais amplo, antes de passarmos a questões jurídicas mais concretas, dir-se-ia que os direitos fundamentais são várias formas de resistência. Mas dentro destes direitos fundamentais, ganharam, na Sociedade de Controle, uma nova importância os direitos que antes eram secundários e hoje tornaram-se primários, a exemplo da privacidade e da proteção de dados.

INVESTIGAÇÃO CRIMINAL E A ERA DIGITAL

Passando então a questões mais concretas de investigação criminal e processo penal na era digital, hoje assistimos a novas formas de ataque. A imagem abaixo, por exemplo, traz um mapa elaborado pela Europol em 2018, em que se mostram certos alvos de um *ransomware* conhecido como Wannacry, através do qual os ficheiros informáticos presentes nos sistemas informáticos atingidos são encriptados e tornados inacessíveis aos respectivos titulares e utilizadores.

Em 2017, houve inúmeros ataques de *ransomware* e o Wannacry foi um dos mais destrutivos. A Europol realça alguns dos serviços que foram vítimas deste ataque apenas aqui na Europa: na Península Ibérica, duas das principais telecomunicadoras – a Telefônica e a Portugal Telecom; na França, a maior empresa da indústria de automóveis; no Reino Unido, o Serviço Nacional de Saúde; e até na Rússia, o Ministério da Administração Interna e vários serviços públicos.



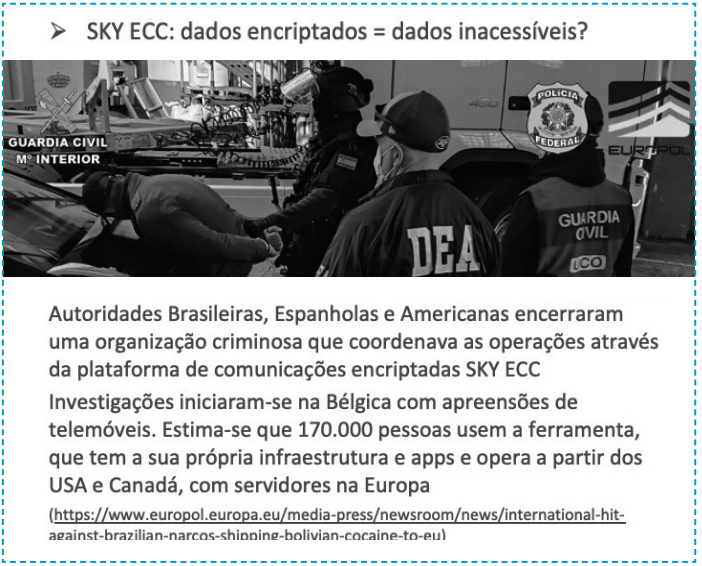
IOCTA (2018): https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment

SCREENSHOT DA APRESENTAÇÃO

Portanto, a era digital tem uma escala que era impensável há 50 ou 60 anos atrás. Através de um único programa informático pode contagiar-se sistemas informáticos no mundo inteiro. É neste ambiente de desconfiança perante possíveis atos criminosos – mas também por *overreach* das próprias autoridades estaduais, como veremos mais adiante –, que o desenvolvimento de encriptação assume-se como um mecanismo de autodefesa nesta nova realidade da sociedade da informação, em especial o *end-to-end encryption* (ou criptografia de ponta a ponta), como diz a revista Wired em artigo recente.[4]

Se é engraçado ver que o *ransomware* também utiliza encriptação – encripta os dados tornando-os inacessíveis aos seus titulares –, por outro lado, a encriptação é vendida na sociedade como uma forma de proteção. É, portanto, ao mesmo tempo uma arma de ataque e um escudo de defesa. Tem uma característica dicotômica.

Também dentro da problemática da encriptação, estão a ser desenvolvidas plataformas de comunicações eletrônicas independentes por alegadas organizações criminosas, como a plataforma SKY ECC. A Europol recentemente deu conta, inclusive, do encerramento de uma organização criminosa brasileira, contando com a ajuda das autoridades norte americanas e espanholas, relacionada com referida plataforma. Tornam-se, pois, cada vez mais comuns no processo penal estas ações policiais e judiciárias conjuntas ou equipas de investigação conjuntas, como ocorre, por exemplo, para desativar e prender os responsáveis de mercados ilegais na *darkweb*.



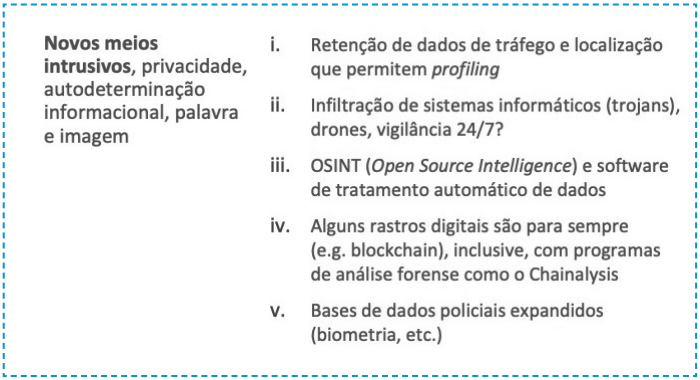
SCREENSHOT DA APRESENTAÇÃO

Esse caso é impressionante. Do meu conhecimento, e com os contatos que tenho tido com a Europol e Eurojust, é até hoje o maior *crackdown* de uma plataforma de encriptação independente. Estima-se que cerca de 170 mil pessoas pelo mundo afora estejam a utilizar esta ferramenta. A investigação iniciou-se na Bélgica, com apreensões de telemóveis, e já está a expandir-se por diversos locais do globo, inclusive no Brasil, com a ajuda da cooperação de forças policiais estrangeiras.

NOVOS MEIOS INTRUSIVOS, PRIVACIDADE, AUTODETERMINAÇÃO INFORMACIONAL, PALAVRA E IMAGEM

Dentro desta nova dinâmica criminal, também se tem verificado novos meios de investigação mais intrusivos, colocando em causa, e de forma significativa, os direitos fundamentais à pri-

vacidade e à proteção de dados, ou autodeterminação informacional, e, inclusive os direitos fundamentais à palavra e à imagem. Estes meios mais intrusivos, como a retenção de dados de tráfego e localização detidos pelos fornecedores de serviço de telecomunicações (ISPs), permitem, desde logo, o *profiling* dos investigados. Voltarei a este assunto no fim da apresentação, que creio ser a questão mais controversa aqui na Europa.



SCREENSHOT DA APRESENTAÇÃO

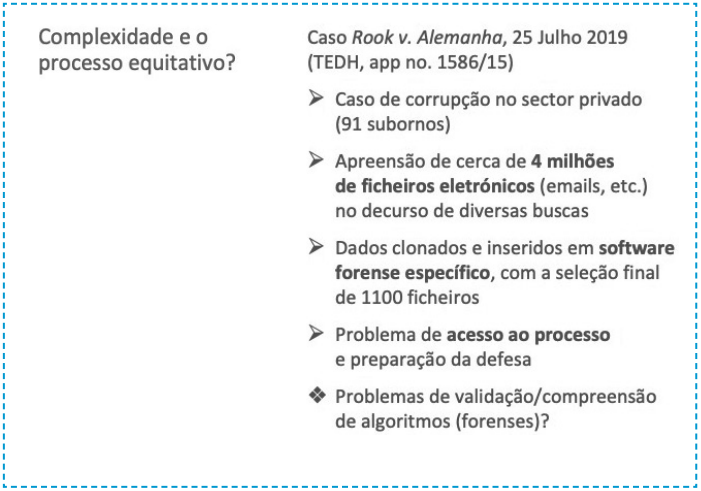
Outro instrumento altamente intrusivo é o uso de programas de *malware*, *spyware* ou *policeware*, como por vezes se chamam, e infiltração de sistemas informáticos com este tipo de programas – que permitem, inclusive, uma vigilância 24/7 e não apenas o acesso a ficheiros armazenados, por exemplo, num determinado telemóvel. Estes tipos de aplicações permitem, portanto, o acionamento dos microfones e das câmaras de telemóveis, como é por vezes nos dado a conhecer através das notícias, por exemplo envolvendo o *spyware* Pegasus de origem israelita. Mas não são só os serviços secretos que utilizam este tipo de programas, são, também, as autoridades judiciárias, atualmente.

Outro instrumento de investigação criminal novo chama-se OSINT (*Open Source Intelligence*), que envolve *software* que

permite a recolha e tratamento automático de dados pessoais presentes na Internet. A ferramenta recolhe dados pessoais, como nomes, moradas, fotografias, locais frequentados pelos visados, que estão em fontes públicas, por exemplo, redes sociais abertas ao público, e faz o tratamento automático de tais dados, comprimindo assim, obviamente, a proteção da autodeterminação informacional.

Por outro lado, alguns dos rastros digitais na internet são para sempre, como por exemplo, o caso dos diversos *blockchain*. Atualmente com programas muito potentes de análise forense (como o Chainalysis), consegue-se fazer o rastreamento das transações feitas com criptomoedas, como o *Bitcoin* ou o Ethereum.

Também, como já foi aflorado, hoje em dia, estão em expansão as bases de dados policiais para o reconhecimento facial, impressões digitais e outros elementos de biometria, e portanto, vemos que a privacidade e autodeterminação informacional são efetivamente alvos de novas violências ou novas compressões, novas restrições em nome da investigação criminal.



SCREENSHOT DA APRESENTAÇÃO

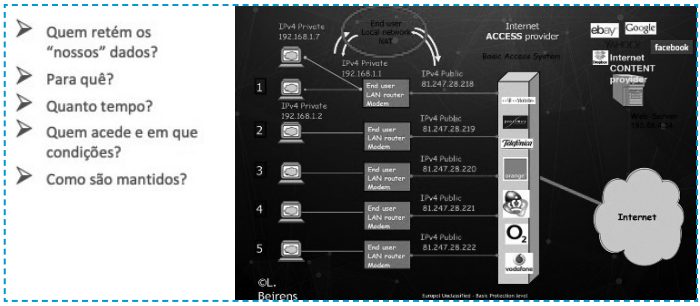
Por último, tratando de direitos fundamentais, gostaria de recordar que estes novos tipos de ciberataques, os novos métodos de investigação, implicam também alterações e uma certa crise do Judiciário, já em fase de julgamento. Por exemplo, neste caso *Rook v. Alemanha*, o Tribunal Europeu dos Direitos Humanos pronunciou-se já em 2019, portanto, já há cerca de três anos. Estava aqui em causa um agente acusado de receber 91 subornos, num caso já algo complexo, de corrupção no setor privado. Durante várias buscas, foram apreendidos cerca de 4 milhões de ficheiros eletrônicos, de e-mails e documentação contida em servidores de diversas empresas e computadores, portanto, alvo de buscas físicas. Estes quatro milhões de ficheiros eletrônicos foram depois clonados, copiados e inseridos em *software* específico que permitiu, portanto, uma seleção final de 1.100 ficheiros. Destes 4 milhões de ficheiros apreendidos, foram aproveitados um número muito residual - 1.100 ficheiros - para serem utilizados contra o arguido daquele processo.

Neste caso, perante o Tribunal Europeu, foram colocados pela defesa questões de "como é que eu me defendo num universo de dados tão elevado?" Como é possível eu, em tempo útil, defender-me num caso como este, quando são apreendidos quatro milhões de ficheiros eletrônicos, utilizados 1.100? Eu tenho que ter acesso, em primeiro lugar, a estes quatro milhões de ficheiros eletrônicos. Tenho que ter conhecimento de como é que o *software* forense específico funciona e, portanto, o caso coloca igualmente questões sobre a validação e a compreensão dos próprios algoritmos forenses utilizados. É, portanto, um caso que demonstra bem as novas problemáticas não só da investigação, mas do próprio julgamento, hoje em dia, nestes casos complexos.

/ ESTES
NOVOS TIPOS
DE CIBERATAQUES,
OS NOVOS MÉTODOS
DE INVESTIGAÇÃO,
IMPLICAM TAMBÉM
ALTERAÇÕES E UMA
CERTA CRISE DO
JUDICIÁRIO /

RETENÇÃO DE DADOS E A JURISPRUDÊNCIA DO TJUE

Para terminar, conforme já tinha antevisto, a questão da retenção de dados e a jurisprudência do Tribunal de Justiça da União Europeia, como sabem, o tribunal mais importante da União Europeia, que tem um poder imenso em sede de todo o tipo de direitos que envolvam o Direito na União Europeia. Subjacente a estes e aos diversos casos que foram sendo decididos pelo Tribunal de Justiça, colocam-se basicamente cinco questões:



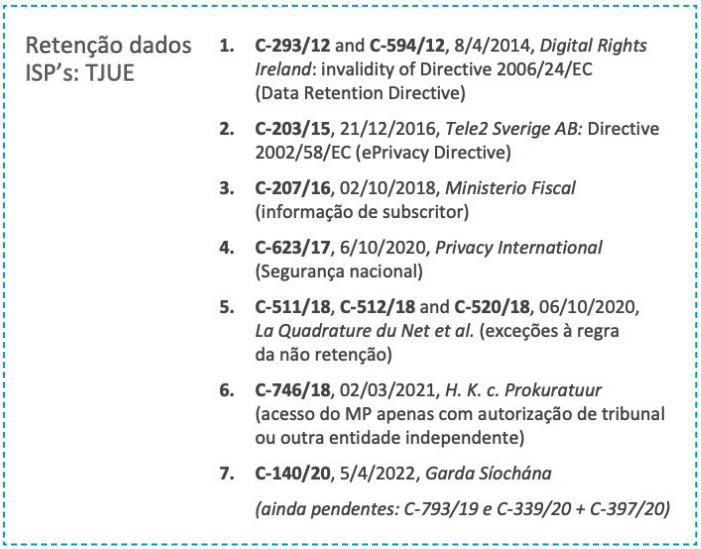
SCREENSHOT DA APRESENTAÇÃO

Quem é que retém os nossos dados, os tais dados de tráfego e localização? Ou seja, aqueles dados que as máquinas automaticamente geram quando realizamos comunicações eletrônicos, quer sejam enviados e-mails, quer seja por mero *browsing* de um site de finanças ou outro website qualquer. Portanto, todos esses registros, todas essas comunicações eletrônicos geram informações úteis, como, por exemplo: o IP de origem (ou o endereço Internet Protocol) e o IP de destino (ou seja, quem contatou com quem); que tipo de ficheiros foram trocados (por exemplo, se foram imagens ou documentos); e outros tipos de informações muito úteis, tais como a locali-

zação dos indivíduos quando estão a comunicar ou mesmo quando não estão a comunicar.

A segunda questão que se coloca é: para que são guardados estes dados por diversas entidades? Por quanto tempo é que guardam estes dados e quem pode aceder a estes dados e em que condições? E, por último, como são guardados ou mantidos, ou seja, quais são os mecanismos de segurança que os protegem contra *data leaks* ou fugas de dados?

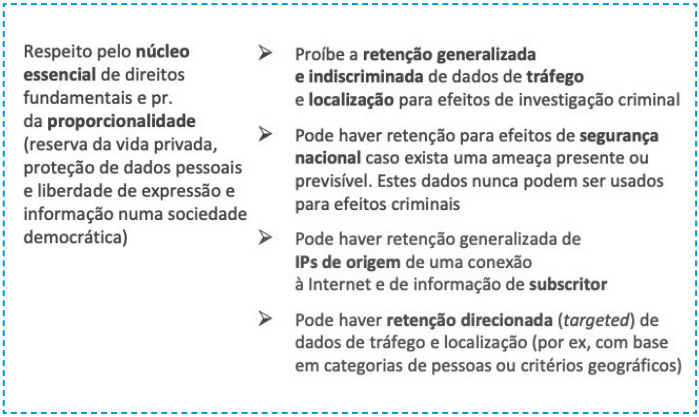
Foi no contexto da investigação criminal e também da segurança nacional que o Tribunal de Justiça foi chamado a pronunciar-se sobre a legitimidade desta retenção de dados que era imposta aqui na Europa por uma diretiva da União Europeia.



SCREENSHOT DA APRESENTAÇÃO

E como vemos aqui, já há sete decisões sobre esta matéria, desde 2014 até uma data recente, e ainda com alguns processos pendentes que estão aqui mencionados. Já há uma vasta

jurisprudência, uma jurisprudência muito complexa que tento resumir e simplificar, mas apontando, aqui, as principais questões ou conclusões desta jurisprudência do Tribunal de Justiça.



SCREENSHOT DA APRESENTAÇÃO

Em primeiro lugar, está em causa uma panóplia, um conjunto de direitos fundamentais que já foram referidos. Em segundo lugar, a reserva da vida privada e a proteção de dados pessoais, e o Tribunal de Justiça também não deixa de sublinhar a liberdade de expressão e informação numa sociedade democrática. Até porque, estando a sociedade sob vigilância 24/7, os fluxos de informação necessariamente se comprimem. As pessoas deixam de se comunicar, havendo uma redução da liberdade de informação, com prejuízo para a própria democracia - que vive de um fluxo livre, mais transparente possível, da informação.

Recordando também dois princípios fundamentais no âmbito dos direitos fundamentais, o respeito pelo núcleo essencial dos direitos e o princípio da proporcionalidade, ou seja, em caso de compressão do direito fundamental, terá que ser feita uma ponderação e, de acordo com o princípio da

necessidade, apenas poderá comprimir o direito fundamental na medida do estritamente necessário.

E, dentro deste contexto de Teoria Constitucional, as conclusões são, portanto, que o direito da União Europeia proíbe a retenção generalizada e indiscriminada de dados e localização para efeitos de investigação criminal, com duas exceções.

Mesmo ao nível de segurança nacional, a retenção só é possível caso exista, desde logo, uma ameaça presente ou previsível e, portanto, não bastará invocar, perante uma entidade independente, um possível ataque terrorista. Esse "ataque terrorista" a um grupo ou ao Estado terá que ser presente ou baseado em fatos concretos, de forma a ser previsível. E outra conclusão é a de que esses dados não podem depois ser utilizados ou aproveitados para efeitos de investigação criminal. Portanto, uma limitação muito grande é imposta ao poder das entidades investigadoras dos Estados Membros.

As duas exceções que o Tribunal de Justiça abre a este respeito são a retenção generalizada de IPs de origem de uma conexão à internet e a informação cadastral (que eu não designaria como a retenção de dados, porque a informação cadastral é aquela que qualquer cidadão dá quando faz um contrato com uma operadora de telecomunicações para ter ligação à Internet, por exemplo, o seu nome, "moradia" e outros dados pessoais).

Já quanto aos IPs de origem, o Tribunal de Justiça permite a sua retenção generalizada... e isto poderá parecer uma contradição com esta regra da proibição de retenção generalizada e indiscriminada. Mas o *ratio* ou razão de ser desta exceção pode ser pensada segundo um esquema muito simples: "como é que se processa o acesso à internet?" Devemos pensar que estão, de um lado as redes privadas, as redes locais que se ligam à internet através de uma operadora, e que portanto fornece os IPs dinâmicos com os endereços de Internet Protocol flutuantes ou variáveis por um determinado IP. E é através deste IP que depois

o cidadão ou a empresa vai consultar o eBay, o Amazon, o Google ou o Facebook, etc., ou seja, a Internet propriamente dita.

O que o Tribunal de Justiça está, portanto, a dizer, é que só podem reter o IP da ligação à Internet. Não podem reter os dados que indicam onde é que estava o cidadão ou empresa, em concreto, o que ela andou a fazer na Internet, ou seja, se visitou a Amazon, se utilizou o Facebook, o eBay ou outro site qualquer. Apenas podem reter o IP de origem. A razão de ser disto é evitar o *profiling* - saber que tipo de pessoa você é. Só a partir do rastreamento das atividades online é possível saber o que é que alguém consultou na internet. Portanto, esta é uma exceção muito importante porque, por exemplo, no mundo da pornografia infantil, sabemos que hoje conhecemos muitas vezes o IP de destino de um ficheiro contendo imagens proibidas, e com essa retenção de dados (por um ano ou dois), tornou-se possível navegar para trás no tempo e ver a quem pertencia aquele IP de destino, perguntando à operadora de serviços de Internet a quem estava atribuído o IP num determinado momento temporal específico.

Uma segunda exceção, que é muito controversa no Tribunal de Justiça, permite a retenção direcionada (em inglês, *targeted retention*). Outrossim adianto que esta retenção direcionada, já não generalizada, pode ser feita com base em categorias de pessoas ou critérios geográficos. Isto é extremamente difícil de implementar e extremamente controverso e delicado, porque, como poderão imaginar, como é que se escolhem as categorias de pessoas? O Tribunal de Justiça dá, por exemplo, alguém com cadastro ou com ligações a certos territórios. Há países em guerra e associados com o terrorismo, como por exemplo a Síria e, portanto, pessoas cadastradas, digamos assim, em determinados tipos de crime.

Mais controverso ainda é o critério geográfico, porque o próprio Tribunal de Justiça afirmou expressamente que, por exemplo, um local conotado estatisticamente com a prática de

crimes, pode ser sujeita a este tipo de retenção de dados. Podemos imaginar que o tráfico de droga, por exemplo, no Brasil, numa determinada favela, justificaria uma retenção direcionada para aquele bairro específico. Ora, isso, em termos do direito de igualdade e de "não-discriminação", parece-me evidentemente muito sensível e, porventura, criticável. Esta abertura a uma vigilância geo-localizada de acordo com critérios estatísticos, que o Tribunal de Justiça diz que são meros dados quantitativos e que não contêm nenhuma parcialidade ou nenhum *bias*... Mas permitam-me discordar do Tribunal de Justiça, uma vez que, como se vê, colocar uma determinada favela, um bairro social, sob vigilância, sob retenção direcionada de dados, em detrimento, por exemplo, de bairros chiques, onde vivem as classes mais favorecidas (porventura, onde habitam clientes dos traficantes), parece-me evidentemente altamente discriminatório, e neutro somente na aparência (estatística).

Ficaria então por aqui, abrindo um espaço para um possível debate, com perguntas e respostas, revelando a minha apresentação apenas alguns problemas que poderão ser desenvolvidos pelo debate.

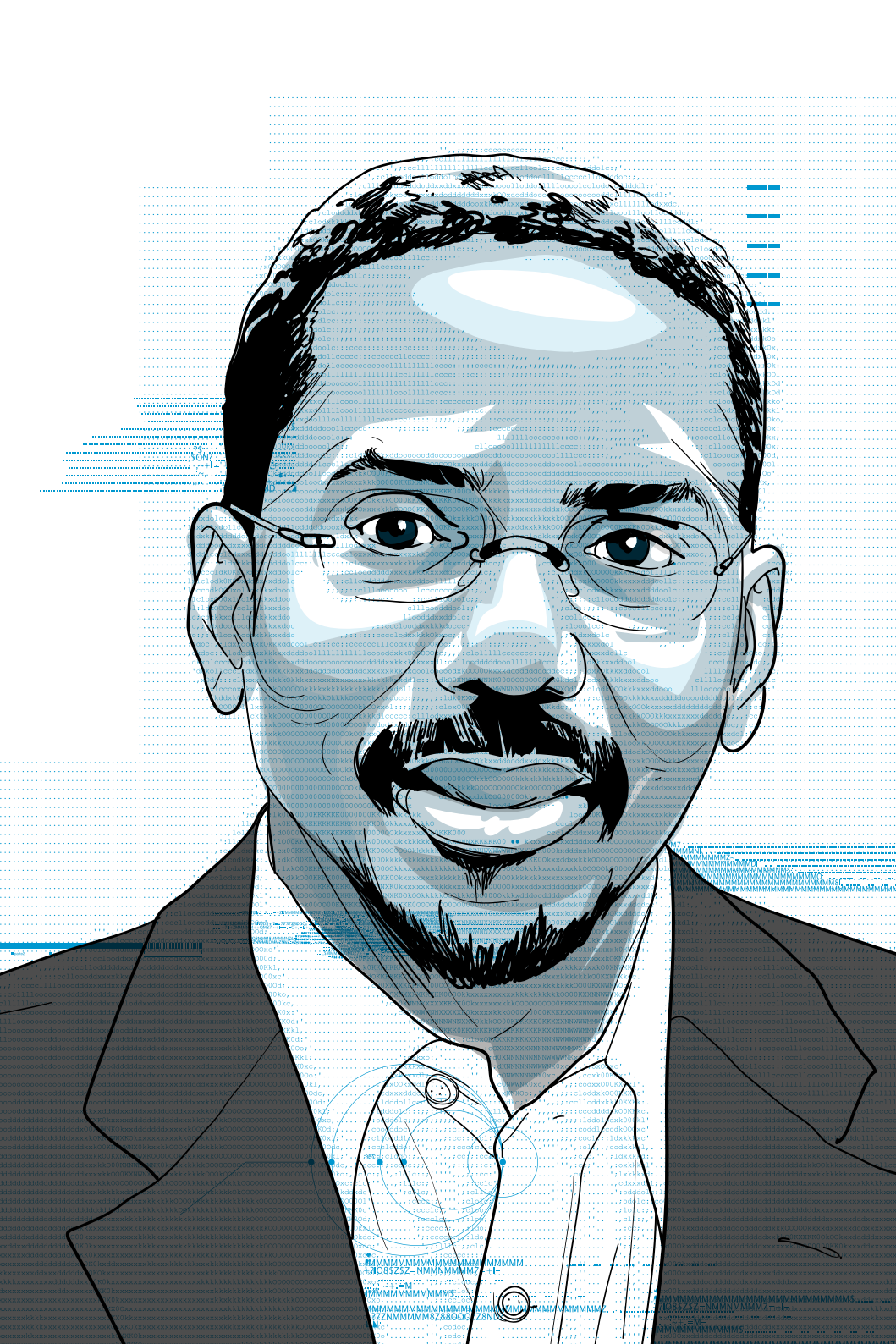
NOTAS

1. Este artigo foi adaptado a partir de palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022.

2. DELEUZE, G. Post-scriptum sobre las sociedades de control. Polis. Revista Latinoamericana, v. 13, 2006.

3. FOUCAULT, M. Vigiar e punir. Leya, 2014.

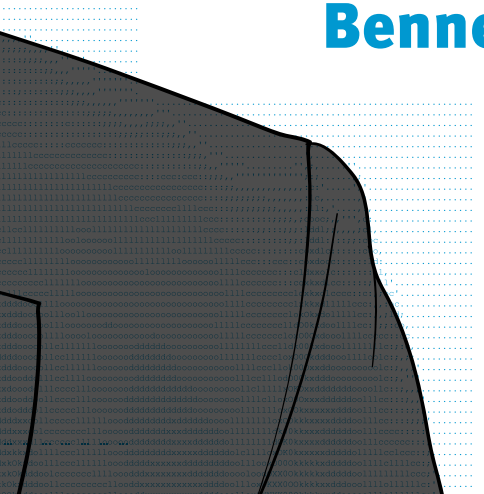
4. NEWMAN, Lily Hay. End-to-End Encryption's Central Role in Modern Self-Defense. **Wired**, Jul 5, 2022. Disponível em: https://shre.ink/9Zve. Acesso em: 11 abr. 2023.



02.

DESRACIALIZANDO A TECNOLOGIA DE POLICIAMENTO[1]

Bennett Capers



Obrigado! Muito obrigado por essa calorosa introdução!

Então, vou começar dizendo que quando a Bárbara Simão me convidou para fazer a palestra como keynote nesta conferência, eu disse "Sim!" bem rapidamente. Eu disse "Sim" porque fiquei intrigado com o tema "*Direitos Fundamentais do Processo Penal na Era Digital*". O e-mail dela também acrescentou - e vou citar o e-mail, se você não se importar - "*Consideramos sua participação de grande importância diante da situação brasileira. Atualmente, nosso Supremo Tribunal Federal reconhece o status constitucional da proteção de dados, e, no âmbito legislativo, apesar da promulgação da Lei Geral de Proteção de Dados Pessoais, ainda não temos uma lei geral voltada para proteger as informações coletadas para fins de processo penal ou segurança pública. Além disso, o Brasil tem um histórico de pouca fraca regulamentação do uso da força e de outros métodos de intervenção policial, e enfrenta um aumento na fiscalização das ações desses agentes e de seus preconceitos*".

Isso também me intrigou, obviamente. Também disse "*Sim*" ao convite por razões - o que eu acredito serem - completamente egoístas. Nunca me pediram para fazer uma palestra como keynote no Brasil antes. Então, uma parte de mim estava tipo "Uau, Brasil!" sabe, mesmo que seja via Zoom. E meu entusiasmo não é exatamente o que você pode pensar com base no que acabei de dizer. Acredito que, como a maioria dos estudiosos do direito americano, eu sei quase nada sobre os processos jurídicos fora dos Estados Unidos, o que significa que eu sei quase nada sobre os processos jurídicos, ou processos penais, no Brasil. Portanto, embora eu vá focar minha palestra na situação nos EUA, também estou esperando aprender com todos vocês durante as sessões de perguntas e respostas para obter um pouco de educação comparativa hoje.

No tempo que tenho, vou falar sobre minha própria exploração da justiça criminal, tecnologia e raça, que é uma das questões que mais me preocupa. Então, um pouco mais de contexto, abordo esse tema como professor de direito que escreve e ensina sobre o direito penal dos EUA e sobre as proteções constitucionais que limitam o que a polícia pode fazer. E, obviamente, por essa razão, provavelmente me destaco nesta conferência. Mais uma vez, sou um estrangeiro em relação à sua jurisprudência. Também abordo esse tema como um homem negro. E nos EUA, isso significa - e suspeito que signifique a mesma coisa no Brasil - que estarei sempre sujeito a uma "hipervigilância" por causa da cor da minha pele e também por causa do meu gênero.

Sabe, alguns anos atrás, um jovem acadêmico escreveu um artigo que eu adoro por causa de seu título. E o título era "*Jovem + Negro + Masculino = Justa Causa*". Então, suspeito que eu já não me enquadro mais na parte "jovem", mas ainda sou um homem negro, o que significa que ainda estou sujeito a muita vigilância e escrutínio policial.

Também abordo esse tema como um ex-promotor federal, e eu pertencia a um escritório que, como parte da guerra às drogas, processava muitos negros e hispânicos, além de outros casos de crimes de colarinho branco. Mas lá, eu vi em primeira mão como a tecnologia era, e *não era*, usada na aplicação da lei. Então, trago muitas das minhas pesquisas e trabalhos acadêmicos, como você sabe, como professor de direito, como homem negro e como ex-promotor federal. E tento trazer tudo isso à mesa quando penso em justiça criminal, raça e tecnologia.

Acredito que dizer um pouco sobre esse contexto provavelmente explica por que, mesmo escrevendo sobre tribunais e direito, tenho pouca esperança de que os tribunais corrijam as desigualdades que enxergo no sistema de justiça criminal.

E provavelmente também explica por que, cada vez mais, concentro mais na parte de tecnologia do que na parte de direito.

Também devo dizer desde o início que o argumento que vou apresentar hoje pode ser diferente do que a maioria de vocês está esperando. Minha palestra não vai realmente tratar da proteção de dados. Fico feliz em falar mais sobre isso na sessão de perguntas e respostas, e posso dizer brevemente que, nos EUA, é basicamente seguro assumir que não há proteção de dados quando se trata da aplicação da lei. Nós simplesmente fazemos exceções para a aplicação da lei. Em vez disso, vou me concentrar em meu curto tempo apenas nas questões de tecnologia, policiamento e raça.

Participo de muitas conferências sobre policiamento e tecnologia, e geralmente a mensagem nessas conferências é sempre a mesma: a vigilância é um ataque insidioso à nossa liberdade. É algo que se ouve frequentemente ou, para citar outro estudioso: "*é praticamente impossível viver hoje sem gerar milhares de registros sobre o que assistimos, lemos e fazemos, e o governo tem fácil acesso a eles*". Sabe, a mensagem é: "*O Grande Irmão está nos observando e devemos ter medo*".[2]

E embora essas preocupações não sejam infundadas, meu interesse acadêmico na interseção entre justiça criminal e tecnologia é diferente. O que me interessa é aproveitar a tecnologia para eliminar preconceitos e desracializar o policiamento.

Como escrevi anteriormente, a possibilidade de o Grande Irmão nos observar não precisa ser assustadora. Então, em vez de uma visão da tecnologia que pareça distópica, quero imaginar o bem que a tecnologia pode fazer. Na verdade, o que quero sugerir é que, se realmente nos importamos em tornar o policiamento mais igualitário e justo para todos, isso provavelmente significa mais tecnologia, não menos. E certamente significará a redistribuição da privacidade.

Há alguns anos, escrevi um artigo intitulado "Afrofuturismo, Teoria Crítica da Raça e Policiamento no Ano de 2044". E é sobre o policiamento no ano de 2044 que quero discutir agora. E a propósito, 2044, escolhi esse ano porque é o ano em que, nos Estados Unidos, prevê-se que a população branca deixará de ser maioria para se tornar uma *maioria minoritária*. Essa era a ideia por trás do artigo. E a parte de 2044 foi realmente focada não apenas no que as mudanças demográficas podem significar, mas também em como os avanços tecnológicos podem mudar radicalmente o policiamento como o conhecemos, mas de maneiras que possamos receber de braços abertos.

Especificamente, era uma forma de eu pensar em tecnologias que podem melhorar a segurança da comunidade e levar a um policiamento mais igualitário. Tenho pensado em como as tecnologias podem reduzir o uso da força policial, especialmente contra nós, que somos negros. E, em resumo, uma coisa que eu estava fazendo em minhas pesquisas era tentar encontrar maneiras de incentivar as comunidades que enfrentam a maior parte do policiamento desigual a pensar seriamente sobre quais tecnologias poderiam realmente beneficiá-las. Existem tecnologias disponíveis que podem lidar com problemas persistentes que vemos repetidamente no policiamento?

Vou dar alguns exemplos do que quero dizer com isso. Podemos aproveitar a tecnologia para contribuir para a redução da criminalidade? Para isso, quero que você considere algumas das tecnologias que já temos e as tecnologias futuras que podemos facilmente imaginar.

Geralmente, com o uso da tecnologia de reconhecimento facial ou outras tecnologias biométricas, tendemos a pensar em como essas tecnologias são falhas e protestamos contra seu uso.

Por exemplo, com a tecnologia de reconhecimento facial, uma das preocupações que se ouve repetidamente nos Estados

Unidos é que ela tem dificuldade em reconhecer rostos de pele mais escura. Mas também devemos pensar em como essas tecnologias podem ser aprimoradas. Portanto, em vez de desistir delas, devemos pensar em como podem ser aperfeiçoadas, como podemos resolver as imperfeições e como melhorar essas tecnologias pode contribuir para a segurança pública de maneiras que não sejam discriminatórias.

O que gosto de fazer é incentivar as pessoas a pensar nessas mesmas tecnologias que acabei de mencionar, mas pensar nelas sem as falhas. E, você sabe, acrescentando a isso, que essas tecnologias poderiam dar às autoridades policiais acesso quase instantâneo a grandes volumes de dados.

Imagine agora - na verdade, há anos - que temos experimentado com *scanners*, *scanners terahertz*, que a polícia pode usar para verificar remotamente se alguém possui uma arma de fogo ilegal. Pense na disponibilidade generalizada de tecnologias de comunicação de curto alcance que poderiam eliminar completamente a necessidade de abordagens policiais em tráfego, ou até mesmo pense em como o surgimento de carros autônomos pode eliminar a necessidade de abordagens em tráfego. Pense no uso de *drones* autônomos. Pense em adicionar aprendizado de máquina e pense em uma série de coisas que alguns de vocês podem ter ouvido falar.

Em Nova York, onde estou agora, o Departamento de Polícia de Nova York está sendo processado por coletar secretamente DNA de suspeitos secretamente. Também há um processo em Nova Jersey que vai além disso. Em Nova Jersey, a polícia é acusada de usar DNA coletado de recém-nascidos para auxiliá-los em uma investigação policial. E quando as pessoas ouvem isso, geralmente ficam indignadas, mas podemos facilmente imaginar um mundo onde a coleta de DNA não seja apenas autorizada, mas geralmente aceita, onde evidências de DNA são coletadas de indivíduos desde o nascimento, juntamente com outros dados,

para que o DNA de qualquer pessoa esteja registrado. E tudo isso obviamente contribuiria para dissuadir a atividade criminosa e melhorar a apreensão quando houver atividade criminosa.

E eu sei que tudo isso pode parecer assustador. Essa é geralmente a resposta que recebo. Mas antes de abordar isso, considere algo mais. As tecnologias sobre as quais estou falando também têm o potencial de reduzir a violência policial injustificada. Câmeras de vigilância, incluindo câmeras mantidas por indivíduos, provavelmente já dissuadem algum comportamento indevido por parte da polícia. Mas imagine o que acontece quando adicionamos outras tecnologias.

Novamente, se tivermos *scanners* que possam informar a polícia se o suspeito está armado ou não, por "isso" que poderia impactar o tipo de uso de força necessária. *Scanners*, que estão ligados ao acesso a grandes volumes de dados, provavelmente também poderiam informar à polícia em questão de segundos se alguém possui um histórico de não violência e, assim, reduzir o risco de escalada. Também poderíamos imaginar tecnologias futuras que permitiriam à polícia desativar armas à distância.

Além disso, todas essas tecnologias sobre as quais falei até agora deixam um rastro de dados para criar mais responsabilidade no final. Já temos policiamento preditivo, algoritmos e ferramentas de avaliação de riscos, e temos certeza de que essas ferramentas têm falhas. Mas e se pudéssemos melhorar isso? Igualmente importante, e se pudéssemos virar o jogo? Não sei exatamente como isso seria traduzido para o português, mas e se pudéssemos mudar as coisas e usar as mesmas ferramentas para prever quais policiais têm maior risco de envolvimento em uso injustificado dae força?

Novamente, antes de descartarmos as tecnologias sem pensar, devemos considerar seriamente como as tecnologias podem beneficiar o restante de nós. Também tenho explorado como as tecnologias podem ajudar a reduzir a violência poli-

cial, a desracializar a polícia em geral, afinal, as câmeras não têm preconceitos implícitos nem sofrem de racismo inconsciente. A tecnologia pode nos aproximar, sabe, como nos EUA, em que é necessária uma suspeita razoável real[3] antes que um policial possa abordar alguém. A tecnologia pode nos aproximar de uma suspeita razoável real, para que as aparências, os encontros, as abordagens e as revistas se baseiem em uma suspeita razoável real, em vez de se basearem simplesmente em coisas como raça, masculinidade e idade.

Como já escrevi antes, *scanners* de armas poderiam dizer à polícia que um volume no bolso de um homem negro - ou de um adolescente negro - é apenas um celular volumoso, mas que o turista branco que parece ser do Texas realmente está armado. Sabe, a tecnologia de reconhecimento facial com acesso a grandes volumes de dados informaria à polícia que o motorista de pele morena que circula repetidamente o quarteirão é, na verdade, alguém que trabalha no bairro e está apenas procurando uma vaga de estacionamento. E que o rapaz bem-apessoado sentado no banco do parque é, na verdade, um agressor sexual registrado que está muito perto de um parquinho.

De uma maneira não intrusiva, ela informaria à polícia se alguém é um arruaceiro observando uma vizinhança ou um estudante voltando para casa com uma sacola de Skittles e uma garrafa de chá gelado. Ela informaria à polícia se alguém é um invasor prestes a cometer um roubo residencial ou um professor de Harvard entrando em sua própria casa. Ela informaria à polícia se alguém é um bandido armado ou se essa pessoa é o chefe de polícia. Ela informaria à polícia se aquela pessoa é um invasor tentando entrar no prédio do Capitólio ou um senador dos Estados Unidos, ou informaria à polícia se a pessoa está procurando sua próxima vítima ou um futuro procurador-geral dos Estados Unidos, e diria se o garoto branco dirigindo em um bairro negro está lá para obter drogas ou para encontrar sua namorada negra.

/ JÁ TEMOS POLICIAMENTO PREDITIVO, ALGORITMOS [...], E ESSAS FERRAMENTAS TÊM FALHAS. MAS E SE PUDÉSSEMOS MELHORAR ISSO? /

/ O QUE ME INTERESSA É APROVEITAR A TECNOLOGIA PARA ELIMINAR PRECONCEITOS E DESRACIALIZAR O POLICIAMENTO /

E, a propósito, estou assumindo que a maioria das pessoas no Brasil não está familiarizada com as referências do que eu estava dizendo, mas basicamente eu estava fazendo referência a todos esses casos nos EUA em que a polícia realmente parou um professor de Harvard, ou um senador dos EUA, ou um futuro procurador-geral dos EUA pensando que estavam envolvidos em atividades criminosas quando não estavam, e eles foram parados principalmente por causa de sua cor de pele.

Por fim, quero argumentar que o uso de mais tecnologia pode ajudar a resolver um problema que raramente recebe a atenção que merece, pelo menos nos Estados Unidos. E esse problema é algo chamado subaplicação da lei (*under-enforcement*), e não sei se isso é um problema no Brasil. Novamente, minhas desculpas, mas definitivamente é um problema nos EUA. O que quero dizer com subaplicação da lei é o seguinte: ao mesmo tempo, as comunidades de cor nos Estados Unidos sofrem com a superaplicação (*overenforcement*) da lei e a o superpoliciamento. Elas também sofrem com o oposto, a subaplicação da lei.

Numerosos estudos confirmam que a polícia é menos propensa a investigar e processar crimes violentos ou contra a propriedade em comunidades de cor. Estudos também mostram que os departamentos de polícia têm uma taxa de resposta mais lenta para os bairros minoritários quando as pessoas chamam a polícia, mesmo quando o bairro minoritário e o bairro não minoritário estão igualmente distantes da delegacia de polícia. E tudo isso acaba enviando uma mensagem de desprezo e desvalorização às comunidades minoritárias.

Mas pense em todas as tecnologias que descrevi e em como elas assumiriam grande parte do trabalho que a polícia faz atualmente. Se isso for verdade, pode liberar os policiais para fazer o que realmente queremos que eles façam, que é investigar e resolver crimes. Mais uma vez, não sei quais são os números no Brasil, mas nos Estados Unidos, quase um terço de todos os

assassinatos neste país permanecem sem solução. Para cada três pessoas mortas, apenas duas são presas. O número é ainda maior para outros tipos de crimes. E isso me preocupa bastante.

Neste ponto, vou apenas dizer mais algumas palavras sobre o quão assustadora essa ideia pode parecer para algumas pessoas. Sei que as tecnologias que estou descrevendo podem parecer invasivas da privacidade. E reconheço também que as tecnologias atuais não são racialmente neutras. Reconheço também que a tecnologia tem sido tudo menos uma mera espectadora quando se trata do encarceramento em massa nos Estados Unidos.

A socióloga Ruha Benjamin, da Universidade de Princeton, cunhou o termo "*o novo código The New Jim Code*",[4] uma referência ao livro "*O Novo Jim Crow*", de Michelle Alexander, para alertar que a tecnologia pode perpetuar e agravar desigualdades, especialmente quando têm a aparência, a ilusão de serem livres de influências humanas e preconceitos.

Mas, mais uma vez, nada disso sugere que a tecnologia tendenciosa seja inevitável. Vieses podem ser identificados e eliminados, ou pelo menos minimizados. Deixe-me dar um exemplo. Vou voltar brevemente para o reconhecimento facial como ilustração disso. Como mencionei antes, uma das críticas ao reconhecimento facial nos EUA é a dificuldade de reconhecer rostos negros e as identificações erradas que ocorrem.

E as pessoas dizem "isso é uma falha que não pode ser corrigida". Mas elas deixam de reconhecer que isso tem mais a ver com os vieses de entrada e saída (*bias-in and bias-out*). Tudo isso tem a ver com quais são as entradas (os *inputs*). E o que quero dizer com isso é que devemos considerar o fato de que a tecnologia de reconhecimento facial desenvolvida e utilizada no Japão e na China tem dificuldades em reconhecer rostos brancos. Não é a tecnologia que tem dificuldades em reconhecer rostos; basicamente, é o que é inserido nela. Isso sugere que adicionar mais entradas ou corrigir as entradas pode resolver o problema do reconhecimento de pele escura.

Isso também leva ao meu argumento geral de que quero enfatizar, porque o que realmente quero fazer é imaginar pessoas mais diversas participando do processo de criação de tecnologia e dizendo que tipo de tecnologia desejam.

Grande parte do meu trabalho é imaginar uma *abordagem ascendente* (*bottom-up*) para a tecnologia, não uma abordagem descendente (*top-down*). Atualmente, as empresas nos Estados Unidos que desenvolvem novas tecnologias basicamente as criam por conta própria e depois as vendem para as forças policiais, que as utilizam contra as pessoas.

Seria bom imaginar um mundo onde as pessoas realmente digam que tipo de tecnologia desejam, ajudem a criá-la e depois digam à polícia como usá-la. Grande parte do meu trabalho é imaginar os benefícios que fluiriam para as comunidades mais policiadas, tendo a capacidade de produzir tecnologia, criar código, recodificar e talvez, como os jovens dizem, "*lançar um remix*". Então, novamente, emprestando as palavras de Ruha Benjamin, o que me interessa é pensar em como a tecnociência pode ser apropriada e reimaginada para fins mais justos.

Acho que vou encerrar por aqui. Como disse, estou feliz em falar mais sobre raça, policiamento e tecnologia. Também estou feliz em falar um pouco sobre proteção de dados, e é isso.

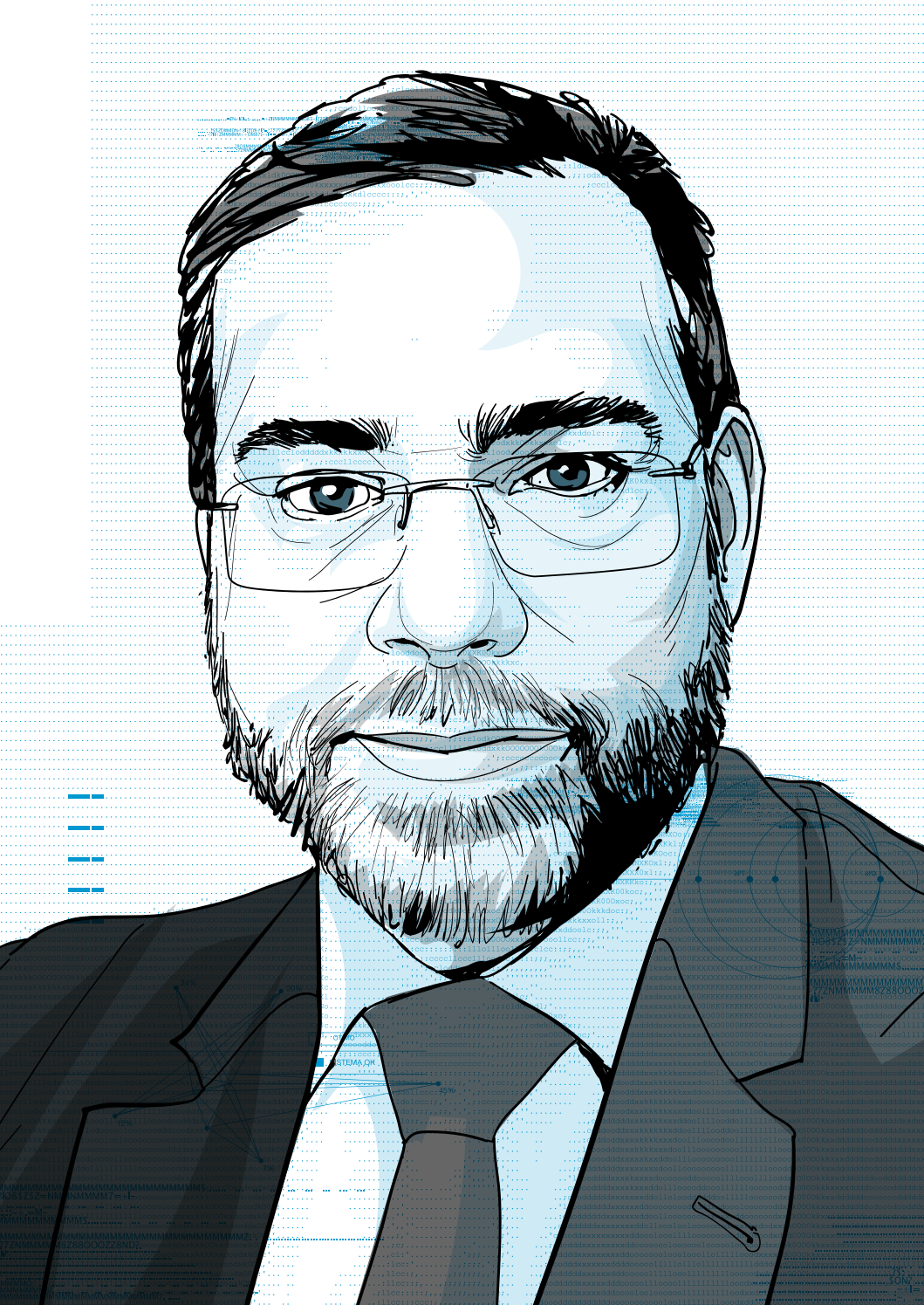
NOTAS

1. Este artigo foi adaptado a partir de palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022

2. Tradução livre de "*Big Brother is watching and we should be afraid*", em referência à obra 1984 de George Orwell.

3. N/E: Em inglês, *probable cause* - que corresponde ao conceito penal de justa causa ou suspeita fundamentada"

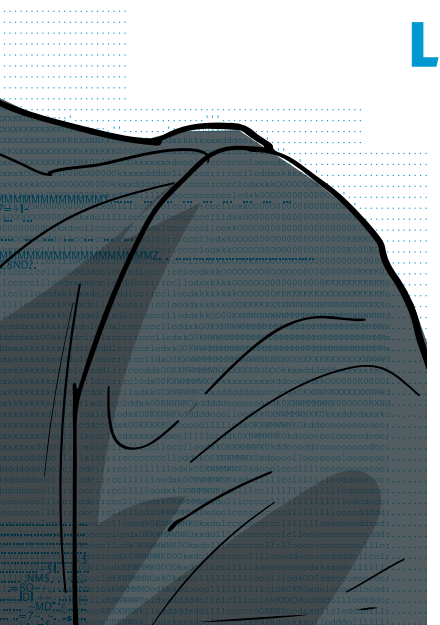
4. Tradução livre de "The New Jim Code", em referência a um código em linguagem de máquina que se assemelhe à legislação segregacionista Jim Crow.



03.

PERSPECTIVAS PARA A NEGOCIAÇÃO DA CONVENÇÃO DAS NAÇÕES UNIDAS SOBRE CRIME CIBERNÉTICO[1]

Eric do Val Lacerda Sogocio



Gostaria de, primeiramente, agradecer muito a oportunidade de estar aqui e falar nesta Casa do Direito a uma plateia tão distinta. Agradeço ao Doutor Francisco Brito Cruz e à Doutora Marta Saad, da Faculdade de Direito da USP; ao Doutor Alexandre Au-Yong Oliveira, do Centro de Estudos Jurídicos de Portugal pela brilhante palestra; a minha colega de painel, Veridiana Alimonti, da Electronic Frontier Foundation, assim como à pesquisadora Laura Matta.

Meu nome é Eric Sogocio, sou diplomata na Missão do Brasil em Viena e conselheiro da carreira diplomática. Ao longo de minha carreira tenho me engajado em temas relacionados ao combate ao crime em geral e, especificamente, ao combate ao crime cyber-dependent. Fui eleito um dos vice-presidentes do Comitê AD HOC para negociar a convenção das Nações Unidas sobre crimes cibernéticos e tenho chefiado as negociações por parte do Brasil.

Em minha exposição responderei a algumas perguntas:

< 01 > Porque uma convenção das Nações Unidas sobre crimes cibernéticos é necessária?

< 02 > Onde estamos na construção desse tratado e como chegamos até aqui?

< 03 > Quais são os principais pontos a serem incluídos no instrumento internacional e as prioridades para a convenção?

< 04 > Quais seriam os riscos e desafios da negociação?

< 05 > Quais seriam os riscos e desafios da aplicação da convenção, uma vez em vigor?

NECESSIDADE DE UMA CONVENÇÃO DAS NAÇÕES UNIDAS SOBRE CRIME CIBERNÉTICO

No que diz respeito à primeira questão, há que ter em mente que o crime cibernético tem características especiais. Nesse sentido, geralmente dividimos em crime cibernético propriamente dito, próprios, (*cyber-dependent crimes*), aqueles cometidos contra sistemas informáticos, estes podemos chamar de crimes "novos", por exemplo: "invasão de dispositivo informático", da lei 12.737/2012 – lei Carolina Dieckman, que acresceu o art. 154-A ao Código Penal. Assim como aqueles descritos na Convenção do Conselho da Europa sobre Cibercrime, também conhecida como Convenção de Budapeste.

Temos, também, os crimes cibernéticos impróprios (*cyber-enabled crimes*) crimes comuns ou já tipificados, mas que possuem importante componente cibernético. Importante fazer essa distinção pois muda o modo como são tratados nas convenções sobre crime cibernético.

Ambos os tipos de crime cibernético têm em comum o fato de que o fator localização, territorialidade se torna impreciso. A vítima está em um lugar, os perpetradores em outro, os provedores de internet em um terceiro lugar, os dados armazenados em um quarto lugar, ou mesmo divididos entre localizações distintas. As fronteiras entre os países, nesse sentido, ficam esmaecidas. A movimentação no mundo virtual é praticamente livre, como se as fronteiras nacionais tivessem se apagado. (Quem retém nossos dados, conforme indagou o Dr Alexandre Oliveira). Mas especialmente aqui, na Casa do Direito, sabemos que esse não é o caso. As jurisdições nacionais são aquelas que têm o dever de coibir, investigar e processar crimes.

Temos, então, um descompasso essencial, que apenas pode ser contornado por meio da cooperação entre as diferentes ju-

risdições. É necessário que as entidades que investigam tenham acesso a informações que estão em outros territórios, em outras jurisdições. Não apenas isso, as informações intercambiadas devem possuir a formalização necessária para que sejam aceitas em processos criminais.

Então, o quadro em que esses intercâmbios acontecem é a cooperação jurídica internacional em assuntos criminais. Isso pode ser feito com base em tratados bilaterais de assistência jurídica mútua, e o Brasil tem acordos com 22 países. Na falta de um tratado bilateral específico, essa cooperação e intercâmbio pode ser feita com promessa de reciprocidade, uma tradição internacional, ou pode ser feita com base em tratados e vários tratados podem basear essa cooperação.

Vários tratados podem basear essa cooperação:

A Convenção de Budapeste, que conta hoje com 66 Estados membros e 16 convidados. Trata-se de instrumento específico para a cooperação no combate ao crime cibernético. O Brasil aderiu à Budapeste em 30 de novembro de 2022.

A Convenção das Nações Unidas contra o Crime Organizado Transnacional e seus Protocolos – esta não trata especificamente de crime cibernético, mas prevê a cooperação jurídica internacional sobre quaisquer "*serious crimes*", crimes que têm como pena ao menos quatro anos de prisão. Esta conta com 190 Partes, 185 Países Membros das Nações Unidas, ou seja, constitui instrumento de aceitação praticamente universal.

Pode-se argumentar que, tendo em vista as três possibilidades que mencionei, não seria necessária uma convenção específica da ONU que tratasse de crime cibernético. Afinal há meios para intercambiar esse tipo de informação.

Entretanto, os crimes cibernéticos têm especificidades. Uma delas, que já mencionei, é a possibilidade de que investigações envolvam várias jurisdições. O Dr. Alexandre Oliveira

deu um excelente exemplo de investigação conjunta em sua apresentação. Brasil, Espanha e Estados Unidos.

A fugacidade dos dados constituem outra especificidade dos crimes cibernéticos. Os dados podem ser movidos, manipulados, apagados. A cooperação tradicional demanda tempos que são analógicos. No que diz respeito à cooperação tradicional, o Brasil tem defendido e incentivado a que o intercâmbio de informações seja feito por meios eletrônicos, o que requer o tempo fugaz de um email. Há, entretanto, ainda hoje, países, mesmo desenvolvidos, que requerem que os documentos sejam tramitados em papel, com carimbos, assinaturas. Pelo correio, ou por Mala Diplomática. Processo de semanas ou mesmo de meses. Até lá, o que terá sido feito da prova eletrônica?

Além da necessidade de que os intercâmbios tenham a velocidade do mundo virtual, um outro fator a recomendar uma nova convenção é que, para muitos territórios, a cooperação apenas pode se dar se o ato for criminalizado nas duas jurisdições cooperantes. Assim como a Convenção de Budapeste, como a Convenção sobre Crime Organizado da ONU, como a Convenção sobre Corrupção da ONU, a nova convenção deverá tipificar certos crimes, em especial crimes propriamente cibernéticos. Em muitos casos, essa tipificação é o que vai possibilitar a cooperação e a troca de informações.

Uma terceira questão muito relevante deverá ser o estabelecimento de padrões de direito processual. Vemos a necessidade de que a convenção tenha como cerne a possibilidade de preservação expedita de dados e o intercâmbio de provas eletrônicas. Trata-se de tornar inteligíveis procedimentos de distintos sistemas jurídicos, de modo a permitir que essas ações sejam efetivadas com a velocidade da internet, das relações eletrônicas. A preservação de provas virtuais deve, também, ter a agilidade da própria internet, mais uma vez.

Assim, a tipificação de certos crimes, ou seja, inovações de direito substantivo, aliada a padrões acordados de direito processual será o que dará consistência, velocidade e utilidade para a convenção das Nações Unidas.

O PROCESSO DE NEGOCIAÇÃO

Como chegamos até aqui? Qual o estado das negociações da convenção? O comitê *ad hoc* foi criado por uma resolução da Assembleia Geral das Nações Unidas em dezembro de 2019, teve uma reunião em fevereiro de 2020, logo quando iniciou a pandemia, passou um ano sem poder se reunir, reuniu-se de novo em maio de 2021 e acordou ali regras de procedimento para as negociações, por meio da Resolução 75/283, cujo parágrafo a ser destacado é este:

> 5. *Also decides that the Ad Hoc Committee shall hold the first, third and sixth negotiating sessions in New York and the second, fourth and fifth sessions in Vienna and shall be guided by the rules of procedure of the General Assembly, while all decisions of the Committee on substantive matters without approval by consensus shall be taken by a two-thirds majority of the representatives present and voting, before which the Chair, upon a decision of the Bureau, shall inform the Committee that every effort to reach agreement by consensus has been exhausted*;[2]

Alguns pontos são importantes nessas regras de procedimento que tornam a negociação diferente de muitas que acontecem. Uma delas é que as negociações acontecem em Viena, onde eu estou baseado e de onde estou falando agora, e em Nova York, ou seja, há alternância de sede. A primeira

reunião foi em Nova York, a segunda reunião foi em Viena, a terceira reunião que começa na semana que vem por duas semanas acontecerá em Nova York, a quarta e a quinta reunião em Viena, a sexta reunião em Nova York e a sétima reunião final para a adoção do documento em Nova York.

Essa alternância de sedes decorre da necessidade de incluir a maior quantidade possível de países. Apesar de nem os membros das Nações Unidas estarem representados em Viena, todos contam delegações em Nova York. Trata-se de desafio adicional às negociações a organização de reuniões em duas sedes, bem como, para os países, a necessidade de transladar negociadores entre uma cidade e outra. Tanto que eu estou em Viena, mas semana que irei para Nova York a fim de participar da terceira sessão organizacional.

Um outro ponto importante relaciona-se com a emenda proposta pelo Brasil, que traz para a negociação uma regra de quase consenso. O consenso para o Brasil e para muitos países era muito importante nessa negociação, por alguns motivos que logo comentarei. Muitos países, no entanto, eram contrários a uma negociação por consenso. Nesse contexto, o Brasil propôs uma fórmula, junto com outros países latino-americanos, que dificulta que as negociações sejam sequestradas por um país do grupo de países. A regra da Assembleia das Nações Unidas, para caso de voto em temas substantivos, estabelece que uma decisão por voto deve ser tomada por maioria simples. Na emenda proposta pelo Brasil, decisões por voto serão tomadas por maioria de dois terços. Além disso, a presidente do Comitê apenas pode trazer uma decisão para ser votada se os membros da mesa (e o Brasil é parte dela, eu sou um dos vice-presidentes), concordarem que não há mais a possibilidade de chegar a um consenso. Esses procedimentos constituem travas que impedem que a convenção seja sequestrada e passe a ser negociada e adotada por voto.

Esse modo de tomar decisões é importante porque do nosso ponto de vista é essencial que a convenção seja adotada por consenso e que tenha, portanto, o potencial de tornar-se universal, como já o são as outras convenções das Nações Unidas sobre crime: a Convenção sobre crime organizado, que já mencionei, com 191 Partes e a Convenção Contra a Corrupção, com 189 Partes. De nosso ponto de vista é essencial que a convenção sobre crime cibernético constitua instrumento universal a fim de evitar que territórios venham a se tornar lugares de abrigo para criminosos virtuais.

Continuando sobre o processo, houve uma primeira sessão negociadora em Nova York, em março de 2022. A segunda aconteceu em Viena, em junho de 2022. A terceira vai acontecer agora em Nova York, em setembro de 2022. Estão ainda previstas duas reuniões consecutivas em Viena (janeiro e abril de 2023), assim como duas reuniões finais em Nova York (agosto de 2023 e janeiro de 2024). A metodologia tem sido receber dos países propostas de texto da Convenção, com base nessas propostas a presidência cria perguntas sobre temas-chave trazidos pelos países, indaga sobre decisões a serem tomadas, ao se construir o texto. Para as duas reuniões finais em Nova York a presidência proporá minuta de convenção sobre a qual deverão ser finalizadas as negociações.

A terceira sessão que acontece em Nova York na semana que vem vai seguir a mesma metodologia e vai abordar os capítulos de cooperação internacional, assistência técnica, prevenção e outros. A partir da quinta sessão, haverá uma minuta inicial, como mencionei, e os países vão passar a debater um texto concreto e, espera-se, terminar as negociações até o início de 2024 – quando a Convenção deveria ser adotada, preferencialmente, como eu falei, por consenso.

O Brasil transmitiu, como proposta nacional, textos completos de conversão e tem buscado construir pontes entre

/ POR UM LADO, NÓS QUEREMOS QUE O TEXTO DA CONVENÇÃO SEJA ADOTADO POR CONSENSO. POR OUTRO, [...] CHEGAR A UM CONSENSO É UM DESAFIO /

/ A CONVENÇÃO NÃO TEM CAPACIDADE DE INSTITUIR OU DE AUMENTAR, POR ELA MESMA, O NÍVEL DE RESPEITO AO DEVIDO PROCESSO LEGAL EM UM PAÍS /

pontos de vista distintos, em especial entre os países que são parte da Convenção de Budapeste, que adotam visão muito específica sobre como deveria ser a convenção, e alguns países que não são partes da Convenção de Budapeste, mas atribuem grande prioridade para a convenção. Nas propostas, o Brasil inclui partes tiradas da Convenção de Budapeste e também traz propostas, por exemplo, da Rússia e da China, bem como oferece propostas originais. Por exemplo, na parte de criminalização, o Brasil introduziu proposta de que a convenção tipifique a coerção ao suicídio, a fim de refletir o que nós temos na Lei 13.969/19, atribuindo pena de dois anos de reclusão. O fator cibernético dessa lei é que ela aumenta a pena em até o dobro, se o incitamento ao suicídio for feito pela internet, bem como aumenta pela metade, se o agente for coordenador de grupo ou rede virtual.

Uma outra proposta original do Brasil é a que criminaliza o acesso ilegal a senhas e credenciais, e a ideia é criminalizar a pessoa que fica no meio. A Convenção de Budapeste criminaliza a obtenção e a venda de dados, de senhas e credenciais. Nós vemos que há uma lacuna sobre uma ação que seria ter as senhas, fornecê-las, mas, convenientemente, não ter conhecimento de como terão sido utilizadas essas credenciais de acesso. Essa adição seria importante, pois o modelo estabelecido pela Convenção de Budapeste inclui a transferência a terceiros de senhas e credenciais para cometimento de crime. Se a pessoa não participa e não tem conhecimento do uso que se dará dessas credenciais, não será alcançada por essa criminalização.

AS PRIORIDADES PARA O BRASIL

Bom, um penúltimo ponto: prioridades para a convenção. O que para nós é importante?

Em primeiro lugar, o tema da criminalização, a tipificação comum de certos crimes, ou seja, o direito substantivo. Nós fazemos a distinção na discussão entre crimes cibernéticos próprios e impróprios. Os próprios devem estar ali, como estão na Convenção de Budapeste. Há uma questão relativa aos impróprios, ou seja, todos os outros crimes que podem ter um componente virtual importante. Do nosso ponto de vista, esses não precisam entrar, por um ponto que eu vou colocar daqui a pouco.

O segundo ponto é o direito processual. A Convenção deve proporcionar meios para preservação e de intercâmbio expedido de provas, bem como estabelecer com que os países harmonizem minimamente ações domésticas de preservação com o intercâmbio de provas por meio da cooperação internacional.

O terceiro ponto é o que alguns países chamam *e-evidence*, ou seja, que os procedimentos estabelecidos pela convenção, por exemplo, o direito processual que ela vai estabelecer, possam ser aplicados não apenas para os crimes tipificados, mas por qualquer outro crime que tenha importante componente cibernético. Então, por exemplo, provavelmente um crime de sequestro não será tipificado pela convenção, mas, por meio desse instrumento internacional, as autoridades poderão cooperar e obter dados e informações para investigar ou processar esse crime.

O consenso para que ela seja amplamente aceita e dificulte a existência de *safe havens*, onde criminosos podem ter mais facilidade de agir, seria um quarto ponto. Adicionalmente é importante que a Convenção seja um acordo que possa ser aperfeiçoado e atualizado por meio de protocolos, a exemplo da Convenção de crime organizado das Nações Unidas e também da Convenção de Budapeste, que, recentemente, terminou de negociar o seu segundo protocolo adicional, sobre intercâmbio de provas eletrônicas.

A capacitação seria um quinto ponto de importância a ser aqui ressaltado. Para os países em desenvolvimento trata-se de

tema essencial, pois há falta de conhecimento e de treinamento, de equipamentos. A convenção poderia constituir caminho pelo qual os países venham a obter esse tipo de treinamento.

Por último, mas não menos importante, encontra-se a proteção dos direitos humanos. Que os mecanismos criados pela Convenção respeitem os direitos humanos consagrados, e que a convenção estabeleça salvaguardas baseadas na defesa das liberdades fundamentais.

RISCOS E DESAFIOS DA NEGOCIAÇÃO DA CONVENÇÃO

Sobre os riscos e desafios da negociação, por um lado, nós queremos que o texto da Convenção seja adotado por consenso. Por outro lado, nós temos pouco tempo, nós temos só quatro sessões substantivas e uma sessão final. Então, chegar a um consenso é um desafio.

Temos a questão dos crimes cibernéticos próprios que já estão na Convenção de Budapeste e dos crimes impróprios, crimes cibernéticos impróprios. Do nosso ponto de vista, não seria ideal começar a discutir uma longa lista de crimes e tentar chegar a definições ou tipificações no âmbito da Convenção de crimes que já estão tipificados por cada país. Então, a possibilidade de usar os mecanismos da convenção para qualquer tipo de crime vai fazer com que a negociação seja mais fácil, que a convenção possa incluir quase só crimes cibernéticos próprios ou *cyber-dependent crimes* e um ou outro crimes impróprios ou *cyber-enabled crimes*, que os países tenham como consenso incluir. Por exemplo, fala-se muito sobre a exploração sexual de crianças pela internet.

Temos outro risco importante que é um desafio geopolítico: evitar que as negociações sejam contaminadas pela conjuntura internacional. Nas sessões até o momento isso tem sido possível, provavelmente pelo reconhecimento dos países de

que se trata de um tema técnico de combate ao crime e que a maior parte dos países, ou todos, querem que esses instrumentos sejam criados e possam ser usados.

RISCOS E DESAFIOS DA APLICAÇÃO DA CONVENÇÃO SOBRE CIBERCRIMES

Como último ponto, elenco aqui alguns riscos e desafios da aplicação da Convenção. Um deles tem a ver com a proteção dos direitos humanos: muitos têm levantado uma preocupação de que os mecanismos da convenção possam ser usados por países de forma contrária a direitos e garantias individuais. Trata-se de preocupação legítima, mas há que ter em mente que a convenção que estamos negociando trata de cooperação internacional, algo que, ao envolver ao menos duas jurisdições, deve estar duplamente sujeita às garantias estabelecidas domesticamente. O controle da legalidade acontece nos dois países, tanto sobre quem pede a informação quanto sobre quem vai mandar a informação. Então, é uma preocupação que se coloca, mas pensando no contexto da Convenção, é algo que pode ser controlado e pode ser superado.

Temos também a questão de novos direitos. Não digo o estabelecimento de novos direitos a serem aplicados na esfera cibernética, porque, no curto espaço de tempo, a Convenção não tem a condição de criar novos direitos. A convenção, no entanto, deve reconhecer e incluir salvaguardas a direitos. As principais salvaguardas, nós acreditamos, são o império da lei e o devido processo legal. Internamente, cada país é quem deve garantir o respeito a esses direitos, pois a convenção não tem a capacidade de instituir ou de aumentar, por ela mesma, o nível de respeito ao devido processo legal em um país.

Por último, obrigações para o setor privado. A convenção não deve estabelecer, do nosso ponto de vista, diretamente

obrigações para o setor privado, mas prescrever padrões mínimos a serem regulados por cada Estado.

Para terminar, eu quero parabenizar pelo lançamento do livro "O direito das investigações digitais no Brasil: fundamentos e marcos normativos". Espero ter condições de ter um exemplar também, que vai me ajudar bastante nos meus estudos e no pensamento sobre essa questão. Era isso que eu tinha por ora e estou à disposição para responder a eventuais indagações.

Muito obrigado.

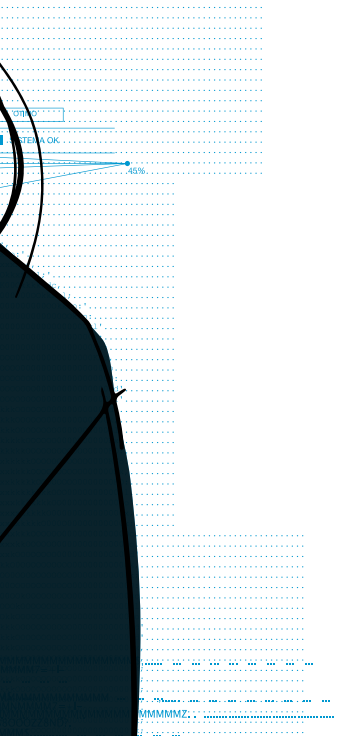
NOTAS

1. Este artigo foi adaptado a partir de uma palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022.

2. Tradução livre: *"5. Decide também que o Comitê Ad Hoc realizará a primeira, a terceira e a sexta sessões de negociação em Nova York e a segunda, a quarta e a quinta sessões em Viena, e será orientado pelas regras de procedimento da Assembleia Geral, enquanto todas as decisões do Comitê sobre questões substantivas sem aprovação por consenso serão tomadas por uma maioria de dois terços dos representantes presentes e votantes, antes do que o Presidente, mediante decisão da Mesa, informará ao Comitê que todos os esforços para chegar a um acordo por consenso foram esgotados;"*

04.

CONVENÇÕES DE CIBERCRIMES E PERSECUÇÃO PENAL INTERNACIONAL[1]



Veridiana Alimonti

Está em curso a elaboração e negociação, no âmbito de Comitê *Ad Hoc* das Nações Unidas, de uma Convenção Internacional Abrangente sobre o Combate ao Uso de Tecnologias da Informação e Comunicação para Fins Criminais. O processo foi iniciado ainda em 2017 com a apresentação, pela Rússia, de uma carta à Assembleia Geral da ONU, contendo a proposta de uma convenção sobre o combate a crimes cibernéticos.[2] Pouco mais de dois anos depois, ao final de 2019, a Assembleia Geral da ONU aprovou uma resolução patrocinada pela Rússia e outros países, como Camboja, Irã, Nicarágua e Síria, para o estabelecimento de uma convenção das Nações Unidas sobre crimes cibernéticos.[3]

Ela vem se somar à Convenção sobre o Cibercrime do Conselho da Europa, conhecida como Convenção de Budapeste, que foi aberta a assinaturas ainda em 2001. Apesar de membro do Conselho da Europa, a Rússia não é parte da Convenção de Budapeste. Por outro lado, mesmo Estados que não são membros do Conselho da Europa são signatários ou podem aderir à Convenção de Budapeste, desde que tenham participado de sua elaboração ou observem o procedimento previsto no artigo 37 da Convenção.[4] A Convenção de Budapeste foi o primeiro tratado internacional sobre crimes cometidos pela internet e outras redes de computador. Ela prevê normas de direito penal material e processual com o intuito de harmonizar a legislação criminal na matéria e reforçar a cooperação em investigações transfronteiriças.

Os debates e preocupações suscitados no bojo do processo em curso nas Nações Unidas por organizações da sociedade civil remontam a problemas identificados na redação ou aplicação de legislações de crimes cibernéticos em distintos países, muitas vezes influenciadas pela Convenção de Budapeste como principal marco internacional na matéria.[5]

Antes de explorarmos estas preocupações em mais detalhes, interessa delinear o que são crimes cibernéticos. O escopo de tal definição também é tema que envolve discordâncias e tensões.

O QUE SÃO CRIMES CIBERNÉTICOS?

Não existe um entendimento comum definitivo, em âmbito global, do que constitui a criminalidade cibernética. Uma primeira delimitação importante é a de que o simples fato de dispositivos tecnológicos serem utilizados na prática de um crime não deve converter este ato em um crime cibernético. Por exemplo, se um agente privado utiliza aplicativos de mensagens para oferecer vantagem indevida a funcionário público para determiná-lo a omitir ato de fiscalização que caberia à sua função, isso não qualifica o ilícito de corrupção ativa como um crime cibernético. Do mesmo modo, o mero uso de dispositivos tecnológicos na prática de um delito não deve ser tratado como fator que agrava a pena ou qualifica o crime, embora isso ocorra com alguma frequência em legislações penais.

Os principais crimes cibernéticos se referem àqueles que se dirigem intrinsecamente às tecnologias de informação e comunicação (TICs), e que dependem delas para a sua configuração (*cyber-dependent crimes*). São os tipos penais que se pode verificar nos artigos 2 a 6 da Convenção de Budapeste e que incluem, entre outros, o acesso ilegítimo a um sistema informático, a interceptação ilegítima de dados informáticos e a obstrução grave e ilegítima ao funcionamento de sistema informático. Nestes casos, as TICs são os objetos diretos e os instrumentos do crime, de forma que os crimes não poderiam existir sem tais tecnologias. Por exemplo, utilizar um *software* malicioso para apagar todos os dados de um grupo de pessoas

no sistema da Receita Federal ou utilizar um gerenciador de senhas para roubar a senha de outra pessoa e acessar suas contas de redes sociais e e-mail. Estes são os crimes cibernéticos puros ou essenciais, que deveriam ser o objeto primordial de regulações de cibercrimes de forma a evitar a criminalização vaga de condutas ou a duplicação do tratamento penal de condutas não intrinsecamente relacionadas à tecnologia.

Outra categoria que se vê com alguma frequência, também por influência da Convenção de Budapeste, são os crimes habilitados pela tecnologia (*cyber-enabled crimes*). Eles dizem respeito a crimes tradicionais cometidos por meio de tecnologias da informação e comunicação, como a fraude e a falsificação, cujo elemento tecnológico pode ocasionalmente cumprir papel relevante em termos de facilidade, velocidade, alcance ou escala da conduta criminosa. O *ransomware*[6] é um exemplo interessante que combina diferentes categorias. Ele inclui elementos de cibercriminalidade pura ou essencial, relativo ao apoderamento dos dispositivos das vítimas com *software* malicioso para danificar ou ocultar dados, elementos de criminalidade habilitada pela tecnologia, como a difusão do *software* malicioso em grande escala por meios como *spam*, e elementos da criminalidade tradicional, que é a prática de extorsão.

Por fim, legislações de crimes cibernéticos por vezes incluem, ainda, crimes relacionados ao conteúdo. É o que se vê na Convenção de Budapeste nos artigos 9 e 10, que tratam de abuso e exploração sexual infantil na internet ("pornografia infantil") e direitos autorais e conexos. Regulações de outros países vão além, podendo incluir blasfêmia religiosa, agitação antigovernamental, a difusão de informações falsas, incitação ao ódio, entre outros. Novamente se referem a condutas que estão fora do escopo central da cibercriminalidade, não representando ataques a dispositivos tecnológicos, sistemas

informáticos ou bancos de dados por meio de instrumentos também tecnológicos.

A previsão de infrações penais relacionadas a conteúdo em legislações de crimes cibernéticos levou, com frequência, à restrição de expressões legítimas e mesmo à proibição de discursos considerados protegidos conforme padrões internacionais de liberdade de expressão. Por exemplo, a jornalista filipina mundialmente conhecida, Maria Ressa, foi condenada por "difamação cibernética" em 2020, sujeita a uma pena de até sete anos de prisão.[7] No âmbito das discussões da Convenção sobre crimes cibernéticos da ONU, a Rússia propôs, juntamente com Belarus, Burundi, China, Nicarágua e Tajiquistão, a criminalização de uma ampla gama de discursos a partir de termos vagamente definidos, incluindo "a distribuição de materiais que incitem a atos ilegais motivados por ódio ou inimizade política, ideológica, social, racial, étnica ou religiosa, ou o fornecimento de acesso a tais materiais por meio de tecnologias da informação e comunicação".[8]

Como vem afirmando a Electronic Frontier Foundation (EFF) e outras organizações da sociedade civil em seu trabalho nesta temática, qualquer legislação sobre crimes cibernéticos deveria evitar a inclusão de infrações baseadas no conteúdo da expressão *online*, pela maneira como tais previsões foram e são utilizadas de forma abusiva em diferentes contextos para silenciar expressões legítimas e perseguir críticos. É preciso garantir que disposições sobre crimes cibernéticos não se apliquem ou sejam interpretadas de modo a restringir indevidamente condutas protegidas por normas de direitos humanos.

Esta preocupação se insere em consideração mais ampla sobre a necessidade de que instrumentos normativos sobre crimes cibernéticos adotem enfoque centrado em direitos humanos. Isso significa prever garantias e procedimentos para assegurar que suas regras não sirvam como ferramentas para

reprimir a liberdade de expressão, violar os direitos à privacidade e à proteção de dados pessoais, ou colocar em risco a integridade física de pessoas e grupos.

PREOCUPAÇÕES DE DIREITOS HUMANOS NA REGULAÇÃO E COMBATE A CRIMES CIBERNÉTICOS

Instituições de direitos humanos se manifestaram sobre a previsão ou aplicação arbitrária de legislações de crimes cibernéticos. O Relator Especial da ONU sobre os direitos à liberdade de reunião pacífica e de associação, Clément Nyaletsossi Voule, afirmou que "a onda de leis e políticas destinadas a combater a cibercriminalidade também levou à punição e à vigilância de ativistas e manifestantes em muitos países do mundo". O relator complementa que leis que criminalizam o acesso e uso de ferramentas digitais, entre elas leis de crimes cibernéticos, estão sendo aprovadas cada vez mais em diversos países – "Nessas leis, a responsabilidade penal é frequentemente enunciada em termos vagos e mal definidos, que permitem a sua aplicação de maneira arbitrária ou discricionária e dão origem à incerteza jurídica. Como resultado, elas descumprem as disposições legais relativas às restrições permitidas de acordo com os artigos 21 e 22 do Pacto [Internacional de Direitos Civis e Políticos]".[9]

Por sua vez, o Alto Comissariado das Nações Unidas para os Direitos Humanos ressaltou ser inegável que crimes cibernéticos colocam em perigo os direitos das pessoas ao redor do mundo. Porém, destacou que, "[a]o mesmo tempo, disposições regulando a cibercriminalidade e sua aplicação podem implicar importantes riscos para os direitos humanos, como evidenciado pelo uso habitual a nível nacional das leis e políticas de crimes cibernéticos para restringir a liberdade

de expressão, atacar vozes dissidentes, justificar apagões na internet, ingerir na privacidade e no anonimato das comunicações e limitar os direitos à liberdade de associação e à reunião pacífica".[10]

Assim, ao mesmo tempo em que regulações sobre crimes cibernéticos servem à proteção de direitos humanos, sua formulação e disposições devem estar de acordo com normas e padrões internacionais de direitos humanos quanto à restrição ou ingerência a liberdades fundamentais. Devem, portanto, cumprir com o princípio da legalidade, sendo aprovadas a partir de lei formal, com regras públicas, claras e precisas em seu alcance. Enquanto regulação de direito penal, devem focar nas condutas mais danosas, no sentido de a resposta penal ser a *ultima ratio* adotada pelo Estado na regulação de comportamentos. Neste sentido, devem ainda ser necessárias e proporcionais em uma sociedade democrática para se atingir o objetivo legítimo de proteger a população contra a criminalidade cibernética.

De forma geral, podemos articular as preocupações de direitos humanos trazidas por regulações ou interpretações arbitrárias de normas voltadas ao combate de crimes cibernéticos em três temas principais: (i) criminalização da expressão; (ii) restrições ao jornalismo investigativo, pesquisa de segurança e denunciantes (*whistleblowers*); e (iii) ingerência indevida ao direito à privacidade e à proteção de dados pessoais.[11]

O primeiro ponto já foi discutido no item anterior. Em relação ao segundo ponto, cumpre destacar que leis de crimes cibernéticos normalmente envolvem a criminalização de acesso não autorizado ou ilegal a sistemas informáticos e dados, assim como a interferência a estes sistemas. Tais regras são importantes para a garantia de direitos. Porém, dependendo de sua formulação, podem levar à criminalização de atividades legítimas e fundamentais, especialmente no caso de previsões

amplas que penalizam o acesso ou interferência a sistemas e dados independentemente de intenção maliciosa ou sem conter exceções a objetivos de interesse público. Muitas vezes a atuação de jornalistas investigativos e denunciantes envolvem o acesso a sistemas e dados de forma a expor violações de direitos por governos e grandes empresas. Nestes casos, a criminalização de tal acesso sem autorização compromete a publicação de informações vitais ao interesse público.

Da mesma forma, a pesquisa de vulnerabilidades de segurança em sistemas e dispositivos informáticos muitas vezes implica a intrusão sem autorização – não com fins maliciosos de comprometer dados ou interferir em sistemas para causar danos ou obter vantagens ilícitas, mas para identificar vulnerabilidades e apontá-las aos responsáveis para que possam ser corrigidas. Desse trabalho depende cada vez mais a nossa segurança digital. Por vezes, pesquisadores de segurança são consultores ou trabalham para empresas e instituições públicas de forma a identificar vulnerabilidades em seus sistemas e dispositivos, contando com as devidas autorizações para esta atividade. Porém, há distintos casos em que especialistas em segurança cibernética fazem isso de maneira independente e se veem ameaçados por possíveis persecuções penais que falham em considerar a inexistência de intenção maliciosa e o aspecto benéfico de tal atividade.

Disposições voltadas ao combate a crimes cibernéticos na América Latina trazem demonstrações deste problema. Previsões no Código Penal do Equador e da Costa Rica, por exemplo, penalizam quem simplesmente acessa um sistema sem autorização ou ultrapassando barreiras de segurança.[12] No caso brasileiro, o crime de "invasão de dispositivo informático" previsto no artigo 154-A do Código Penal busca agregar uma finalidade ilícita como elemento do tipo, embora a criminalização da mera obtenção de dados sem autorização, sem uma

exceção de interesse público, possa dar margem à perseguição de jornalistas investigativos e denunciantes comentada acima.

Quanto a pesquisadores de segurança e especialistas em segurança cibernética, há distintos casos documentados na região de utilização arbitrária de normas de crimes cibernéticos para dissuadir a sua atuação ou a revelação de vulnerabilidades encontradas.[13] Um caso paradigmático, em que sequer se demonstra efetivamente a ocorrência de acesso não autorizado a sistema informático, é a persecução penal em curso no Equador contra o desenvolvedor de *software* livre e ativista em segurança digital sueco, Ola Bini. Embora declarado inocente por decisão unânime de tribunal equatoriano no início de 2023,[14] a Procuradoria Geral do Estado apelou da decisão levando à manutenção das cautelares que restringem os direitos de Ola Bini e prolongando ainda mais a sua persecução penal arbitrária.

Parte destes problemas encontra raízes na própria Convenção de Budapeste, como norma internacional influente no combate a crimes cibernéticos. Suas disposições de direito penal material, que devem ser incorporadas no ordenamento jurídico doméstico dos Estados que aderem à Convenção, também falham em explicitar exceções de interesse público na criminalização de condutas e, algumas delas, em estabelecer a necessidade de intenção maliciosa como elemento do tipo.

Por fim, o terceiro ponto, relacionado a ingerências abusivas ao direito à privacidade, diz respeito a normas de direito processual voltadas à guarda e ao acesso a dados de comunicações e provas digitais em investigações criminais. Essa combinação de direito material e processual se verifica em legislações de combate à criminalidade cibernética e também tem inspiração na Convenção de Budapeste. A preocupação aqui se coloca em relação à previsão de poderes de investigação sem salvaguardas suficientes de direitos humanos e mecanismos de controle, como

necessidade de ordem judicial, garantias de devido processo e de remédio efetivo em caso de violações. Por exemplo, a Lei de Prevenção a Crimes Cibernéticos das Filipinas autoriza a polícia a obter dados informáticos em tempo real sem ordem judicial.[15] Outras legislações, como a de crimes relacionados a computadores na Tailândia, estabelecem amplas obrigações de retenção massiva de dados de comunicação, entre outros problemas.

A necessidade de aplicação de normas e padrões internacionais de direitos humanos no acesso a dados de comunicações e provenientes de sistemas digitais por autoridades de investigação vem se afirmando há pelo menos uma década.[16] No entanto, assegurar que a intensificação do uso e das capacidades de coleta e processamento da informação por tecnologias digitais seja acompanhada de salvaguardas robustas de direitos humanos, em especial de privacidade e proteção de dados, é um desafio constante que se apresenta de maneira mais ou menos problemática a depender de cada marco legal e institucional.

Neste ponto, interessa trazer algumas considerações mais específicas sobre a Convenção de Budapeste e seu Segundo Protocolo Adicional, relativo ao acesso transfronteiriço a dados em investigações criminais.

A CONVENÇÃO DE BUDAPESTE SOBRE O CRIME CIBERNÉTICO E SEU SEGUNDO PROTOCOLO ADICIONAL

Como notado acima, a Convenção de Budapeste foi o primeiro tratado internacional a abordar a tipificação de crimes cibernéticos e a previsão de regras de processo penal e cooperação internacional na matéria. Foi negociada no âmbito do Conselho da Europa, que é a instituição de direitos humanos da Europa, não se confundindo com instâncias da União Europeia.

/ QUALQUER LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS DEVERIA EVITAR A INCLUSÃO DE INFRAÇÕES BASEADAS NO CONTEÚDO DA EXPRESSÃO ONLINE /

Outros Estados que não são membros do Conselho da Europa fizeram parte das negociações e da elaboração da Convenção, como os Estados Unidos, Japão e Canadá. O artigo 37 da Convenção estabelece o procedimento para que outros Estados, que não sejam membros do Conselho da Europa ou envolvidos na formulação de seu texto, possam aderir e se tornar parte do instrumento. Atualmente, a Convenção de Budapeste conta com 68 adesões ou ratificações.[17] Na América Latina, ela foi ratificada pela Argentina, Brasil, Chile, Colômbia, Costa Rica, República Dominicana, Panamá, Paraguai e Peru.

A Convenção de Budapeste é um instrumento bastante influente no desenvolvimento de normas destinadas ao combate ao crime cibernético, mesmo em países que não aderiram formalmente ao seu texto. O Brasil é um exemplo. A formalização da ratificação do Brasil ocorreu muito recentemente, em 2023, com aprovação congressual e assinatura em 2022. Ainda assim, disposições da Convenção influenciaram o texto inicial da "Lei Azeredo" (Lei n. 12.735/2012), a elaboração da "Lei Carolina Dieckmann" (Lei n. 12.737/2012) e do próprio Marco Civil da Internet (Lei 12.965/2014), que surgiu como reação a iniciativas legais focadas na criminalização de condutas na internet. Discussões em torno da reforma do código de processo penal brasileiro (PL n. 8045/2010) também têm em vista questões de acesso a dados de comunicação e prova digital em investigações criminais que se associam a temas presentes na Convenção.

Preocupações descritas acima foram apresentadas por organizações da sociedade civil, inclusive a EFF, no contexto mais recente da adesão do Brasil à Convenção de Budapeste. Em especial, o fato de que a adesão ocorreu sem considerar que havia mais tempo para a discussão e dispensando a oportunidade única de realizar importantes reservas e declarações ao texto.[18] Relatório da organização Derechos Digitales traz um

panorama sobre a adesão e a implementação da Convenção de Budapeste em países da América Latina, atentando também a algumas das questões levantadas acima.[19]

Ao tornar-se parte na Convenção de Budapeste, além das normas de cooperação internacional, o Estado se obriga a adotar disposições em seu direito interno para criminalizar as condutas previstas nos dispositivos de direito material da Convenção, assim como a estabelecer os poderes e medidas de investigação previstos em suas regras de direito processual. Tais medidas incluem, entre outras, a obtenção de dados de computador em tempo real e a preservação expedita de dados armazenados em computador. Quanto à criminalização de condutas, o artigo 13 estipula que cada Parte assegurará que tais condutas sejam punidas por meio de sanções criminais eficazes, proporcionais e dissuasivas.

A expressão "proporcionais" se refere ao princípio da proporcionalidade, que implica um balanço entre a punição e a conduta, considerando o objetivo legítimo que se visa proteger e os direitos da pessoa punida. É um princípio central no âmbito da proteção de direitos humanos e fundamentais. É interessante notar, no entanto, que a tradução do tratado que consta da Mensagem Presidencial enviada ao Congresso para aprovação da Convenção de Budapeste (Mensagem n. 412/2020) e o Decreto Presidencial que a promulga na ordem interna (Decreto n. 11.491/2023) apresentam, no artigo 13, parágrafo 1, a expressão "adequadas" em vez de "proporcionais". Ainda que seja pertinente questionar a razão de tal alteração no texto traduzido, sua aplicação deverá observar o princípio da proporcionalidade, seja por força do texto original da Convenção de Budapeste, seja por garantias do próprio ordenamento jurídico brasileiro.

A referência mais direta à garantia de direitos humanos na implementação do tratado se encontra no artigo 15. Ele

estabelece que a aplicação dos poderes e procedimentos previstos na seção de direito processual da Convenção se sujeita às condições e garantias instituídas na legislação interna do Estado Parte, que deverá prever proteção adequada aos direitos humanos e às liberdades públicas, incluindo os direitos originados em conformidade com as obrigações que o Estado tenha assumido em instrumentos internacionais de direitos humanos, bem como que tais poderes e procedimentos incorporarão o princípio da proporcionalidade.

Embora tal previsão seja importante, o tratamento conferido à garantia de direitos humanos na Convenção de Budapeste, consubstanciado nesta disposição, é insuficiente em ao menos dois aspectos. Primeiro, diz respeito apenas à seção de direito processual da Convenção, em vez de de se referir a todo o seu texto, incluindo as previsões de direito material. Segundo, é genérica e pouco especificada quanto às garantias que busca estabelecer. O dispositivo faz referência a outros tratados internacionais, porém suas garantias podem ser interpretadas e aplicadas em cada jurisdição nacional de forma diferente. Além disso, alguns Estados que integram a Convenção podem não ter ratificado parte desses tratados e não estar sujeito aos seus compromissos. O art. 15 chega a mencionar que tais condições e garantias incluirão controle judicial ou supervisão independente, fundamentação da aplicação e limitação no âmbito de sua aplicação e duração. Porém, deverão fazê-lo "quando apropriado", sem qualquer detalhamento adicional ou critério a ser considerado.

Na prática, enquanto a Convenção estabelece obrigações detalhadas de criminalização de condutas e poderes de investigação, ela não vincula os Estados Parte a correspondentes garantias de direitos humanos. Se as primeiras impactarão o ordenamento interno destes Estados, que deverão incorpo-

rá-las e assegurá-las, as segundas tenderão a ser aplicadas conforme cada Estado já as estabelece e interpreta.

Em 2003, foi aberto à assinatura o Primeiro Protocolo Adicional à Convenção de Budapeste, voltado à criminalização de atos de natureza racista ou xenofóbica cometidos através de sistemas informáticos, que entrou em vigor em 2006 após 5 ratificações.[20] Mais recentemente, em novembro de 2022, foi adotado o seu Segundo Protocolo Adicional, aberto a assinaturas em maio de 2022, que entrará em vigor após 5 ratificações.[21]

SEGUNDO PROTOCOLO ADICIONAL À CONVENÇÃO DE BUDAPESTE

Os Estados que são parte da Convenção de Budapeste podem aderir ao seu Segundo Protocolo Adicional. Na América Latina, até o momento, Argentina, Chile, Colômbia, Costa Rica e República Dominicana assinaram o Segundo Protocolo, estando ainda pendente a ratificação. Seu foco é estabelecer regras de cooperação para o acesso transfronteiriço a dados em investigações criminais. O fato de que os Estados Unidos é Estado Parte da Convenção de Budapeste e pode vir a ratificar o Segundo Protocolo pode ser um incentivo a que diferentes países, incluindo os latino-americanos, adiram ao Segundo Protocolo, de forma a facilitar o acesso a dados sob o controle de plataformas digitais situadas em território estadunidense.

Entre as medidas de cooperação se encontram: assistência mútua em situações de emergência, revelação rápida de dados informáticos armazenados em caso de emergência, cooperação entre autoridades para a revelação de dados informáticos armazenados e procedimentos de cooperação direta com os provedores de serviços no território de outro Estado Parte.

O principal marco para a cooperação entre Estados em investigações criminais através de fronteiras tem sido tradicionalmente fornecido por Tratados de Assistência Jurídica Mútua (MLATs). MLATs são tipicamente acordos bilaterais, negociados entre dois Estados e incorporando salvaguardas jurídicas relevantes de seus ordenamentos. Muitos Estados argumentam que o processo de cooperação via MLATs é lento, atrasando ou mesmo comprometendo investigações criminais. As medidas mais invasivas do Segundo Protocolo buscam responder a esses argumentos com a criação de novos mecanismos que permitirão às autoridades competentes acessar dados em outros Estados de maneira mais fácil e rápida.

No entanto, esforços para obter maior eficiência no acesso a dados pessoais em investigações criminais transfronteiriças devem estar sempre fundamentados em sólidas garantias de direitos humanos. A legalidade e legitimidade das investigações dependem do respeito a garantias de processo penal, legislações de proteção de dados e ao Direito Internacional dos Direitos Humanos. Se investigações criminais através de fronteiras são desafiadoras para o acesso a dados e à produção de provas, assegurar a proteção a garantias de direitos humanos em tais investigações é igualmente ou ainda mais difícil.

Como garantir que qualquer ingerência ao direito à privacidade se baseie em uma legislação acessível ao público, precisa e não discriminatória, e que tal ingerência seja legítima, necessária e proporcional? Como assegurar que o acesso a dados e seu compartilhamento estejam autorizados por uma autoridade judicial competente, imparcial e independente? Como assegurar que prevalecem o devido processo, aplicam-se mecanismos de supervisão, assim como sigilos e imunidades são respeitados?

Diante destes desafios, o texto do Segundo Protocolo gera algumas preocupações articuladas em mais detalhes na publi-

cação *Assessing New Protocol to the Cybercrime Convention in Latin America*.[22] Estas preocupações se colocam principalmente em relação: (i) aos mecanismos de cooperação direta entre autoridades de um Estado Parte e prestadores de serviço localizados no território de outro Estado Parte; (ii) à compreensão problemática de informação cadastral (*subscriber information*) como inerentemente pouco sensível; (iii) aos possíveis efeitos de ambos elementos em marcos legais de privacidade na América Latina; e (iv) a um desequilíbrio entre poderes obrigatórios às autoridades de investigação e garantias de direitos humanos tratadas como opcionais ou dispensáveis.

O primeiro ponto diz respeito ao artigo 7º do Segundo Protocolo. Este dispositivo autoriza que um Estado Parte solicite informações cadastrais de usuários diretamente a provedores de serviços situados em outro Estado Parte. Se o provedor de serviço se negar a entregar a informação, aí sim o mecanismo jurídico de efetivação da solicitação envolve, por padrão, a intermediação de uma autoridade do Estado requerido.

Informações cadastrais são aquelas que permitem a identificação de um usuário ou usuária de determinado serviço (ex.: o nome e endereço). A definição do que engloba este tipo de informação está prevista no artigo 18 da Convenção de Budapeste. Ela se estende a informações que vão além da definição de dados cadastrais presente no Decreto n. 8.771/2016, que regulamenta o Marco Civil da Internet (Lei n. 12.965/2014). O artigo 18 da Convenção inclui, por exemplo, informações sobre pagamento e cobrança. Um ponto controverso, que abordaremos mais adiante, é a intenção de interpretar a definição de informação cadastral na Convenção de forma a incluir também endereços IP.

Assim, com base no artigo 7º do Segundo Protocolo, a autoridade competente de um Estado Parte pode solicitar informações cadastrais diretamente a um provedor de serviço situado em outro Estado Parte, seguindo as garantias proces-

suais e de direitos fundamentais aplicáveis de acordo com o marco legal do Estado Parte solicitante (e não do Estado Parte em que está situado o provedor de serviço). A depender das diferenças no marco legal de cada Estado Parte, isso pode significar que autoridades estrangeiras consigam ter acesso a informações cadastrais, no território do Estado requerido, seguindo garantias legais menos robustas do que àquelas aplicáveis às autoridades deste próprio Estado.

Por exemplo, se a legislação no Estado requerido, onde está localizado o provedor de serviço, determina a necessidade de uma ordem judicial para revelar dados cadastrais e o marco jurídico do Estado solicitante estabelece que um pedido direto da polícia é suficiente para este acesso, a autoridade estrangeira poderá obter dados que identificam um usuário investigado sem uma ordem judicial prévia, enquanto isso é exigido das autoridades de investigação locais.

Estados Parte podem fazer uma declaração para que tais pedidos diretos sejam emitidos por uma autoridade independente do Estado solicitante, mas não é possível especificar que tal autoridade seja judicial. Importa notar que no Brasil, por força do art. 10 do Marco Civil da Internet, a regra geral é a necessidade de prévia autorização judicial para a revelação de dados cadastrais de usuários de serviços de conexão ou de aplicações de internet, a não ser que legislação específica determine o contrário.

Além disso, o procedimento padrão do artigo 7º não assegura que uma autoridade no Estado Parte onde está situado o provedor acompanhe a solicitação por ele recebida e verifique se o pedido foi realizado de forma adequada ou se implica uma ingerência indevida a direitos humanos. Como regra geral, caberá ao provedor de serviço avaliar se a autoridade estrangeira solicitante é de fato competente, se ela é realmente a autoridade que diz ser, se o que ela pede está de acordo com o marco jurídico do Estado Parte solicitante, assim como outras

implicações a direitos humanos relativas ao pedido. A questão da autenticidade do pedido é importante aqui, ou seja, verificar se o contato vem de emissor autêntico. Se isso é mais fácil de verificar por meio de canais oficiais entre autoridades estatais, pode ser bastante desafiador para prestadores privados.

Esta questão não está devidamente detalhada no Segundo Protocolo. De acordo com o seu Relatório Explicativo, a solicitação vir de um e-mail institucional da autoridade competente seria suficiente para demonstrar a autenticidade do pedido. Uma solução mais adequada, também citada no Relatório Explicativo, seria obter a confirmação de autenticidade por meio de uma autoridade conhecida no Estado solicitante. Porém, um caminho que é mais facilitado para Estados do que para agentes privados. Mesmo grandes agentes privados podem ser levados ao engano. Por exemplo, reportagens da imprensa revelaram que Apple e Meta disponibilizaram dados de usuários, como seus endereços, número de telefone e endereços IP, em resposta a pedidos de emergência forjados por criminosos cibernéticos, passando-se por autoridades de investigação.[23]

É possível estabelecer um dever de notificação simultânea ao Estado Parte onde está localizado o provedor de serviço, mas isso depende de declaração do Estado Parte interessado ao Secretário Geral do Conselho da Europa. É possível, ainda, afastar o mecanismo de solicitação direta, para que as solicitações de autoridades estrangeiras sigam procedimento que envolva uma autoridade responsável no Estado requerido. Contudo, é necessário fazer uma reserva neste sentido no momento da assinatura ou ratificação do Segundo Protocolo. Caso o Estado o faça, não poderá se valer do artigo 7º para solicitar dados diretamente de provedores de serviços em outro Estado Parte.

O Segundo Protocolo permite que autoridades estrangeiras solicitem informações cadastrais diretamente a provedores de serviço situados em outro território por uma compreensão

equivocada de que tais informações são inerentemente pouco sensíveis. Esta é a preocupação apresentada no segundo ponto acima. O Relatório Explicativo do Segundo Protocolo (parágrafo 92) afirma que "informação cadastral [...] não permite conclusões precisas relacionadas à vida privada e hábitos diários dos indivíduos em questão". No entanto, as informações cadastrais são justamente aquelas que servem à conexão de nossos rastros digitais à nossa identidade. Podem ser a ponta do *iceberg* revelando um perfil detalhado sobre alguém, a partir de suas atividades, expressões, relações e movimentos. Além disso, há uma série de aplicativos relacionados a comunidades específicas, cuja mera informação de que determinada pessoa está entre os usuários nele cadastrados pode revelar sua orientação sexual ou religião, por exemplo. Ambos se referem a dados pessoais considerados sensíveis em diferentes leis de proteção de dados, incluindo a brasileira. Dependendo do provedor de serviço, a impressão digital ou mesmo a biometria facial podem fazer parte dos dados pessoais fornecidos a título de cadastro e, a depender da interpretação, consideradas informação cadastral.

Por fim, há a discussão quanto à abrangência da definição de informação cadastral prevista no art. 18 da Convenção de Budapeste. Ao longo do tempo, o Comitê de Crimes Cibernéticos do Conselho da Europa (T-CY), que tem a atribuição de interpretar a Convenção de Budapeste, vem emitindo diretrizes que estabelecem um entendimento amplo da definição do artigo 18 para considerar o endereço IP como informação cadastral. Na legislação brasileira, o endereço IP faz parte dos registros de conexão e dos registros de acesso a aplicações, definidos pelo artigo 5º do Marco Civil da Internet. Em ambos os casos, o acesso depende de ordem judicial, garantia que não necessariamente valeria diante de solicitação de autoridade estrangeira a provedor de serviço situado no Brasil, conforme

explicado acima. Novamente, caso o Estado Parte não queira que o mecanismo de solicitação direta inclua o acesso a endereços IP, deverá fazer uma reserva específica no momento de sua adesão ao Segundo Protocolo. É importante ressaltar que o mecanismo de solicitação direta do art. 7º pode se aplicar mesmo quando a autoridade estrangeira está buscando dados de pessoas que estão localizadas ou vivem no Estado requerido.

A compreensão de que informações cadastrais são inerentemente pouco sensíveis e a dispensa de autorização judicial para o seu acesso por autoridades de investigação se alinha aos padrões de privacidade mais fracos entre os países da América Latina. Deriva daí a terceira preocupação principal apresentada acima – a possível influência negativa do Segundo Protocolo em marcos legais da região, no sentido de estabelecer garantias legais reduzidas no acesso de autoridades a informações cadastrais de usuários e usuárias e fomentar uma definição ampliada de informações cadastrais, sujeitas a este menor grau de proteção. Em marcos legais que permitem interpretação mais garantista, organizações da sociedade civil vêm pressionando prestadores de serviço a demandarem ordem judicial antes de entregarem dados de usuários a autoridades de investigação,[24] o que poderia ser comprometido com a cristalização de regras legais mais permissivas nos ordenamentos de países da região.

Quanto ao último ponto de preocupação, a análise do art. 7º já permite identificar que muitas salvaguardas importantes são deixadas à discricionariedade dos Estados, para que as estabeleçam por meio de reservas ou declarações ao texto do Segundo Protocolo. É preciso reconhecer que o Segundo Protocolo conta com um artigo mais detalhado com garantias de proteção de dados (artigo 14). Porém, a aplicação das salvaguardas do artigo 14 podem ser substituídas por outros acordos *ad hoc* entre os Estados Parte, sem exigência de que

tais acordos sejam transparentes ou tenham o mesmo nível de proteção do artigo 14. Ainda, algumas garantias deste dispositivo deixam a desejar em relação a outros padrões internacionais de proteção de dados, em especial a Convenção 108 e sua versão modernizada (Convenção 108 +), sobre a proteção das pessoas relativamente ao tratamento de dados pessoais, também do Conselho da Europa.

O guia *Assessing New Protocol to the Cybercrime Convention in Latin America* detalha todos esses pontos e oferece recomendações a Estados que estejam discutindo a adesão ou não ao Segundo Protocolo, incluindo formas de mitigar seus problemas caso decidam ratificá-lo. É fundamental que tal decisão se dê a partir de debate qualificado, transparente e participativo, em que os diferentes impactos a direitos humanos e fundamentais sejam devidamente considerados.

CONSIDERAÇÕES FINAIS

Se a proteção efetiva a direitos humanos envolve o combate à criminalidade cibernética e mecanismos de cooperação jurídica internacional que viabilizem o acesso a dados em outras jurisdições e investigações através de fronteiras, é preciso que tais disciplinas estejam, elas próprias, centradas e assentadas em direitos humanos. Para tanto, a definição de crimes cibernéticos deve ser clara e precisa, privilegiar os crimes cibernéticos essenciais, afastar a criminalização de conteúdo e proteger a atividade benéfica de pesquisadores de segurança, jornalistas investigativos e denunciantes.

Os poderes e medidas de investigação estabelecidos em leis de crimes cibernéticos e instrumentos que embasam o acesso transfronteiriço a dados devem se estruturar a partir de padrões internacionais de garantia da privacidade e da proteção de dados pessoais. Incluem-se aí salvaguardas, como autorização

judicial, sólida base probatória, mecanismos de transparência de solicitações por autoridades de investigação dentro e através das fronteiras, assim como supervisão do exercício de tais poderes de investigação por uma autoridade independente. É preciso haver paridade entre salvaguardas e poderes de vigilância e investigação, inclusive e principalmente na sua natureza vinculante aos Estados Parte de um tratado. Ainda que se deva aprimorar os mecanismos de cooperação internacional para torná-los mais efetivos, as solicitações de assistência jurídica mútua devem estar sujeitas à aprovação das autoridades competentes de ambos os Estados. Por certo, os Estados mantêm sua responsabilidade de avaliar a adequação das solicitações de autoridades estrangeiras a garantias legais e de direitos humanos.

A mensagem-chave emitida pelo Alto Comissariado das Nações Unidas para os Direitos Humanos,[25] no contexto da elaboração de uma nova convenção internacional sobre crimes cibernéticos, ainda no início de 2022, articula tais preocupações e apresenta recomendações fundamentais a qualquer iniciativa neste campo que busque efetivamente combater e investigar crimes, dentro e através das fronteiras, tendo como princípio e finalidade a garantia de direitos humanos e de liberdades fundamentais.

NOTAS

1. O conteúdo deste artigo elabora sobre trabalho realizado com Katitza Rodriguez, em atividades na Electronic Frontier Foundation (EFF) sobre temas de crimes cibernéticos e direitos humanos.

2. A carta pode ser acessada em https://encurtador.com.br/cEIJQ.

3. Para uma linha do tempo acerca do processo de elaboração e negociação da convenção da ONU, ver GULLO, Karen; RODRIGUEZ, Katitza. **UN Cybercrime Draft Treaty Timeline**. Electronic Frontier Foundation. 7 de abril de 2023. Disponível em: https://encurtador.com.br/FP059.

4. Ver o texto da Convenção de Budapeste em https://shre.ink/letq.

5. Neste sentido, ver HUMAN RIGHTS WATCH, **Abuse of Cybercrime Measures Taints UN Talks.** Include Nongovernmental Organizations in Treaty Negotiations. 5 de maio de 2021. Disponível em: https://shre.ink/letl.

6. *Ransomware* é um tipo de software malicioso que sequestra dados da vítima e os criptografa, cobrando um resgate (*ransom*) para reestabelecer o acesso a estes arquivos.

7. Ver HUMAN RIGHTS WATCH. **Philippines: Rappler Verdict a Blow to Media Freedom**. Manila Court Convicts Duterte Critic Maria Ressa for Libel. 15 de junho de 2020. Disponível em https://shre.ink/le2S.

8. BAGHDASARYAN, Meri; RODRIGUEZ, Katitza; GULLO, Karen; GREENE, David. **Speech-Related Offenses Should be Excluded from the Proposed UN Cybercrime Treaty**. Electronic Frontier Foundation. 6 de junho de 2022. Disponível em: https://shre.ink/lekJ.

9. Nações Unidas. Assembleia Geral. **Relatório do Relator Especial sobre os direitos à liberdade de reunião pacífica e de associação**, Clément Nyaletsossi Voule. A/HRC/41/41. 17 de maio de 2019. Parágrafos 3 e 32. Disponível em: https://shre.ink/lekF.

10. Nações Unidas. Alto Comissariado para os Direitos Humanos. **OHCHR key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes**. 17 de Janeiro de 2022. Disponível em: https://shre.ink/lekh.

11. Esta categorização tem em conta artigo da Human Rights Watch citado na nota 6 *supra*, que contém exemplos de normas problemáticas de combate a crimes cibernéticos afetando cada uma das três categorias.

12. Ver RODRIGUEZ, Katitza; UGARTE, Ramiro; OPSAHL, Kurt; CARDOZO, Nate; WILLIAMS, Jamie; ISRAEL, Tamir. **Protecting Security Researchers' Rights in the Americas**. Electronic Frontier Foundation. 16 de Outubro de 2018. Disponível em: https://shre.ink/leka. Este relatório analisa distintas legislações de combate a crimes cibernéticos nas Américas e apresenta recomendações a partir de garantias de direitos humanos do sistema interamericano aplicáveis ao trabalho de pesquisadores de segurança.

13. Ver ACCESS NOW. **La persecución de la comunidad de la seguridad informática en América Latina**. Agosto de 2021. Disponível em: https://shre.ink/lekI.

14. ALIMONTI, Veridiana. **The Aftermath of Ola Bini's Unanimous Acquittal by Ecuadorian Court**. Electronic Frontier Foundation. 15 de março de 2023. Disponível em: https://shre.ink/leGU.

15. Ver HUMAN RIGHTS WATCH. **Philippines: New 'Cybercrime' Law Will Harm Free Speech**. Supreme Court to Rule on Act That Worsens Criminal Defamation. 28 de setembro de 2012. Disponível em: https://shre.ink/leGE.

16. Neste sentido, ver os Princípios Internacionais para Aplicação de Direitos Humanos à Vigilância nas Comunicações em https://shre.ink/leGK. Na mesma plataforma é possível encontrar relatórios por países, considerando diferentes países da América Latina.

17. Ver a relação completa em https://shre.ink/leGM.

18. Ver, neste sentido, Carta aos Membros do Senado Federal sobre a Convenção de Budapeste (https://shre.ink/leGd) e Sugestões de Emendas ao PDL 255/2021 (https://shre.ink/leSj)

19. SANTOS, Bruna Martins dos. **Convenção de Budapeste sobre o Cibercrime na América Latina**. Uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México. Maio de 2022. Disponível em: https://shre.ink/leSj.

20. Mais informações sobre o Primeiro Protocolo disponíveis em https://shre.ink/leSS.

21. Segundo Protocolo Adicional à Convenção sobre o Crime Cibernético sobre a cooperação reforçada e revelação de prova digital. Informações disponíveis em https://shre.ink/leSb.

22. ALIMONTI, Veridiana. **Assessing New Protocol to the Cybercrime Convention in Latin America**. Concerns, Human Rights Considerations, and Mitigation Strategies. Electronic Frontier Foundation and Al Sur. Maio de 2022. Disponível em: https://shre.ink/leSB. Nessa página também é possível acessar a tradução do guia para o espanhol.Ver também ISRAEL, Tamir; RODRIGUEZ, Katitza. **On New Cross-Border Cybercrime Policing Protocol, a Call for Caution**. Just Security. 13 de maio de 2022. Disponível em: https://shre.ink/leXN.

23. Ver em Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests. **Bloomberg**. 30 de março de 2022. Disponível em: https://shre.ink/leXL

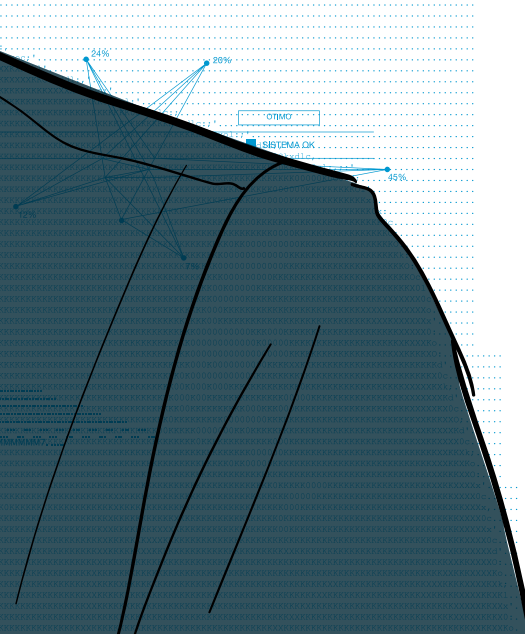
24. Ver, por exemplo, o trabalho realizado no âmbito dos relatórios do projeto *Quién Defiende tus Datos*, coordenado pela EFF em parceria com diferentes organizações da América Latina. Disponível em: https://shre.ink/leXr.

25. Ver nota 11 *supra*

05.

O DIREITO À INTIMIDADE NA ERA DIGITA

Maurício Zanoide



Boa noite a todas e a todos.

Eu queria, antes de tudo, agradecer o convite que foi feito a mim pelo InternetLab, de modo que possa tratar de um assunto que me interessa tanto, que é o estudo do processo penal e as novas tecnologias e os novos desenvolvimentos. E queria agradecer especialmente ao Francisco Brito Cruz, diretor executivo do InternetLab, e à Bárbara Simão, que estão aqui.

Eu sou professor de processo penal. Defendo as ciências criminais conjuntas e acho que nós começamos a colocar tecnologia nas ciências criminais conjuntas. Ou se é que a gente vai conseguir tirar as ciências criminais conjuntas da tecnologia que nós temos hoje em dia. Mas eu falo principalmente a partir do marco do processo penal, que é a minha área e que eu me sinto mais à vontade a dizer. Principalmente, eu me sinto mais à vontade a fazer algumas considerações, que, num primeiro momento, talvez possam passar a impressão de que são críticas, e são, mas não são críticas destrutivas, mas críticas construtivas para minha área do direito.

Eu tenho cada vez mais gostado de trabalhar o processo penal brasileiro, não abrindo mão das experiências estrangeiras, mas preocupado em que o processo penal brasileiro seja efetivamente brasileiro e não uma colcha de retalhos de direitos estrangeiros, que tentam nos enfiar goela abaixo, porque talvez uma casta da intelectualidade acha que isso é mais interessante para o povo brasileiro do que o que o povo brasileiro precisa de fato.

Com essa perspectiva, o processo penal brasileiro, sendo muito realista, ele não é nem garantista, nem punitivista. Eu encontro decisões de todas as formas. Se eu tivesse que fazer um neologismo, eu diria que o processo penal brasileiro é "seletivista" e ocasional. Ocasionalmente, ele decide de uma forma, ocasionalmente decide de outra forma. Isso é péssimo. Isso é péssimo porque, aos olhos da população - que na

verdade é a quem se dirige o processo penal, são os principais atingidos -, isso gera um descrédito em todas as instituições que trabalham no sistema criminal. Todas. Porque cada vez mais, a população percebe que ela não tem guarida, que ela não tem certeza de nada e que a única certeza que ela tem é que no sistema que nós vivemos, "quem pode mais chora menos", como diria minha avó.

Aos olhos dos operadores do direito, o processo penal, a partir dessa constatação, ele é uma perfeita, acabada e completa insegurança jurídica. Quem distribui a Constituição brasileira não são os juízes e os magistrados do nosso país, quem distribui a Constituição brasileira é o funcionário do distribuidor dos fóruns. Se for distribuído para a Turma A, para a Câmara A, a Constituição vai ser uma, e se for distribuída para o Juiz B, para a Câmara B, a Constituição será outra. Portanto, de verdade, quem garante a Constituição para alguns e nega para outros é o funcionário do distribuidor. E por que isso é assim? Por que que isso é assim em face da tecnologia e por que que isso é assim no Brasil de hoje? Isso é assim por uma razão que talvez seja um problema nacional, que talvez precisemos começar a dar passos firmes para consertar. Não que eu espere consertar aqui, mas talvez indicar um caminho para que possamos começar. E a outra realidade é uma realidade atávica ao processo penal, não apenas brasileiro, mas em geral no mundo inteiro.

A REALIDADE ATÁVICA BRASILEIRA

Comecemos pela atávica. O processo penal é um processo que foi construído, concebido, desenvolvido e guarda uma cultura e normas legais, comportamentais e culturais para um mundo sólido, foram construídas para um mundo físico e, portanto, para uma sociedade que não é mais a nossa. É a sociedade do passado que não nos serve mais. O nosso tempo é um tempo

diferente do tempo do processo. A nossa velocidade é uma velocidade diferente da do processo e a nossa busca de resultados é algo que nem se aplica ao processo. Esse é um problema atávico do processo penal. Precisamos começar a construir um processo penal não para outros tempos ou outra sociedade, mas talvez para outro ambiente e ter os dois, o antigo e o novo, que possam agir cada qual na sua mais apropriada condição.

O problema situacional do Brasil, portanto, não é atávico, não é congênito, a ideia de processo penal, é que o processo - e aqui eu quero assumir todas as responsabilidades com relação às insuficiências acadêmicas e científicas - não é discutido e desenvolvido a partir do que seja melhor, mas normalmente é discutido a partir de posições institucionais em que as discussões têm muito mais a ver com a prevalência de poder, ou de determinadas instituições sobre outras, do que efetivamente o bem comum.

O que vou dizer aos senhores é um dado histórico. Se pegarmos todos os marcos de legislações processuais penais consistentes, não leis pontuais, mas algo como o código, para ficar mais fácil. E se pegarmos os códigos desde 1832, passando por todos os códigos estaduais, o código federal pós-República, Primeira República e o atual código, que não é nada mais nada menos que de 1941. Mil novecentos e quarenta e um. Tirando alguns seres humanos privilegiados, o que mais dura de 1941 até hoje? Qual era a tecnologia, cultura, sociedade, padrão ético, moral, constitucional e legal que havia em 1941 que existe hoje? É tudo diferente, mas o processo penal persiste. O processo penal é uma dessas sobrevivências.

Até o código de 1941, todos os códigos brasileiros foram aprovados na mão de ferro. O Brasil não tem na sua história nenhum código de processo penal aprovado de uma forma democrática. Todos foram impostos, mais ou menos impostos. Isso não é coincidência. Para que tenhamos uma história

mais recente, em 2009, o projeto de Código Civil e o projeto de Código Processo Penal saíram do Senado Federal e se encaminharam para a Câmara. O Código de Processo Penal na frente, com prioridade de trâmite e o Código Processo Civil depois. O Código Processo Civil foi comentado, melhorado, mudado algumas partes, debatido. Foi posto à aprovação e homologação, entrou em vigência em 2015. E o Código de Processo Penal ainda se discute na Câmara dos Deputados, na primeira rodada. Depois que acabar isso - e obviamente não acabará esse ano de eleição - ele volta para o Senado, para depois voltar para a Câmara, depois para o Senado, para a Câmara, para o Senado e fica assim. Essa é uma realidade. Isso é um dado objetivo. Eu estou contando história para vocês.

A sociedade brasileira está envolta em tecnologia. Eu vejo muitas pessoas aqui presentes que me ouvem e veem o celular. Eu, quando venho para cá, tenho um certo hábito. Já tenho uma certa história de vir para essa faculdade. Eu já vim de metrô, eu já vim de táxi. Eu só não vim de bike, mas eu já vim de tudo o que vocês podem imaginar, em vários anos da minha vida. Mas quando saí de casa hoje, eu liguei o Waze para dizer para mim que era o melhor caminho para vir para cá. Nesse trecho de lá até aqui, eu vi minha mãe pelo vídeo, eu conversei com a minha esposa, eu resolvi alguns problemas. E respondi alguns *whatsapps*. Como vocês veem, eu sou o motorista irresponsável. Ouvi música que tinha no meu celular e que eu gosto de ouvir quando venho para a faculdade. E também vi as últimas notícias que saíram, afinal de contas, hoje é um dia agitado no campo processual penal no Brasil.

Talvez a última coisa que eu veja antes de dormir seja a tela do meu celular e, com certeza, a primeira coisa que eu vejo quando eu acordo é a tela do celular, porque nele tem um despertador. Difícil imaginar que alguém consiga se desconectar dessas questões todas. A sociedade, portanto, hoje é

uma sociedade atavicamente ligada, por vontade própria, por desejo próprio, a esse mundo tecnológico. Isso tem um preço a ser pago. Esse preço a ser pago é uma necessária adaptação pela qual nós precisamos passar. Nós precisamos passar psicologicamente, nós precisamos passar socialmente, porque muitas vezes nós estamos com as pessoas em momentos muito curtos de presença física e, mesmo assim, ambas as pessoas estão falando no celular ou mexendo no celular, ou seja, estão em outro lugar. E precisamos também mudar com relação à questão do processo penal.

ARE 1.042.075

Eu queria trazer um problema. Esse problema é um dado objetivo muito importante, que eu, quando fui convidado pela Bárbara para vir aqui fazer essa apresentação, fiquei muito feliz quando ela me deu a data, porque eu acreditei que até o dia de hoje teria sido julgado, no Supremo Tribunal Federal, um tema que seria fantástico ser explorado na palestra de hoje. Mas a palestra veio, o dia chegou, e o Supremo não julgou o caso do Agravo em Recurso Extraordinário (ARE) 1.042.075, deixando essa burocracia do número de lado, vamos tratar do caso em si. Esse caso consta como Tema 977, de repercussão geral. O Supremo Tribunal Federal elegeu esse tema como de repercussão geral. Portanto, para o Supremo Tribunal Federal, que zela pelas questões constitucionais mais relevantes, esse é um dos temas de repercussão geral. Portanto, é um dos assuntos mais relevantes.

A situação é a seguinte: no caso - passo brevemente pelos fatos para que possamos entender o contexto - no Rio de Janeiro, uma pessoa foi roubada. Uma pessoa que se imagina o acusado, o culpado pelo roubo, o agente da conduta, foge. Na sua fuga, ele deixa cair o próprio celular. A vítima recolhe o celular do

chão e leva o celular até a delegacia de polícia, informa o ocorrido e entrega o celular para os policiais. Os policiais, então, entram no celular sem qualquer tipo de cuidado ou autorização judicial. Acessam as fotografias, as últimas ligações, o cadastro de imagens e as agendas. Com isso, os policiais chegam na namorada do dono do celular. Chegando na namorada, eles chegaram no dono do celular. Chegando no dono do celular, eles prenderam o rapaz. O rapaz foi acusado de roubo e condenado em primeira instância.

O Tribunal de Justiça do Rio de Janeiro anulou o processo, dizendo que todo o caminho da coleta de provas começou a partir de uma invasão de celular sem ordem judicial prévia e, portanto, uma prova ilícita. Anula todas as demais provas decorrentes a partir dali, e a pessoa é inocentada. O Ministério Público do Rio de Janeiro recorre e chega no Supremo Tribunal Federal, para encurtar o caminho. Quando chega no Supremo Tribunal Federal, a questão também teve toda uma burocracia, tanto que é um Agravo em Recurso Extraordinário. Teve uma triagem que não foi aceita e não vem ao caso. Mas o que importa é que, o relator deste caso é o ministro Dias Toffoli.

O ministro Dias Toffoli se depara com a questão e vota no seguinte sentido: através de precedentes do Supremo Tribunal Federal, ele explica que os dados que estavam dentro do celular não faziam parte da comunicação telefônica e, por não fazerem parte de comunicação telefônica - já que estavam parados, estáticos dentro, uma vez que a comunicação seria o trânsito -, aplicando o inciso XII do artigo 5º em um enfrentamento do artigo 144, parágrafo 4º. O Ministro Dias Toffoli disse: "*Aqui, eu não tenho a proteção da Lei 9.296. Eu não preciso de ordem judicial. Os dados estavam lá. E, além do mais, isso já foi julgado no precedente no Habeas Corpus 91.867/12 do Paraná, e foi decidido que isso poderia ser pego*". Só uma curiosidade: lendo esse *habeas corpus*, que era um dos precedentes invoca-

dos pelo ministro - muito apropriado para o caso, porque era ao feitio -, da outra vez também tinha-se tido acesso aos dados de um celular sem ordem prévia.

O ministro então relator do caso, ministro Gilmar Mendes, decidiu que a prova era lícita, que se podia pegar todos os dados que estivessem ali, porque não era comunicação telefônica. Até porque, o ministro Gilmar Mendes na época, escreveu no voto: "*O celular é como se fosse um bloco de anotação. Os telefones que as pessoas tiveram é um conjunto numérico. Isso não tem nada a ver com a intimidade de ninguém e, portanto, a prova é lícita*". O ministro Dias Toffoli, com base nesse precedente, invocou novamente a diferença entre comunicação telefônica e dados telefônicos estáticos e votou pela licitude da prova.

Ele sugere - como é um caso de repercussão geral, para quem não sabe, eles ao final têm que se votar uma tese, um texto que passaria a ser o referencial para os próximos casos. Já que num caso de repercussão geral, deve-se julgar os próximos casos da vida, da vida humana, da vida da sociedade brasileira com base nele - o seguinte: "*É lícita a prova obtida pela autoridade policial sem autorização judicial, mediante acesso ao registro telefônico, agenda de contatos de celular apreendido, ato contínuo, no local do crime, atribuído ao acusado, não configurando esse acesso, ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo*". Na interpretação dele, não há qualquer tipo de perturbação com acesso aos dados da intimidade e da privacidade do proprietário do celular.

Logo depois do voto do ministro Dias Toffoli, o próximo ministro a votar é o ministro Gilmar Mendes. O ministro Gilmar Mendes, então, vota em sentido contrário ao decidido pelo ministro Dias Toffoli e ele diz que está votando contrário ao que ele havia decidido em 2012. E ele alega - e eu quero usar as expressões dele, que constam do voto, porque relevantes - o seguinte: "*A modificação das circunstâncias fáticas*

e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação, do tráfico de dados e dos aparelhos smartphones, leva-nos, nos dias atuais, a solução distinta. Sem dúvidas, cada vez mais, a nossa vida quase inteira está registrada em nossos aparelhos celulares". Ele abre o voto dele com essa consideração, desenvolve o voto, dizendo, concordando que existe uma diferença entre comunicação telefônica e dados registrados no telefone, mas diz que a questão aqui é outra.

Eu não vou me ater ao voto, mas vou direto ao ponto: quais são as novidades legislativas para ele, que apareceram entre o seu voto de 2012 e o ano de 2020 - que foi quando esse caso começou a ser julgado e ainda não acabou? Foi o Marco Civil da Internet. Com relação ao Marco Civil da Internet, ele destaca, no capítulo 2 que trata dos direitos e garantias dos usuários, ele destaca o artigo 7º que diz: "*o acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (iii) a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial*". Então, o que ele diz foi: "*quando eu dei o voto lá atrás, isso aqui não existia. Agora que existe...*".

O caso ainda está aberto. Os votos podem mudar, as posições podem ser alteradas. E quando o ministro Gilmar Mendes fez esse voto, mudando a sua posição - e eu ainda não entrei nas novidades fáticas, eu estou falando só das jurídicas - ele foi seguido pelo ministro Edson Fachin, que votou exatamente no mesmo sentido. Eles não destacaram a mudança constitucional de 2021, que inseriu, dentro do capítulo dos direitos e garantias fundamentais, a intimidade informática. Ele não citou isso porque não existia no momento do voto. Essa é uma outra novidade que surgiu, assim como também a Convenção de Budapeste, que foi incorporada e também poderia ser usada aqui se existisse naquela época. Eu estou me atendo ao voto.

Com relação à situação fática, eu gostaria de destacar as palavras exatas do voto: "*a utilização habitual das novas tecnologias torna necessária a obtenção de prova de tipo tecnológico, que, embora contribua para aprimorar a eficácia estatal na persecução dos delitos, em igual medida aumentará o risco de lesividade ao direito fundamental à autodeterminação informática das pessoas investigadas*".

A sugestão de ementa de tese para essa repercussão, por parte do ministro Gilmar Mendes, é a seguinte: "*o acesso ao registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado, depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade de adequação da medida e delimita a sua abrangência nos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e de dados dos indivíduos*". E cita o artigo 5º, incisos X e XX da Constituição Federal. Portanto, ele desloca a proteção do inciso XII, que fala das comunicações, para o inciso X, que trata da intimidade e da privacidade. Por isso, fez questão de destacar aquilo naquele momento inicial. Ele é seguido pelo ministro Fachin. O ministro Alexandre de Moraes pediu vista, e estamos nessa situação.

A questão está aberta, e é uma questão crucial, me parece, para explorarmos hoje, como um dado, um exemplo. Estou trazendo o exemplo concreto porque conjecturas a respeito do que deve ser feito, se não tiver uma repercussão prática e com uma repercussão geral como essa, também não têm muita utilidade para nós. O mundo hoje em dia demanda essa questão menos dogmática - para nada -, e um pouco mais de teoria concreta dos fatos da vida real.

E por falar nisso, vamos tratar a vida como ela é. A partir desse ponto, são minhas reflexões. Eu gostaria de propor essas reflexões aos senhores.

A NATUREZA DAS COISAS

Se nós olharmos para a doutrina processual penal que nos marcou até o presente momento, e para a legislação processual penal, estaremos olhando para o lugar errado. Basta dizer que, olhando para a lei processual penal de 1940, existe a fundamentação do voto do ministro Dias Toffoli, que recorreu à fundamentação do STJ, o qual já teria citado, dizendo que "*se a busca pessoal exige circunstâncias que evidenciam o perigo de risco, mas não exige ordem judicial prévia, e a pessoa porta o celular com ela, é uma extensão natural que se possa fazer a verificação do celular sem ordem judicial prévia, porque o celular está com a pessoa*".

Não me parece que essa seja a melhor opção.

Dois anos atrás, eu fiz uma matéria de pós-graduação na faculdade, junto com dois professores, o senhor Marcos Zilli e o professor José Raul Gavião de Almeida, que era de Processo Penal e Tecnologia. E quanto a uma das coisas que nós queríamos discutir – e, de fato, discutimos, naquele momento –, eu tinha uma visão que me parecia um pouco vanguardista, mas, nesse presente momento, eu já acho que ela é muito careta e tenho uma outra. Eu vou contar para os senhores. Ainda bem que eu não escrevi, e me impuseram: "*escreva, escreva*", mas eu tinha outras coisas para fazer e não escrevi. E hoje eu fico feliz, ainda bem que não escrevi, porque o professor Tércio escreveu um artigo brilhante sobre a questão da intimidade da comunicação, essas questões, e depois de 20 anos ou 30 anos, ele escreveu um outro artigo dizendo: "*olha, eu mudei de ideia*". Eu teria mudado em dois anos. Não é uma coisa que seja muito nobre, mas eu vou contar aos senhores, com o compromisso de que os senhores não comentem com ninguém, para que ninguém saiba.

Em 2020, eu olhava o celular com a necessidade de proteção do celular - e quando eu falo do celular, entenda o computador, iPad, *smartphone*, enfim, *gadgets* inteligentes. Eu

olhava aquilo como uma necessidade de que aquele objeto fosse interpretado como uma extensão do conceito de casa. Por que indo nos primórdios da preservação da casa como um lugar inviolável, aquilo que também está no inciso X, aquilo remetia à ideia de que eu preciso ter um lugar - o ser humano precisa ter um lugar - em que a sua intimidade seja respeitada e seja absoluta, porque o ser humano precisa - e essa é expressão criada doutrinariamente - ter o direito de estar só.

O Estado não pode aviltar isso, porque isso perturba, as pessoas precisam ter vidas próprias. E no espaço da sua casa, na intimidade da casa, na privacidade dos dados, nas coisas que você faz, imagine, por exemplo, uma agenda, não se pode ter a sua violação, a não ser por casos excepcionalíssimos e, no caso, ordem judicial.

Eu achava que seria importante nós começarmos a fazer uma extensão, pensava em 2020, porque ainda não tinha o dispositivo da intimidade que foi inserido depois. Então, eu queria dar uma extensão como direito fundamental para proteção do indivíduo, a partir do inciso X, porque é lá o que me parecia possível estender, era o conceito de casa. Por quê? Porque se historicamente a casa foi preservada porque lá eu tinha as coisas mais íntimas, eu guardava as coisas mais íntimas naquele ambiente, hoje, eu guardo as coisas mais íntimas no celular. Muito mais coisa tem a revelar o celular de cada um, do que o que eu guardo na minha casa. Se a pessoa entrar na minha casa e revistar tudo o que tem lá, ela vai saber muito menos da minha intimidade do que se ela pegar o meu celular e for investigar.

Eu achava que, portanto, o conceito de casa deveria ser estendido para que se construísse um conceito amplo, para que casa não fosse só o lugar onde se mora, mas se fosse também o lugar onde se preserva a intimidade, e aí o aparelho celular seria abarcado por isso. Hoje, eu não penso mais assim. E hoje,

/ TALVEZ A INTIMIDADE NESSE MUNDO SEJA UMA INTIMIDADE REALMENTE [...] QUE PRECISA SER REPENSADA, PORQUE ELA SOZINHA JÁ NÃO SE BASTA /

eu não penso mais assim porque eu talvez tenha caminhado e dado passos para efetivamente começar a fazer uma construção diferente, nova. Porque, se eu não fizer uma construção nova, eu ainda fico dentro dos lugares antigos, e com isso, eu não consigo efetivamente fazer um processo penal nos moldes atuais, eu vou ter que ficar emprestando palavra, e as palavras têm significados. E se eu começar a emprestar as palavras para lugares e coisas para as quais elas não foram criadas, elas perdem até mesmo o contexto original, e aí tudo fica diluído, e aí não é mais a sociedade que é líquida, como diria Bauman, mas aí a própria linguagem fica líquida, e eu não me lembro de ter lido nenhum livro de Bauman sobre a linguagem líquida. Mas nós fazemos isso. Nós, no Direito, tornamos a linguagem líquida, damos nomes para as coisas e mudamos. Queremos achar que mudando nomes nós mudamos a natureza das coisas, mas as coisas são o que são.

DIGNIDADE DA PESSOA HUMANA

Eu não vou ficar fazendo aqui a diferença sobre o direito à intimidade, direito à privacidade, são coisas distintas. Não é o caso de se discutir isso agora. Vamos tratar esses dois espaços no seu lugar comum. Qual é o lugar comum da intimidade, da privacidade? São os direitos da personalidade. Os direitos da personalidade implicam intimidade, privacidade e tantos outros. Onde os direitos da personalidade buscam guarida? Qual é o passo atrás? Qual é o passo fundamental que eu dou? Por que existem os direitos da personalidade? Porque, sem esse nome, no passado, mas mais recentemente com esse nome, se reconhece a dignidade da pessoa humana.

Portanto, garantir às pessoas intimidade e privacidade é um respeito à dignidade da pessoa humana. Que não está no artigo 5º dos direitos e garantias fundamentais, a dignidade da

pessoa humana está no inciso III do artigo 1º da Constituição. E o artigo 1º da Constituição está no capítulo dos princípios fundamentais da Constituição. O nosso constituinte, quando fez esse capítulo primeiro dos princípios fundamentais, disse o seguinte: "*Olha, se nessa Constituição que eu estou fazendo, no futuro, vocês precisarem de alguma coisa, houver algum tipo de conflito, vocês tiverem necessidades outras, que não estão previstas aqui. Olhem no capítulo 1, os princípios fundamentais dessa Constituição, porque isso vai orientar o que pode ou não ser feito dentro dessa Constituição*".

A dignidade da pessoa humana, portanto, faz com que eu tenha uma proteção da intimidade e da privacidade, que não precisa estar vinculada a lugares físicos. Porque se estiver vinculado a lugares físicos, eu ainda estou preso ao mundo físico. E se eu estou preso ao mundo físico, eu não consigo pensar ou tornar normas que sejam aceitáveis ou apropriadas para mundos digitais. Com tempos, lugares e modos de outra velocidade e com outra razão e como outra lógica.

Aqui eu faço uma passagem importante, e eu quero terminar de fazer essa passagem para que todos vejam como eu faço a ligação das duas coisas depois. No capítulo "a vida como ela é", nas nossas casas, no mundo físico, que eu abandonei, a minha ideia original tinha uma coisa que não cabia. Algo que eu nunca deixei nas casas. Eu nunca deixo na minha casa. Carrego comigo. São os desejos, os sentimentos, as emoções. O que é imaterial e tão relevante para a minha intimidade, para minha privacidade além de para mim, como pessoa. Essas questões imateriais, elas podem ficar em memórias que eu tenho de objetos da minha casa, mas quem olha aquele objeto não sente as emoções que eu sinto. Aquelas emoções são minhas.

Quando a teoria da intimidade, da privacidade ou dos círculos concêntricos foi construída, e quando a ideia de casa foi criada, as pessoas imaginavam o local onde se deixavam

registros, mas não onde se deixavam sentimentos, desejos, emoções, pensamentos, a menos que ficassem escritos.

Aqui, eu deixo tudo isso. Tudo isso está aqui. Basta que alguém consiga compreender, basta que alguém consiga ler. E já existe esse alguém. Que faz isso assim, chama-se Inteligência Artificial. Nós estamos sendo lidos no que nós carregamos na alma. Todos os minutos da nossa vida que nós ligamos esse aparelho. Nós estamos entregando isso. Todos os instantes. Isso são dados. Dados que são absorvidos velozmente, acumulados velozmente e trabalhados para que desses dados se obtenham informações. Informações do quê? Informações de nós.

RENDIÇÃO

A tecnologia da informação e a inteligência artificial ultrapassaram, faz muito tempo e numa velocidade muito rápida, os registros do que nós somos. Nós já entregamos nossos dados há muito tempo. Hoje, a tecnologia da informação não se satisfaz mais com o saber quem eu sou. Saber quem eu sou, é uma informação de gerações passadas para a inteligência artificial. Agora, a inteligência artificial prediz quem eu devo ser. A inteligência artificial implanta desejos, vontades, sentimentos, aspirações, ideias, pensamentos com base naquilo que eu entrego para ela das minhas tendências. Eu deixo portanto de ser o que eu acho que é um livre arbítrio meu - isso implica até em programas religiosos - e passou a ser aquilo que alguém, das BigTechs, deseja que eu seja, por várias razões, sejam econômicas, políticas, por várias razões. E nós tivemos muitas experiências em outros países e documentários feitos exatamente por essa condição.

E por que eu fiz esse parênteses? Para muitas pessoas, chocante; para outras pessoas, "*pô, mas ele precisava dizer isso agora? Que cara desagradável. Que quando ele estava dizendo*

isso do mundo jurídico, eu ia para casa dormir feliz, mas agora que ele está dizendo isso, eu vou pra casa e como é que eu faço pra me despedir do celular?".

Eu tenho um relógio que há muito tempo me pede para dormir comigo. Eu tirava ele para dormir e quando eu voltava de manhã cedo, ele falava assim: "*e suas horas de sono?*". Por conta dessa palestra, faz três dias que eu, porque ele sempre pediu: "*use três noites*", usei as três noites. Hoje de manhã foi a terceira noite. E aí, quando eu acordei, eu olhei para o celular, peguei as coisas, enfim, vi as mensagens. Acordei estressado. Aí, olhei o relógio e ele tinha me dito a hora e o minuto que eu dormi, a hora e o minuto que eu acordei, quanto de tempo verdadeiramente eu dormi, quanto foi meu sono x, meu sono y. Alguém passou a saber isso.

Eu volto agora para o processo penal. Quem acha que o celular tem pouca coisa agora, e que eu posso fazer a abertura dele sem uma ordem judicial prévia e sem uma análise de ponderação de proporcionalidade? Agora que os senhores sabem o que entregam, isso tem um nome, esse fenômeno se chama "rendição". Quem trouxe essa expressão da rendição humana aos *gadgets* e às *Bigtechs* foi Shoshana Zuboff, uma professora titular de administração da Harvard Business School. Ela escreveu um livro fantástico, se chama "*O capitalismo da vigilância*", que eu recomendo que todos leiam. Precisa ter fôlego, mas vale a pena ler. Aliás, cada vez mais, eu me convenço que tudo o que vale a pena ler precisa de fôlego. Qualquer coisa que caiba numa profundidade de um pires, serve como uma mensagem de autoajuda e acabou. Ponto final. Aquelas coisas: seja forte, seja feliz, pense positivo, cante essa música, e todos os seus desejos se realizarão hoje. Eu fico pensando se alguém realmente faz aquilo.

Diante dessa realidade a qual nós nos rendemos, a pergunta é: o celular é nossa casa? Não, o celular não é a nossa casa. A

nossa casa não é maior que um celular, o nosso celular é muito maior que a nossa casa. O celular é quase tudo o que nós somos. E pior, nós precisamos do celular para dizer o que nós queremos ser, o que eu preciso comprar, o que eu tenho que gostar, o que eu preciso ler.

E se os senhores forem ler nos aparelhos inteligentes. Eles vão saber exatamente acompanhar os olhos dos senhores e saber quanto tempo os senhores param em determinada coisa. E quando os senhores comprarem o livro pelo Kindle, o livro já virá marcado e grifado - um livro novinho. Quando eu comprei um livro no Kindle, eu vi todo riscado, fui lá e cliquei e dizia "*73% das pessoas que compraram esse livro grifaram esse trecho e gostaram desse trecho*". Os caras estão me dizendo o que as pessoas gostam, mas isso não sou eu. Mas aí eu passei a gostar daquele negócio porque eu achava que não gostar daquilo...bom, 73% gostaram, porque eu não estou gostando? E aí eu comecei a pensar, mas será que alguém está mentindo para mim? Será que 73% gostaram mesmo? Eu gostei disso? Há muito tempo, já parei de ler. Perdi a leitura do livro. Agora o livro deixou de ser o que é. Um hábito sozinho. O livro agora é um hábito que eu faço pra alguém ver para onde o olho.

Nós não temos mais intimidade. E aqui é um problema crucial para essa discussão. Eu posso abrir mão da minha intimidade para algumas pessoas ou para alguns lugares, e exigir que na investigação criminal exista uma ordem prévia do juiz? Olha que desafio. Por que eu posso entregar para as pessoas, mas para polícia e para os órgãos de investigação, eu preciso de ordem judicial?

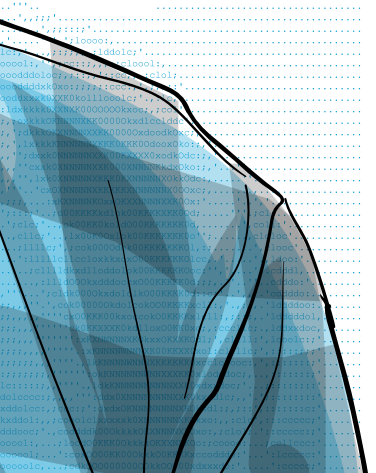
Então, talvez a intimidade nesse mundo seja uma intimidade realmente como conceito de direito fundamental que precisa ser repensada, porque ela sozinha já não se basta. Porque a intimidade com ela foi criada lá atrás, ela era quase um ato isolado, sozinho, privado, exclusivo, e agora não é mais.

Como se pode ver, eu estou longe de ter vindo aqui para apresentar para os senhores as soluções de qualquer coisa, porque realmente eu não sei, mas tenho certeza que deixei os senhores bastante incomodados. Se eu consegui fazer isso, eu atingi o meu objetivo.

Muito obrigado. Boa noite. 

06.

CONSTITUCIONALISMO DIGITAL NA RELAÇÃO ENTRE DADOS PESSOAIS E DIREITO PENAL NO BRASIL: DIAGNÓSTICOS, PERSPECTIVAS E UM CHAMADO[1]



Paulo Renã da Silva Santarém

Em 2006, o professor da Universidade de São Paulo Maurício Zanoide de Moraes já escrevia[2] que estava se institucionalizando o caos. Em 2022, chegamos à conclusão de que, passados 16 anos, as coisas realmente não melhoraram. E eu quero – a partir da reflexão que o professor promoveu, com foco no Supremo Tribunal Federal – avançar para outra abordagem: a do processo legislativo. Quero observar as propostas normativas que podem afetar, para melhor ou para pior, as garantias de proteção de dados no âmbito do processo penal de maneira geral.

O cenário normativo vigente poderia ser suficiente para o respeito e a maximização das garantias constitucionais, das garantias individuais, da proteção de dados pessoais. Temos a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018, conhecida pela sigla LGPD)[3] que fez aniversário em agosto de 2022: quatro anos desde a sanção e dois anos da vigência (um ano da vigência plena, dois anos da vigência das normas de garantia).[4] Mas sua aplicação não é plena para segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, mas a própria LGPD define que a lei específica a ser criada deverá prever medidas proporcionais e estritamente necessárias a atender o interesse público, o devido processo legal e os princípios gerais de proteção dos direitos dos titulares de dados pessoais nela previstos. Ela não amarra completamente as regras para persecução penal, mas direciona minimamente o que se pode exigir no enfrentamento ao crime cibernético.

Além da LGPD, a Lei nº 9.296, de 1996,[5] regula interceptações telefônicas e telemáticas. Em 2019,[6] acrescentaram-se a ela regras para a captação sonora ambiental e a criminalização de ordens judiciais ilegais "*para a interceptação telefônica telemática*" e para "*quebrar segredo de Justiça*". É uma reação ao episódio absolutamente caótico de nossa história republicana recente, em que o então juiz Sérgio Moro autorizou a

divulgação de dados pessoais e conteúdo fora do tempo de validade fixado na sua própria ordem judicial de interceptação. O argumento foi de que o material colhido em procedimento fora da autorização não afetaria as pessoas envolvidas e, portanto, não estaria proibido de ser divulgado. Em vez de primar pela preservação do interesse privado em relação ao sigilo das comunicações, o juiz fez uma leitura e ao contrário da garantia de direitos individuais de proteção da privacidade de dados pessoais e do conteúdo de conversas telefônicas.[7] Bom, esse tipo de decisão foi criminalizada em 2019.

Antes, adveio o Marco Civil da Internet no Brasil (Lei nº 12.965, de 2014),[8] inaugurando o estabelecimento mínimo de proteção legal para alguns dados digitais. O MCI previu requisitos para a guarda de dados, desde a retenção até a preservação, passando pelo acesso de autoridades a esses dados. Retomo o diálogo com o professor Zanoide: se compartilhamos tantos dados com as *Big Techs*, o que justifica ter ressalvas no compartilhamento de dados pessoais com o Estado? É um ponto fundamental para os direitos individuais, em sua contraposição ao poder público.

O Estado deveria ser, ao mesmo tempo, um guardião, a quem cabe preservar, promover e defender nossos direitos; e um fiscal, a quem cabe analisar se estamos violando direitos ou até mesmo cometendo crimes. E na medida em que a defesa de direitos pretende limitar o abuso por parte das empresas privadas, não faz sentido que o Estado esteja do outro lado, dando "mau exemplo". O Estado não pode, a pretexto de realizar direitos, incorrer na violação sistemática de direitos, ou na redução sistemática de direitos como procedimento. Pelo contrário, ele tem que ter uma postura estritamente legalista: por meios estritamente autorizados em lei, cabe ao poder público promover direitos, promover justiça, em completa coerência com o ideal do Estado Democrático de Direito e os

fundamentos explícitos e implícitos no artigo 1º da Constituição da República Federativa de 1988.

Finalizo o diagnóstico sobre o cenário normativo citando a Constituição, emendada em 2022. Aprimorando as garantias originárias do artigo 5º, da presunção de inocência, das garantias do inciso XII, da proteção do sigilo de dados telefônicos e até sigilo bancário, a Emenda Constitucional nº 115 inseriu, no artigo 5º, o inciso LXXIX. Eu sou da época em que os telefones faziam muito menos coisas, bem como da época que o artigo 5º só ia até o inciso LXXVIII, desde 2004. Agora, o acréscimo de mais um inciso veio afirmar que os dados pessoais são objeto de uma garantia constitucional: de proteção de dados pessoais, inclusive digitais, nos termos da LGPD.

Pois bem, nesse cenário, estão sendo debatidas pelo Congresso Nacional algumas propostas normativas. Gostaria de que as pessoas interessadas em Direitos Fundamentais e Processo Penal na era digital observassem os desafios inaugurados pela tecnologia digital com uma nova sensibilidade. Miremos essas propostas normativas com um olhar específico de afirmação de nossos direitos fundamentais, e para isso lanço mão do que se pode chamar de "Constitucionalismo Digital".

Entre os principais debates sob os holofotes neste início de 2023 temos a reformulação do Código de Processo Penal, por meio do projeto de lei nº 8.045, de 2010. O assunto, muito relevante, assistiu a uma aceleração recente, mesmo sendo muito complexo e, reputo eu, estando pouco amadurecido. É uma matéria árida, não só por envolver numerosos dispositivos com incisos, parágrafos, alíneas, mas por exigir e muita tecnicidade legislativa. Um debate complicado vem sendo feito por um grupo de trabalho na Câmara dos Deputados.[9] Os temas analisados incluem a forma de coleta das provas digitais, a ideia de uma cadeia de custódia, e outras tantas garantias individuais que estabelecessem um ambiente jurí-

/ O ESTADO NÃO PODE, A PRETEXTO DE REALIZAR DIREITOS, INCORRER NA VIOLAÇÃO SISTEMÁTICA DE DIREITOS /

dico protetivo adequado à perspectiva de que hoje o celular e outros dispositivos eletrônicos permitem identificar a pessoa para além do que ela própria sabe de si mesma.

Nós não temos condições de, organicamente, saber o momento preciso em que adormecemos, nem a que horas exatamente despertamos, por mais que a primeira coisa que vejamos a cada dia seja uma tela. Tem certos dados, como a qualidade do nosso sono, que a gente mesmo não pode inferir. A quantidade de tempo de tela que temos no consumo de determinado aplicativo ou o rastreamento da localização, enfim, vários dados pessoais produzidos a partir do processamento dessas informações telemáticas e que vão além, repito, do que cada pessoa sabe sobre si mesma. Nessa medida, não se trata do fim da privacidade ou da proteção de dados pessoais, mas, antes, o extremo contrário. Temos um cenário que exige a maior necessidade de proteção jamais existente.

Mas na direção oposta, a reformulação do CPP, nos termos ora em análise: a) expande desproporcionalmente a retenção massiva de dados para futuras investigações; b) retrocede em garantias com relação à interceptação das comunicações; c) cria certas exigências tecnológicas para os provedores de serviço que podem provocar a impressão de vulnerabilidades de segurança nos sistemas e nos serviços que nos são oferecidos; e d) legitima a prática do chamado hacking governamental ou *hacking* realizado por agentes estatais, explorando vulnerabilidades dos sistemas telemáticos. Em vez de serem resolvidas ou solucionadas pelo poder público, essas vulnerabilidades estariam sendo exploradas, mantendo abertas portas clandestinas ou caminhos não detectados pelas pessoas que poderiam ser exploradas por pessoas deliberadamente mal-intencionadas, por criminosos, fora a possibilidade de abusos por parte do próprio poder público.

Além do Código de Processo Penal, passa por análise legislativa o projeto de lei da chamada "LGPD Penal": uma lei geral de proteção de dados pessoais para preencher a já mencionada inaplicabilidade específica da LGPD para segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. O tema ensejou, em novembro de 2019, a convocação, pela Câmara dos Deputados, de uma comissão de especialistas, que apresentou, um ano depois, um anteprojeto de lei (APL), com uma minuta equilibrada, ainda que fique aquém de algumas expectativas mais esperançosas. Todavia, objetivamente, o APL se encontra "ultrapassado" pelo projeto de lei nº 1515, de 2022, formalmente apresentado na Câmara dos Deputados pelo dep. Coronel Armando. A proposta do deputado se mostra absolutamente redutora de garantias, pois estabelece mais instrumentos para que o Estado acesse nossos dados pessoais, e menos preocupações em afirmar os nossos direitos individuais. O PL nº 1515/2022 é muito menos protetivo em comparação ao APL, mas foi formalizado – ao passo que a minuta da comissão foi entregue ainda ao Rodrigo Maia, em novembro de 2020, mas nunca virou projeto de lei.

Somando a reforma do CPP e a LGPD Penal, o saldo são duas propostas de mais quebras de sigilo, mais restrição de liberdade em situações de menor presunção de inocência, mais paradigma de persecução criminal e segurança pública, com menos proteção adequada aos nossos dados pessoais, menos segurança jurídica aos controladores, e menos harmonia na cooperação internacional. Enfim, lidamos com um âmbito de aplicação excessiva, uma base principiológica frágil, um prejuízo às bases de tratamento previstas na LGPD e a redução de direitos, além de afetação tecnológica em termos de segurança da informação e de garantias na transferência internacional de dados.

Fecho com um terceiro elemento pessimista: a Convenção de Budapeste sobre o cibercrime.[10] Por mais que ela pareça ser um caminho adequado para uma melhor racionalização da forma como o Brasil pode produzir provas digitais, estabelecer uma tipologia de crimes cibernéticos e cooperar internacionalmente – o que percebemos é que o processo de adesão foi açodado. O Brasil foi convidado para aderir à Convenção em dezembro de 2019. É uma norma de 2001, mas formalmente o Brasil só foi convidado a aderir em dezembro de 2019.[11] Não é verdade o argumento de que o Brasil estivesse atrasado na adesão. Ela é um tratado produzido no âmbito do Conselho da Europa,[12] que estabeleceu essa Convenção sobre os cibercrimes aprovada em Budapeste em 2001.

E o Brasil não foi chamado para elaborar a norma, tampouco para ocupar o posto de país observador ao longo desses anos todos. Repito: o Brasil somente veio a ser convidado em dezembro de 2019, e o nosso processo doméstico de aprovação dessa adesão ocorreu de forma açodada, na prática sem nenhum debate, sem nenhuma consideração de mérito por parte do Congresso Nacional. O Projeto de Decreto Legislativo referente à adesão começou a tramitar em junho de 2021 e foi aprovado em dezembro de 2021, tendo sido realizada apenas uma audiência pública. A participação, basicamente, ficou restrita às pessoas que concordaram com a decisão do Brasil, não tendo sido tomadas precauções, cuidados ou medidas para aprofundar o debate. Por exemplo, com relação a quais aspectos da convenção deveriam ser objeto de reserva ou de declarações por parte do Brasil, o que é procedimento absolutamente comum em termos de normas internacionais. É imensa a lista dos países que aderiram à Convenção de Budapeste e que listaram declarações e ressalvas na aplicação, porque é uma norma internacional que tem que ser adequada à métrica de cada país.

A Convenção de Budapeste, em tese, é um caminho adequado para o Brasil lidar com os cibercrimes e a produção de provas digitais, porque se trata de um problema internacional, e não de uma questão que respeite fronteiras nacionais em qualquer uma de suas diversas modalidades. Há necessidade, sim, de diálogo internacional, embora haja ressalvas quanto à adesão a essa norma específica. É um caminho potencialmente frutífero, mas a forma como o Brasil realizou é surreal.

Por previsão expressa da própria Convenção, o Brasil precisa fazer algumas definições no momento da adesão. Por exemplo, que órgão nacional vai compor a rede de 24 horas, sete dias por semana, de interação na troca desses dados que vão ser coletados na cooperação internacional? O Brasil não indicou o órgão. Vai ser a ANPD, vai ser a Polícia Federal, vai ser o Ministério da Justiça, o Gabinete de Defesa Institucional? Nessa linha, não houve definição de vários pontos pelo Congresso Nacional. Há algumas questões do tipo: na adesão, o país tem que escolher se é "a", "b" ou "c", e o Brasil respondeu que "sim". Esse é o posicionamento que a gente tem hoje na nossa adesão específica à Convenção sobre o Cibercrime, que se concluiu com o Decreto nº 11.491, de 13 de abril de 2023.[13]

Nesses três elementos - uma norma internacional, a reforma de um código e a complementação da LGPD - temos hoje um cenário legislativo muito preocupante, em que ao mesmo tempo a gente celebra a vigência da LGPD, o amadurecimento da ANPD, e a elevação da proteção de dados ao grau de garantia constitucional, não temos boas expectativas sobre como isso vai ser detalhado em relação ao combate ao cibercrime no Brasil.

Por fim, expresso um recado em tom de proposta, que é a ideia do constitucionalismo digital. A versão proposta do professor Edoardo Celeste,[14] pesquisador italiano radicado na Irlanda, faz um mapeamento, citado pelo professor Gil-

mar Mendes e Victor Fernandes ao traçarem uma agenda de pesquisa para essas questões avançarem no Brasil.[15] Celeste defende que os desafios propostos pelas mudanças no cenário da Sociedade da Informação, das tecnologias digitais de informação e comunicação, da nova forma como interagimos (dirigindo ou pegando carona num Uber,[16] pedindo a iFood, dormindo com um relógio no pulso, consumindo vídeos sob demanda, produzindo tantos dados pessoais ao carregar um celular no bolso ou usar uma smart TV, um computador, um carro, até Airfryer, etc.) trazem algo distintivo para as questões de afirmação de direitos humanos e para as questões de equilíbrio e harmonização de poder (incluindo não só o poder público, mas também o poder privado das empresas), por exemplo, no tratamento dos dados pessoais de maneira mais ampla, e na assimetria entre os interesses dos indivíduos e da coletividade em relação às pessoas jurídicas.

Então, o Constitucionalismo Digital abarca tanto a harmonização dos poderes, como a reafirmação dos direitos fundamentais, essas duas facetas do direito constitucional, aplicadas a esses novos cenários, ou seja: as garantias de privacidade, de liberdade de expressão, de presunção de inocência, de dignidade da pessoa humana, de valorização social do trabalho, de soberania, de cidadania etc.

Aqui abro um parêntese com a notícia de que o iFood fez um convênio com a Polícia Militar do Estado de São Paulo, para que os dados dos entregadores sejam compartilhados de modo a que sejam liberados de forma mais rápida nas *blitzes*. A Secretaria de Segurança Pública de São Paulo e a Polícia Militar também do Rio de Janeiro fizeram uma parceria para evitar que os empregadores fiquem retidos nas *blitz* organizada pelos órgãos de Segurança Pública.[17] A resposta do iFood foi de que o cadastro de dados que são prestados pelos próprios motociclistas têm a intenção de assegurar mais segurança

aos entregadores. Eu, lendo nas entrelinhas, entendo que é mais segura para os entregadores *contra a polícia*. Para evitar que a polícia agrida um empregado do iFood ou confunda um entregador com alguém que esteja sendo procurado. Então, os dados estão mais rapidamente compartilhados e enfim, o reconhecimento facial e liberação rápida não vão evitar que eles recebam multa, apenas vão ser analisados mais rapidamente, e a polícia vai ter mais acesso aos dados do entregador. Isso não é valorização social do trabalho, fundamento da República previsto no art. 1º da Constituição. Insatisfeito com o presente, temo muito pelo futuro do nosso direito constitucional.

Entendo ser necessário pautarmos esses debates por uma ideologia que afirme o valor da análise dessas questões pelo prisma constitucionalizante das soluções. Uma ideologia de reafirmação dessas bases historicamente envolvidas no direito constitucional do Estado Democrático de Direito em cada uma dessas muitas questões – os desafios trazidos pela tecnologia em todos os âmbitos, no comércio, no direito do consumidor, nas questões tributárias e também nas questões de persecução do cibercrime. Defendo ser necessário reafirmarmos nossos direitos fundamentais, o equilíbrio e a harmonização dos poderes diante desses desafios que vão acontecer cada vez mais rápido tanto no âmbito doméstico quanto internacional.

Espero que todas as pessoas interessadas na articulação entre direitos fundamentais, processo penal e a era digital possam se sensibilizar para essa possível abordagem, que oferece alguma salvaguarda à nossa proteção de dados pessoais no enfrentamento ao cibercrime no Brasil. Este é o "chamado às armas" que eu ouso fazer.

NOTAS

1. 'Este artigo, atualizado em 23 de maio de 2023, deriva da palestra proferida em 23 de agosto de 2022 durante o painel "Proteção de dados e cibercrimes no Brasil", no VI Congresso Direitos Fundamentais e Processo Penal na era digital,

promovido pelo InternetLab com a habitual alta qualidade. Pude participar com imensa satisfação ao lado de tantos nomes conhecidos e relevantes para o tema, com destaque para o professor Zanoide, cujo fala em tom melancólico e pessimista, de que as coisas realmente não estão bem, serve de ponto de partida para minhas reflexões.

2. MORAES, Maurício Zanoide de. Política criminal, constituição e processo penal: razões da caminhada brasileira para a institucionalização do caos. Arquivos do Ministério da Justiça, v. 51, n. 190, p. 175-209, 2006. https://shre.ink/lefX. Acesso em: 07 abr. 2023.

3. BRASIL. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. "Lei Geral de Proteção de Dados Pessoais (LGPD)." (Redação dada pela Lei nº 13.853, de 2019). https://shre.ink/LeiLGPD

4. A LGPD entrou em vigência, mesmo, já em 2018, com as previsões sobre a criação da Autoridade Nacional de Proteção de Dados – ANPD, mas o preenchimento de cargos só ocorreu em 2020. Sobre o tormentoso período de espera pela vigência plena da Lei, uma alegórica descrição detalhada pode ser encontrada em SANTARÉM, Paulo Renã da Silva; SANTOS, Bruna Martins dos. Vigência da LGPD: uma odisseia brasileira. JOTA. 18 set. 2020. https://shre.ink/lefoAcesso em: 07 abr. 2023.

5. BRASIL. Presidência da República. Lei nº 9.296, de 24 de julho de 2016. "Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)". https://shre.ink/9P1f

6. BRASIL. Presidência da República. Lei nº 13.869, de 05 de setembro de 2019. "Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal". https://shre.ink/9P1s

7. Para uma explicação sintética dos fatos e uma análise jurídica, ver CANÁRIO, Pedro; VASCONCELOS, Marcos de. Sergio Moro divulgou grampos ilegais de autoridades com prerrogativa de foro. Conjur, 16 mar. 2016. https://shre.ink/lejz. Acesso em 17 mai. 2016.

8. BRASIL. Presidência da República. Lei nº 12.965, de 23 de abril de 2014. "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". https://shre.ink/lwaR

9. Trata-se de uma nova organização parlamentar, cuja forma e dinâmica são frutos diretos da necessidade de distanciamento social durante a pandemia de COVID-19. O Congresso Nacional se organiza habitualmente a partir de comissões temáticas, mas elas já não estavam funcionando desde março de 2020, com a declaração da Organização Mundial de Saúde sobre a gravidade da pandemia. Então, de modo criativo, formaram-se esses grupos de trabalho para que os projetos pudessem ter encaminhamento. O Projeto de Lei das Fake News, por exemplo, passou por um grupo de trabalho conduzido pelo Deputado Orlando Silva.

10. COUNCIL OF EUROPE. The Budapest Convention (ETS No. 185) and its Protocols. Acesso em: 27 jul. 2023.

11. COUNCIL OF EUROPE. Committee of Ministers. Ministers' Deputies, Decisions, CM/Del/Dec(2019)1363/10.3a, 11 December 2019. 1363rd meeting, 10.3. Convention on Cybercrime (ETS Nº. 185).

12. Trata-se, em síntese, de organização semelhante à União Europeia, mas é uma outra organização que tem a sua dinâmica própria, e que não se confunde com a UE.

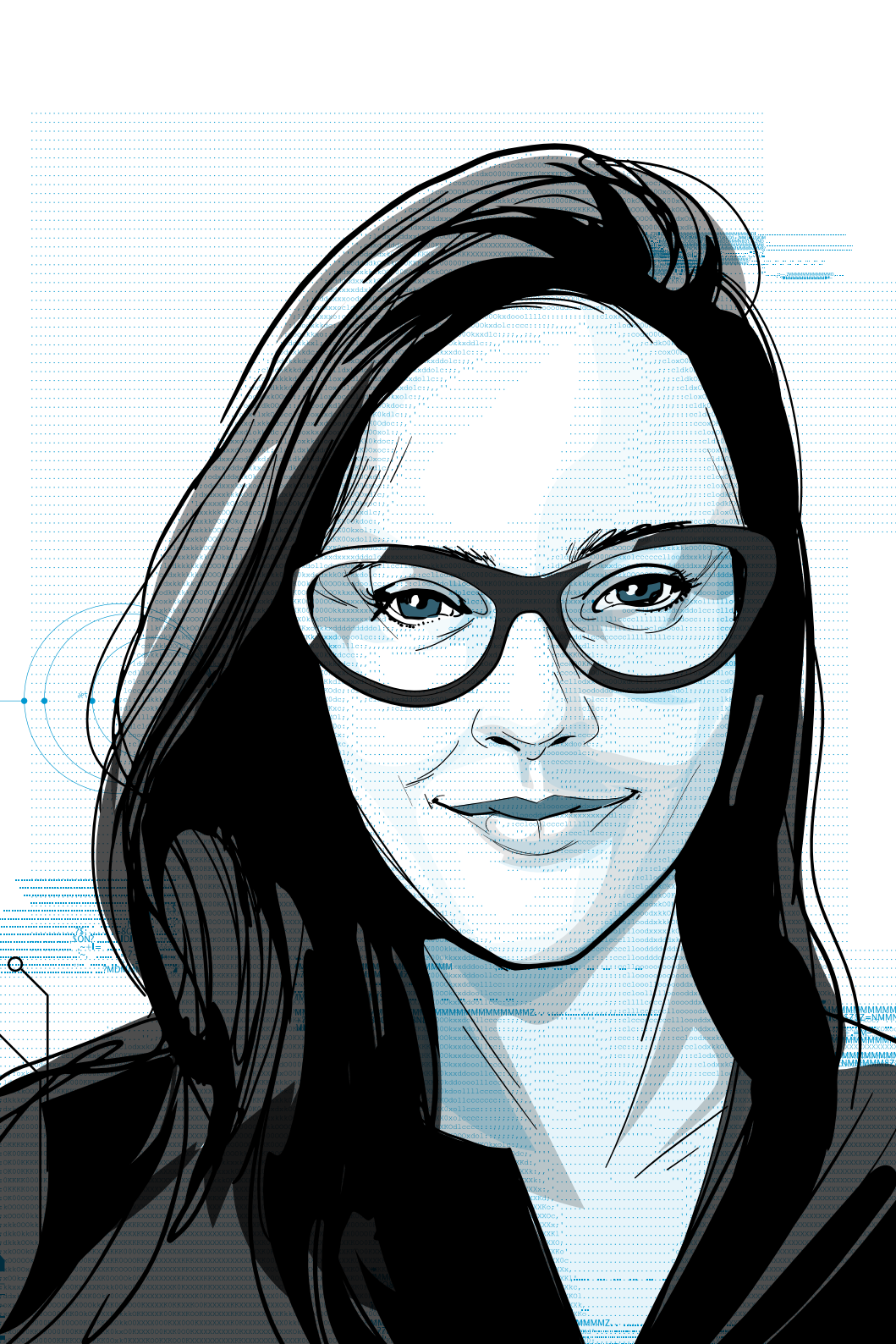
13. BRASIL. Presidência da República. Decreto nº 11.491, de 12 de abril de 2023. "Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001." https://shre.ink/9PzH

14. CELESTE, Edoardo. Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. Tradução de Paulo Renã da Silva Santarém. Revisão de Graziela Azevedo. Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 2021.

15. FERREIRA MENDES, Gilmar; OLIVEIRA FERNANDES, Victor. Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Justiça do Direito, [S. l.], v. 34, n. 2, p. 6-51, 2020. DOI: 10.5335/rjd.v34i2.11038.

16. AMORIM, Henrique; MODA, Felipe Bruner. Trabalho por aplicativo: gerenciamento algorítmico e condições de trabalho dos motoristas da Uber. Fronteiras-estudos midiáticos, v. 22, n. 1, p. 59-71, 2020. https://shre.ink/lejS

17. SARINGER, Giuliana. iFood faz acordo para PM de SP e RJ liberar entregador mais rápido em blitz. Acesso em: 27 jul. 2023.



07.

RANSOMWARE EM CONTEXTO DA PROTEÇÃO DE DADOS: O COMPLIANCE COMO MITIGAÇÃO DE RISCOS[1]

Daniela Eilberg

Em primeiro lugar, gostaria de agradecer o convite em nome da Bárbara Simão, do Francisco e da Dra. Marta Saad. É um prazer para mim poder estar aqui ao lado de grandes profissionais e, principalmente, nessa instituição, InternetLab, que produz tanto conhecimento nessa área, que é realmente muito importante e, inclusive, fonte de muitos dos meus estudos. Cumprimento aos colegas da mesa, Dr. Antônio Gesteira, Dr. Guilherme Caselli, e agradeço à Clarice pelas palavras.

Eu gostaria de trazer algumas questões relacionadas à repaginação de inúmeros desafios, a questão da tecnificação dos velhos e novos desafios. Quero abordar uma série de problemáticas que vêm com a inserção das tecnologias, mas não focar em uma visão pessimista, de que a tecnologia traz meramente problemas, mas uma mudança completa. Sobre também compreendermos que a tecnologia, na verdade, muitas vezes, apenas uma ferramenta de sofisticação de institutos processuais que já estavam lá. Então, é muito importante a gente reconhecer quando que a tecnologia, de fato, está trazendo uma mudança que compreende a alteração escatológica de tempo, uma mudança que nos impõe o passado, presente e futuro juntos. Uma mudança de espaço – isso, de fato, a tecnologia traz. E, portanto, uma mudança paradigmática para o processo penal. Assim, precisamos compreender certas topologias para saber como enfrentar tais alterações, já que de fato as nossas normativas não conseguem dar conta, e como a gente pode então compreender certas ferramentas e instrumentos que vêm sendo utilizados sobre um controle formal e material.

Então, é importante observar tal influência da tecnologia significativamente na produção probatória. Como os colegas de mesa já trouxeram, uma série de questões inerentes à investigação que passam a ser produzidas na fase de investigação e toda essa guinada no campo probatório são fruto da avalanche digital. A tecnologia é de fato imprescindível para a gente

repensar como enfrentar dificuldades e desafios e como tambémém driblar a forma tradicional de enfrentarmos diante da mudança que é, ao mesmo tempo, sistemática, porém refém da permanência normativa.

A possibilidade de utilizar programas maliciosos por infiltração remota desperta inúmeros debates tanto internacionalmente como no Brasil. Os ataques aos governos e empresas do setor privado passaram a ocupar manchetes, capturam a atenção das autoridades policiais e estatais em geral. Então, diante da série de ataques cibernéticos de alto perfil e interrupções, tais ataques são foco da mídia e reformulam o foco de um dos problemas. Os ataques de *ransomware* foram inúmeros e vimos a evolução tecnológica – *malware*, compreendido como *software* malicioso utilizado para infectar sistemas (seja para monitorar, coletar dados, ou ter o controle) - e o *ransomware*, como um *malware* projetado especificamente para tornar todo esse sistema (arquivos e dados) reféns de um pagamento de resgate - por vezes sequer devolvido após o pagamento, como bem mencionou o Dr. Antônio.

Nessa evolução, desde *ransomware* da forma original como surgiu, mas também do *crypto-ransomware* com a possibilidade de criptografar os documentos do usuário e, por fim, o *doxware*, como forma de *crypto-ransomware* muito utilizado contra as vítimas como ameaça de liberar os dados e torná-los públicos se o resgate não for pago.

Por que é importante falar sobre *ransomware* em um contexto de proteção de dados? O porquê da importância de se pensar em compliance e proteção de dados a partir dessa realidade que a gente tem de invasões? *Ransomware* e *compliance* de proteção de dados chamam atenção de ICO (Information Commissioner Office) que, em seu site, apresentam oito cenários sobre os problemas de conformidade de *ransomware* mais comuns, bem como um *checklist* para

auxiliar na prevenção de tais ataques: governança, identificação de ativo, seleção de controle externo, gerenciamento de vulnerabilidades, capacitações, etc.

Dentre os setores de maior foco nessas invasões tivemos a saúde e o Judiciário ocupando altas posições no *podium*, mas todas as empresas que processam dados estão sujeitas a esse tipo de risco. Portanto, é necessário que se tomem algumas medidas. Como bem trouxeram nas fala da mesa, medidas com relação a todo um preparo, conscientização das pessoas, dos funcionários, que são imprescindíveis para que se faça toda uma política de segurança digital e que se consiga concretizar. Não basta apenas as ferramentas e tudo que se disponibiliza tecnologicamente, mas também é necessário esse preparo dos funcionários.

À medida em que os atores desses ataques cibernéticos, já tipificados como crimes em certos locais, passam a explorar os dados capturados, os riscos aumentam. A potencial perda permanente dos dados pessoais e a perda de controle sobre esses dados devem ser consideradas, assim como a fraude financeira.

Por isso, metodologias são utilizadas para que se possa fazer um programa de prevenção a ataques de *ransomware* e o *National Institute of Standards and Technology* traz cinco etapas para que a gente possa pensar essa proteção: (i) identificar; (ii) proteger; (iii) detectar (iv); responder e (v) recuperar.

Portanto, é interessante pensar também em algumas informações que são trazidas com relação à sofisticação desta invasão, a violação desses dados relacionada ao pagamento do *ransom*. E como a higiene básica da conta e dos dados tem um papel imprescindível para que se possa pensar em como protegê-los. Revisões regulares das permissões, avaliação dos riscos de participação que precisam ser levadas em conta porque nos últimos anos, esses incidentes cibernéticos têm trazido problemáticas para os dados, reconfigurando todo um cenário de disponibilização de dados.

Como resultado, é necessário ter uma relação que hoje em dia é imprescindível. A gente percebe o quanto ela está intrínseca a toda essa lógica de vigilância massiva, que é o setor público-privado trocando muitos dados. Então, como esses ataques de *ransomware* podem trazer uma informações que podem, posteriormente, ser compartilhadas, transmitidas para empresas privadas ou autoridades estatais e como os dados são coletados a partir desses ataques.

No segundo trimestre de 2022, foi um recorde de ciberataques, aumentou 32% em relação a 2021 e a gente tem a pesquisa, a educação e a saúde como principais focos desses ataques. A gente tem a África com um volume de ataques enorme, depois a Ásia, também é outro local em que cresceu muito esses ataques de *ransomware* e, principalmente, o uso da *darkweb* em uma série de crimes cibernéticos e os outros tipos de crime que passam a ter relação com a lavagem.

Com relação ao setor da saúde, houve um crescimento de 60% significativo também que a gente presenciou, inclusive aqui no Brasil, a partir da coleta de dados dos órgãos relacionados à saúde, mas afetando também outros setores.

O que o Dr. Antônio trouxe com relação ao pagamento ou não do resgate foi uma discussão que inclusive foi foco do *FBI*, que se pronunciou quanto a isso. Um ponto discutido foi a questão da criminalização desse pagamento quando se trata de um pagamento de resgate por exemplo, para uma célula terrorista que teria feito um ataque de *ransomware*. Houve todo um debate sobre criminalizar ou não a pessoa pagar resgate para essa organização terrorista, então o *FBI* se pronunciou com relação justamente a como os resgates são pagos tradicionalmente e não se condena a pessoa por pagar para obter algo que era seu por direito.

Um outro questionamento diz respeito ao compartilhamento público-privado e de como os ataques de *ransom* po-

dem ser analisados a partir da narrativa de vigilância, ou do denominado complexo industrial de vigilância e da ameaça que se tem de crescimento de uma vigilância massiva que, por exemplo, os tribunais vêm encarando a respeito. Como o Tribunal Europeu de Direitos Humanos vem se posicionando, como o Tribunal de Justiça da União Europeia vem decidindo.

A abordagem tradicional de segurança *versus* privacidade fundada na ideia de "moeda de troca" acaba por estar desatualizada, porque simplifica questões da vigilância em si. A relação do público-privado é vez que o mercado explora os ganhos comerciais a partir dos dados. Ontem mesmo, o Dr. Maurício Zanoide falou sobre a questão do capitalismo de vigilância. Mencionou como a espionagem comercial vem trazendo uma necessidade de compreender como as empresas privadas, que fazem um monitoramento consistente, muitas vezes focam nesse lucro e, por vezes, transmitem dados coletados de certas formas e corroboram com vigilâncias estatais. Então, a indústria de vigilância global, que também foi o foco da palestra de ontem, levanta um questionamento – verbalizada em uma das perguntas de ontem: como e por que as pessoas passam a voluntariamente ceder os seus dados e se expor? Há toda uma disposição massiva que muitas vezes é fornecida voluntariamente com relação à privacidade, sem consciência total.

Eliza Watt sugere que, em vez de um *trade-off* de segurança e privacidade, possamos redefinir os termos de análise de custo benefício. Existe toda uma estimativa do custo real da privacidade dos direitos humanos que está associada à vigilância em massa, e a gente tem a necessidade de reconhecer esses ganhos comerciais que são resultantes dos governos e do setor privado.

Por exemplo, a jurisprudência do Tribunal Europeu de Direitos Humanos sobre vigilância em massa, após as divulgações do Snowden, aumentou. A narrativa do Tribunal passa a tratar de de privacidade *versus* segurança. A gente vê isso no

/ A ABORDAGEM TRADICIONAL DE SEGURANÇA VERSUS PRIVACIDADE FUNDADA NA IDEIA DE "MOEDA DE TROCA" ACABA POR ESTAR DESATUALIZADA /

caso *Roman Zakharov vs. Rússia, Centrum for Rattvisa vs. Suécia, Big Brother Watch vs. Reino Unido*. São importantes casos jurisprudenciais que o Tribunal Europeu de Direitos Humanos ajusta os princípios, acaba relativizando, na verdade, certos princípios em que se baseava anteriormente e traz mudanças significativas em seus entendimentos. Por um lado, o Tribunal Europeu de Direitos Humanos traz a compreensão da possibilidade do *status* de vítima, a aceitação de uma abordagem de uma queixa individual com a compreensão de que não é necessariamente preciso comprovar todos os critérios que precisava se comprovar anteriormente, porque atualmente estamos sob ameaças de vigilâncias estatais massivas e, portanto, possibilitou que essa demanda individual fosse trazida com essa aceitação de uma vigilância em massa.

Só que, em contrapartida, apesar desse direito de apresentar reclamação perante o Tribunal Europeu de Direitos Humanos tenha, digamos assim, aumentado, também mudou a compreensão relacionada à ponderação. Então, o Tribunal Europeu de Direitos Humanos com relação à interceptação, apesar de reconhecer explicitamente essa vigilância em massa estatal, considera ser o compartilhamento de dados sem haver qualquer incompataibilidade com o que está na Convenção da Europa de Direitos Humanos, principalmente em relação à luta contra o terrorismo.

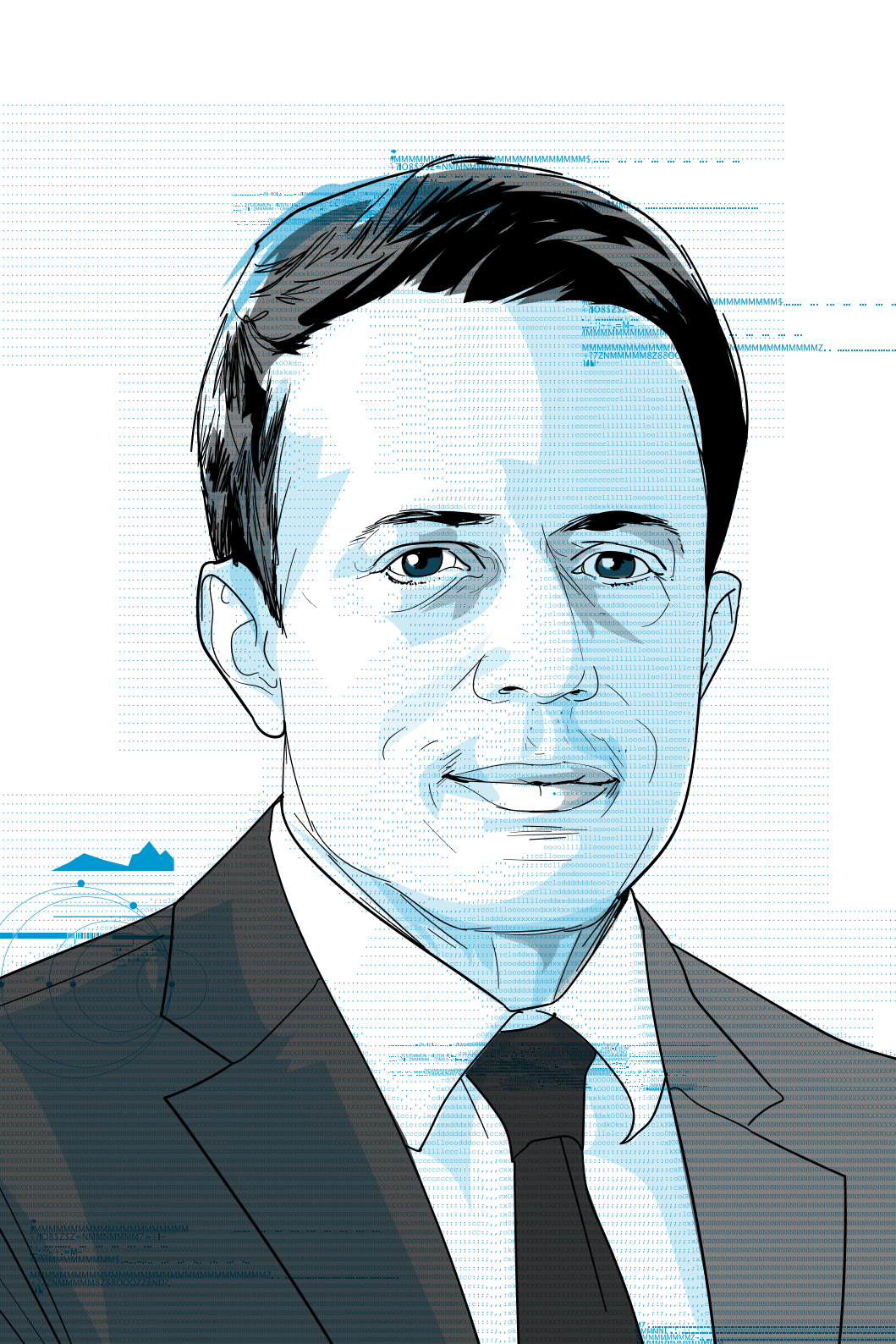
Só para trazer um pouco mais do que se tem em termos de casos jurisprudenciais, sugiro a leitura do *Big Brother Watch and Others vs. Reino Unido*, Romans Zakharov vs Russia, do caso da Suécia, *Centrum for Rattvisa*, sugiro também *Weber e Saraiva* vs. Alemanha e *Liberty vs. Reino Unido*, em que o Tribunal Europeu de Direitos Humanos reconhece expressamente que as autoridades nacionais gozariam desta ampla margem de apreciação para se proteger a segurança nacional em prol da luta contra o terrorismo.

Mas, enfim, *ransomware* é um debate bastante em voga. Ainda tem muita coisa para acontecer nessa seara. Muitas das leis do cibercrime e de segurança cibernética passam a abordar tópicos relacionados. Então, acho que eu recomendaria, para finalizar a minha fala, o relatório do *Congressional Research Service* que foi publicado explorando algumas abordagens potenciais para se combater o *ransomware*. Eles trazem algumas das percepções nos Estados Unidos das leis que se tem, a lei de fraude e abuso de computadores, a lei de espionagem. Então, é bem interessante para se pensar a questão da extorsão e como isso vai refletir nas próprias vítimas que realizam o pagamento.

E, por fim, a questão da preocupação do modelo de *ransomware as a service*, como foi também abordado aqui na palestra, por conta justamente de como isso passou a fazer parte do mercado e vender ou alugar estas ferramentas passa a trazer uma série de lucros. E, portanto, a gente vê como as criptomoedas acabam assumindo um papel essencial quando a gente pensa na prevenção à lavagem de cripto ativos. Tem uma série de documentos internacionais, relatórios informativos como o da *Interpol* com a ASEAN trazendo o aumento significativo de ataques de *ransomware* em todo o mundo e o que se vem adotando de política, etc. Enfim, devemos constantemente nos informar. Agradeço a oportunidade do espaço de fala e fico à disposição para eventuais perguntas e debates.

NOTAS

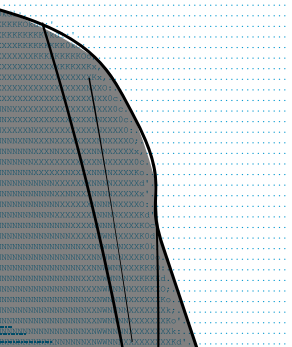
1. Este artigo foi adaptado a partir de palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022.



08.

LAVAGEM DE DINHEIRO E CRIPTOATIVOS[1]

Alexandre Senra



Bom dia a todos! É um prazer estar aqui com vocês.

Eu queria começar perguntando a quem está presente aqui: quantos de vocês já compraram criptomoedas? Levantem a mão. [Presentes levantam as mãos] Quantos de vocês já usaram a MetaMask? Quantos de vocês já compraram NFTs? E quantos já interagiram com protocolos de finanças descentralizadas?

Bom, para quem não está aqui e não conseguiu ver a resposta da plateia, a gente teve mais ou menos seis pessoas que já compraram criptomoedas, uma ou duas pessoas que já usaram a MetaMask e nenhuma que já comprou NFT ou interagiu com protocolos de finanças descentralizado. O que isso significa? Isso significa que a gente tem que começar do zero. É incontornável esse nosso obstáculo. A gente tem que começar do início, e a gente está em uma mesa aqui que é a primeira mesa a tratar da temática criptoativos neste seminário. Então, não tem como ser diferente.

Eu vou falar sobre criptoativos e *blockchain*, para que depois a gente possa chegar nas discussões. Vamos fazer uma abordagem descritiva. Posso falar eventualmente do que já fizeram ou do que, em tese, pode ser feito, mas nada disso deve ser encarado como instrução sobre como lavar dinheiro! [risadas entre os presentes].

Bom, o que são criptoativos? Vou dar um exemplo para vocês: hoje, eu mandei a apresentação para a Laura, do Internetlab, que está organizando o Congresso, por WhatsApp. Mandei em PDF para ela. E, vejam, eu posso falar que eu enviei a minha apresentação em PDF para Laura e agora a apresentação vai ser exibida. Mas será que, de fato, sob aspecto técnico, foi isso que aconteceu? Não foi. No momento em que eu enviei o meu PDF para ela, eu passei a ter um PDF no meu celular, e ela passou a ter outro PDF no celular dela. No momento em que ela pegou esse mesmo PDF e disponibilizou para ser exibido aqui a vocês, a gente passou a ter mais um PDF. Guardem este primeiro exemplo.

Segundo exemplo: na minha adolescência, (isso aí na década de 90, tudo prescrito já...) como eu sou do Rio de Janeiro... O que a gente fazia? A gente ia no Centro do Rio de Janeiro, na Uruguaiana – que é equivalente à Rua 25 de março em São Paulo –, comprar programas de computador e joguinhos de computador piratas. Por que fazíamos isso? Primeiro, porque não tínhamos dinheiro para comprar o original, né? Era todo mundo ferrado... E segundo, e mais importante, porque era possível, tecnicamente, fazer cópias de joguinhos e de programas de computador.

Vejam, o que esses dois exemplos têm em comum? Eles evidenciam um problema que sempre existiu relacionado aos bens digitais. Que é: bens digitais podem ser copiados. E criptoativos, não. Criptoativos são bens digitais, são ativos digitais e escassos. Entendam como "escassez" a impossibilidade de que esse bem, esse ativo, seja copiado. Vamos ver ainda como é que isso foi possível. Mas, por ora, eu preciso que vocês entendam que, em contraposição ao PDF, em contraposição aos joguinhos e aos programas de computadores, criptoativos não podem ser copiados e, nesse sentido, são escassos.

Segunda afirmação: criptoativos são o designativo de um gênero.

Podem dizer: "Poxa Senra, se você está numa mesa sobre lavagem de dinheiro e criptomoedas, por que você deu o nome da apresentação de 'lavagem de dinheiro e criptoativos'?"

Porque criptoativo é o gênero, criptomoeda é a espécie. Esse gênero pode ser classificado e ele pode ser "cortado" de variadas formas. Por ora, o que interessa a gente saber é que todos os ativos digitais escassos vão estar dentro desse conceito. Criptomoedas estão dentro do gênero criptoativos. NFTs estão dentro do gênero criptoativos. *Tokens* de finanças descentralizadas também. Então, nossa temática aqui é o gênero de criptoativos.

O que é *blockchain*? Eu não havia revelado, ainda, como foi possível criar essa escassez digital. É através da *blockchain*. A *blockchain* é uma tecnologia de registro distribuído.

Pensem num registro como um livro, um livro onde são anotadas transações: tudo que é feito, tudo que é enviado e recebido de uma conta para outra. Isso aqui [apontando para um livro] é um registro. Tudo bem, mas o que isso tem a ver com *blockchain*? A *blockchain* é um registro com algumas particularidades. Duas delas vão nos interessar.

A primeira delas: ele é um registro distribuído. Se fosse um registro centralizado, como, por exemplo, o banco de dados da Caixa Econômica Federal, seria possível tirá-lo do ar.

Isso foi feito há alguns meses com o Telegram.[2] Por que foi possível o STF nos privar, durante algumas horas, pelo menos, do Telegram? Porque ele funciona com base em uma estrutura centralizada. Se você cortar o serviço que está sendo fornecido pelo provedor, todo mundo fica sem serviço.

Já com a tecnologia *blockchain* não é assim, porque esse registro na *blockchain* está distribuído. Ele existe em várias vias ao redor do mundo. Importante: notem que eu não falei que existem várias *cópias* ao redor do mundo. Ele existe em várias *vias*, que estão permanentemente sincronizadas entre si. Então, se você tirar algumas dessas vias do ar, o que acontece com a rede? Nada. As outras vias continuam funcionando e processando as transações. Isso é a *blockchain*. Ela não é a única tecnologia de rede distribuída, mas é a principal e é dela que a gente vai tratar hoje.

Segunda afirmação relativa ao *blockchain*: é o nome dado ao próprio registro distribuído.

Eu não sou uma pessoa de preciosismos, tá? Não tenho problema com os usos "a *blockchain*" ou "o *blockchain*". Eu preferia que fosse em inglês ("*the blockchain*") e aí não teríamos essa discussão. Mas, em português, vou explicar por que, por vezes, eu falarei "a *blockchain*" e, por vezes, eu vou falar "o *blockchain*".

Sempre que não há uma tradução do termo, eu faço uso daquela concordância mental, da silepse. Então, se estiver fazendo referência à tecnologia, eu vou falar "a *blockchain*". Se eu estiver fazendo referência ao nome do próprio registro, eu vou falar "o *blockchain*". Por exemplo, existe um registro distribuído que é o da rede *Bitcoin*: então, eu vou falar "o *blockchain* do *Bitcoin*". Agora, se eu quiser fazer referência à tecnologia, eu vou falar "a tecnologia *blockchain*" ou somente "a *blockchain*".

"QUEM TEM CRIPTOATIVOS EM *EXCHANGES* NÃO TEM CRIPTOATIVOS"

Então, vamos lá. Alguns de vocês têm conta em *exchange* nacional? *Exchanges* são corretoras de criptoativos, mas não são criptoativos que vocês compram lá. São saldos em criptoativos. Quando eu falo isso, talvez venha à mente uma frase que é muito conhecida nesse mercado, que é "*not your keys, not your coins*". Se as chaves não estão com você, as moedas não são suas.

Cuidado com essa frase. Não é que ela seja mentirosa, mas o problema é muito mais sério do que esse. E as pessoas descobrem que o problema é mais sério do que esse nos piores momentos. Explico: a pessoa pensa "se eu tenho esse saldo lá na Binance, as moedas não são minhas porque a chave está com a Binance. Mas se um dia der algum problema com a Binance, basta que eu entre na Justiça...".

Ou vamos falar de uma nacional – do Mercado *Bitcoin*, por ser a maior, ou de qualquer outra *exchange* nacional. A pessoa pensa "se ela funciona no Brasil, basta que eu entre na Justiça e obtenha uma ordem judicial de bloqueio que vai estar tudo bem". Não, não vai estar tudo bem. Porque se os criptoativos são ativos digitais cuja escassez é controlada pelo *blockchain*, por esse livro-razão distribuído, os saldos não são!

O que vocês têm dentro de uma corretora de criptoativos é um lançamento no banco de dados privado dessa corretora. Não me assustaria que a gente pegasse uma corretora qualquer, somasse o saldo de todos os clientes e chegasse à conclusão que o somatório desses saldos é muito superior do que o número de criptoativos efetivamente custodiados pelo *exchange*. Por quê? Porque hoje não há uma exigência legal no Brasil de comprovação de saúde financeira. As *exchanges* não estão obrigadas a comprovarem que de fato elas têm a custódia de criptoativos correspondente ao somatório do saldo de seus clientes.

Por que isso acontece no pior momento? Porque quando a *exchange* quebra, vem aquele monte de demanda judicial e a *exchange* diz: "Então, na verdade, a gente estava operando aqui no mercado de risco... E eu preciso contar uma coisa para vocês: a gente não tem essa custódia toda". E aí começam aquelas histórias... "Ah! Fomos recentemente *hackeados*" ou "ah, o CEO morreu e só ele que tinha a chave privada e levou para o túmulo". Então, cuidado com isso. Saibam diferenciar criptoativos, que são lançamentos neste livro [aponta para o livro usado como exemplo] aqui distribuído em várias vias ao redor do mundo, de um saldo em criptoativos que é o lançamento em um registro privado da *exchange* centralizada.

"Isso daí não é igual ao seu saldo na conta da Caixa Econômica, por exemplo?" Não. Também é um saldo, mas a Caixa Econômica faz parte de um sistema bancário que é fortemente regulado no Brasil. A *exchange* faz parte do setor que é pouquíssimo regulado. Então cuidado, porque os riscos são totalmente diferentes.

/ A *EXCHANGE* FAZ PARTE DO SETOR QUE É POUQUÍSSIMO REGULADO. ENTÃO CUIDADO, PORQUE OS RISCOS SÃO TOTALMENTE DIFERENTES /

/ O PRINCIPAL DESAFIO DO COMBATE À LAVAGEM DE DINHEIRO COM CRIPTOATIVOS [...] NÃO É DE INOVAÇÃO E SIM DE CONHECIMENTO TÉCNICO /

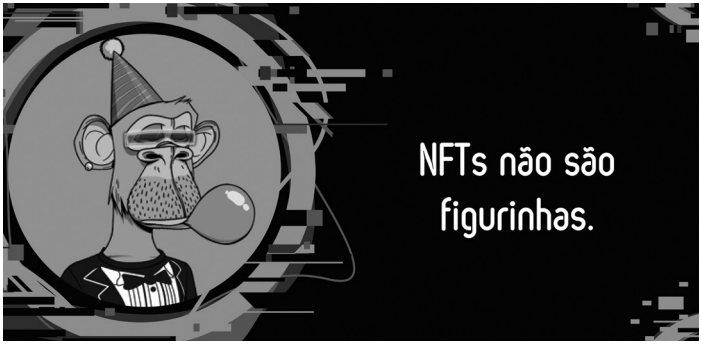
CARTEIRAS DE CRIPTOATIVOS NÃO ARMAZENAM CRIPTOATIVOS

Eu trouxe aqui duas carteiras: uma carteira de dinheiro e uma carteira de criptoativos. Minha carteira de dinheiro tem 100 reais. O que aconteceu perder essa carteira com 100 reais? Eu perco 100 reais.

O que acontece se eu perder essa carteira de criptoativos que, digamos assim, permite que eu acesse um valor muito superior a 100 reais? O que acontece com os criptoativos que podem ser acessados nas carteiras? Nada, não acontece nada, porque os criptoativos não estão aqui dentro. Carteiras de criptoativos armazenam chaves privadas; o que está armazenado aqui é um código que permite que os criptoativos sejam movimentados de um endereço público do *blockchain* para outro endereço público. Então é isso o que a carteira armazena.

Por que é importante vocês saberem disso? Por conta disso: "Ah, na operação judicial, apreendemos uma *hardware wallet*, uma carteira física do alvo. É só colocar no cofre da Justiça Federal que está tudo certo". Não, está tudo errado. Você estará armazenando no cofre chaves privadas às quais outras pessoas podem ter acesso. Afinal, a chave privada é um código. Você não tem como garantir que outras pessoas não têm, por exemplo, um *backup* desse código (escrito por extenso) e os criptoativos, que estão no livro público distribuído, continuam podendo ser movimentados.

NFTS NÃO SÃO FIGURINHAS



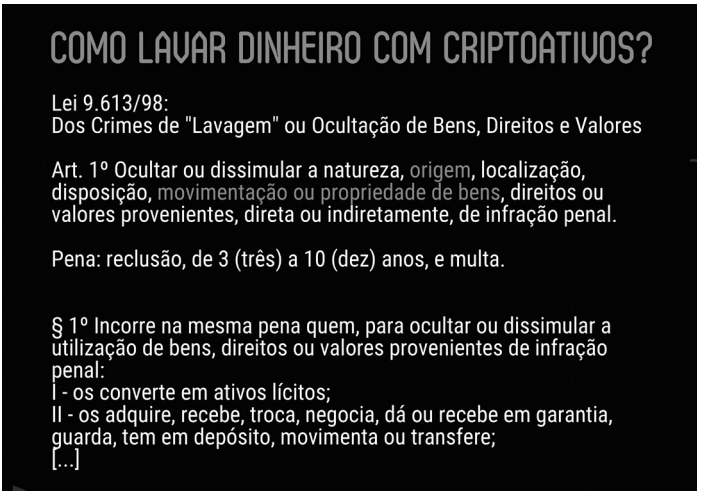
SCREENSHOT DA APRESENTAÇÃO

Essa imagem ficou conhecida como o macaco comprado pelo Neymar por milhões. Quando, no início de 2022, ele comprou o NFT atrelado a essa imagem (BAYC#6633), pertencente à Coleção Bored Ape Yatch Club, começaram piadinhas no Twitter dele. Ele escreveu um tweet: "*I am an ape*!". Aí o pessoal começou a comentar em baixo: "ai, eu também tenho!", começaram a "printar" a imagem do macaco (ctrlC+ctrlV) e postar: "Eu também tenho e você foi o otário que pagou mais de um milhão. Eu não paguei nada. Também tenho..." Isso é uma brincadeira, mas revela também uma profunda ignorância das pessoas sobre o que é um NFT.

Vejam o que aconteceu na sequência desse fato em específico. A empresa por trás da Coleção entregou tokens fungíveis, uma espécie dentro do gênero criptoativo, a quem tinha o NFT. Na sequência, foi lançado um metaverso desse mesmo projeto, o *Otherside*. Quem tinha o NFT recebeu pedaços desse metaverso. Adivinhem o que foi recebido por quem tinha só a imagem "printada": nada.

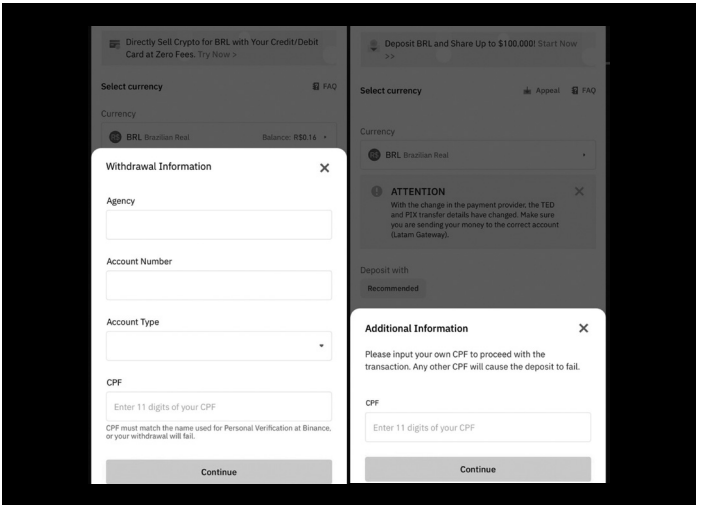
Então, essa história de que "mas Neymar tem o direito de exploração comercial da imagem"... Vocês acham que o Neymar ou qualquer outra pessoa que pague mais de um milhão em um NFT vai ter tempo de ficar processando quem imprimiu a imagem na camisa e está usando? É lógico que não. A conversa aqui é outra. NFTs não são figurinhas. O que são então, afinal, os NFTs? São registros únicos no *blockchain*.

Lembram que eu falei do registro público e distribuído? Eu dei aqueles dois exemplos iniciais de que a novidade do *blockchain* inaugurada através do *bitcoin* foi a criação e controle de uma escassez digital, de se ter a garantia que aquele ativo digital não pode ser copiado. Pois é, o NFT – além de ser um ativo digital escasso, porque faz parte do gênero dos criptoativos – tem uma característica que o particulariza. Ele é não-fungível, único, um *token* numerado. Isso é algo muito simples, mas que permite várias coisas.



SCREENSHOT DA APRESENTAÇÃO

Como lavar dinheiro com criptoativos? Eu trouxe o artigo 1º da nossa Lei de Lavagem e vou abordar alguns exemplos do que pode ser feito, do que já foi feito e de uma iniciativa exitosa para coibir a lavagem de dinheiro com criptoativos.



SCREENSHOT DA APRESENTAÇÃO

Esses são os *prints* que eu dei da minha conta da Binance, hoje pela manhã. O primeiro *print*, tentando sacar reais, e o segundo, tentando depositar reais, moeda fiduciária. O que eu quero mostrar para vocês? Uma estratégia muito bem-sucedida ao longo do tempo para reduzir os casos de lavagem de dinheiro com criptos foram "políticas antilavagem de dinheiro" (AML) e de "conheça o seu cliente" (KYC), implementadas e impostas às *exchanges* centralizadas. Por quê? Porque você estrangula as pontas.

Hoje, como funciona no Brasil? Só é possível fazer depósitos ou saques em reais se isso estiver sendo feito pela conta do titular. Só será creditado o seu saldo em criptoativos se a transferência ou o pix for feito a partir de uma conta titularizada por você. Para saque, é a mesma coisa, você fecha as pontas dessa maneira.

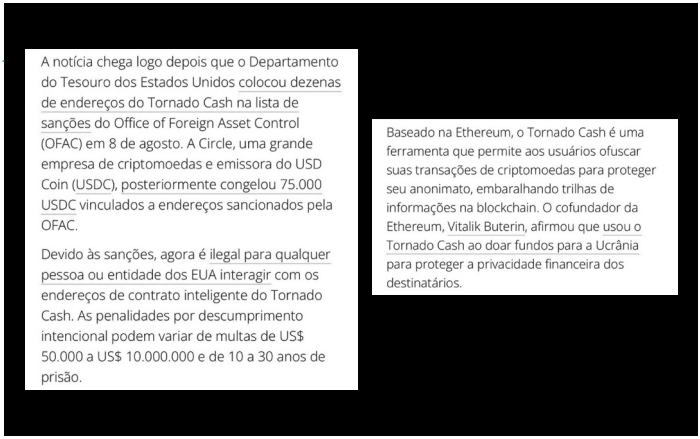
Mais do que isso: você quer abrir uma conta na *exchange*? Eles vão pedir cópia de seu passaporte ou de um documento de identidade.

"Ah, mas o documento pode vazar e outra pessoa pode abrir a conta com o meu documento". Qual foi o passo seguinte que deram? Não basta mandar fotos do documento: "Mande fotos dos documentos com você sorrindo em um papel anotado a data e essa frase aqui". Várias estratégias foram sendo adotadas para que se dificultasse a abertura e manutenção de contas em *exchanges* em nome de terceiros. Esse era um problema muito sério: a pessoa manter contas em nome de terceiros. Esse foi um longo caminho trilhado.

Qual é o problema que subsiste? Isso tudo é válido para as movimentações de moeda fiduciária. Quando você está movimentando criptoativos ou saldos não existe, ainda, uma imposição a que a *exchange* pergunte a quem pertence o endereço de destino.

Os *blockchains* em geral são públicos, mas são pseudônimos. As informações não são propriamente anônimas, mas são protegidas por pseudônimos. Você consegue identificar tudo o que aconteceu dentro dele, mas não quem está por trás das contas ali identificadas de modo alfanumérico.

SCREENSHOT DA APRESENTAÇÃO



SCREENSHOT DA APRESENTAÇÃO

A notícia chega logo depois que o Departamento do Tesouro dos Estados Unidos colocou dezenas de endereços do Tornado Cash na lista de sanções do Office of Foreign Asset Control (OFAC) em 8 de agosto.

A Circle, uma grande empresa de criptomoedas e emissora do USD Coin, posteriormente congelou 75.000 USDC vinculados a endereços sancionados pela OFAC.

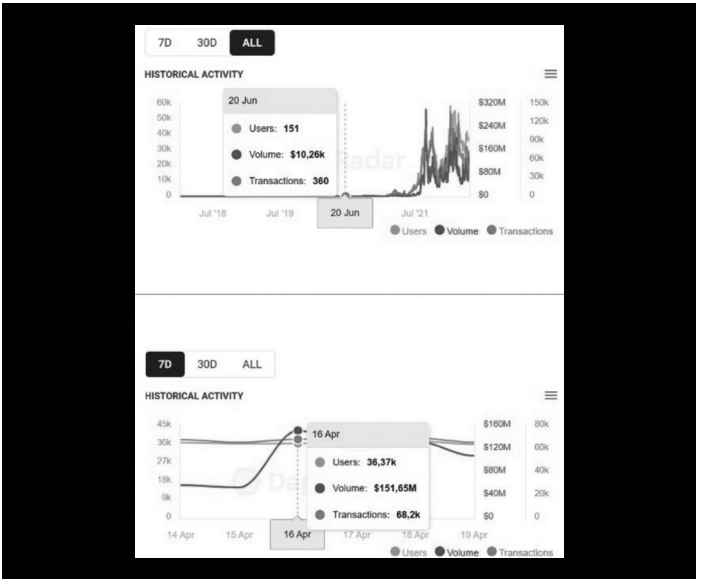
Devido às sanções, agora é ilegal para qualquer pessoa ou entidade dos EUA interagir com os endereços de contrato inteligente do Tornado Cash. As penalidades por descumprimento intencional podem variar de multas de US$ 50.000 a US$ 10.000.000 e de 10 a 30 anos de prisão.

Baseado na Ethereum, o Tornado Cash é uma ferramenta que permite aos usuários ofuscar suas transações de criptomoedas para proteger seu anonimato, embaralhando trilhas de informações na blockchain. O cofundador da Ethereum, Vitalik Buterin, afirmou que usou o Tornado Cash ao doar fundos para a Ucrânia para proteger a privacidade financeira dos destinatários.

Autoridades holandesas prendem o suposto desenvolvedor do Tornado Cash. Tornado Cash é uma aplicação. Pensem nele como o aplicativo, instalado em um *blockchain*, que mistura transações.

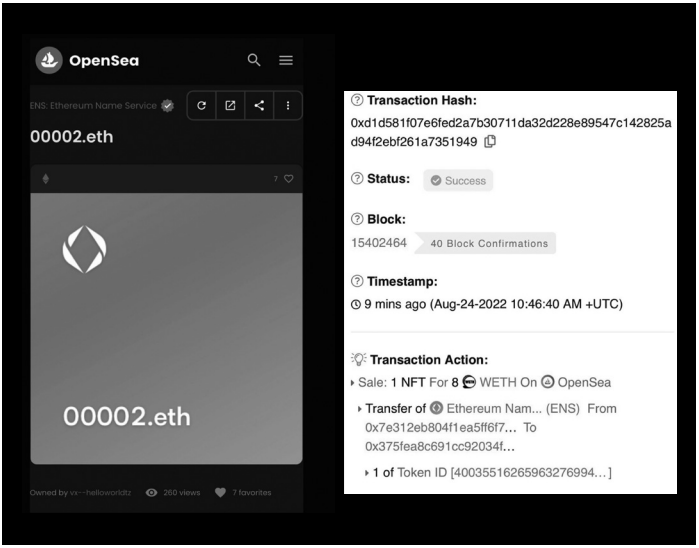
Por que eu trouxe a notícia de prisão do desenvolvedor do Tornado Cash? Porque ela é bastante ilustrativa da dificuldade que se tem de lidar com isso. Prenderam o desenvolvedor não à toa, é porque simplesmente não tinham outra pessoa para prender nessa história toda.

Um último exemplo. Lavagem de dinheiro com NFTs. São tokens não fungíveis, como aquele de Neymar. Qual é o problema nisso? São ativos, em geral, de menor liquidez, porque são únicos. Como você estima o preço de mercado de um ativo de baixa liquidez?



SCREENSHOT DA APRESENTAÇÃO

Na imagem acima vocês vão ver o volume de movimentação do OpenSea, maior galeria de NFTs em funcionamento. No dia 20 de junho de 2020 o volume diário era da ordem de 10 mil dólares. Em abril de 2022 o volume diário estava na ordem de 150 milhões de dólares em transações com NFT.



SCREENSHOT DA APRESENTAÇÃO

Nesta imagem, vê-se que uma transação aconteceu hoje de manhã, quando eu estava chegando no aeroporto. Vamos ver se tem alguma coisa interessante aqui. O domínio "00002.eth" foi vendido 8 ETH. Uns 13 mil dólares. Alguém pagou 13 mil dólares para poder chamar uma carteira de "00002.eth". Qual é o sentido disso? A meu ver, nenhum. Como que você faz para saber se não é a própria pessoa com duas carteiras diversas comprando dela mesma para esquentar o patrimônio? Não dá para saber através do *blockchain*, porque o *blockchain* é pseudônimo.

Então, cuidado com isso. "Ai, não! É porque tem um domínio que é Nike.eth". Tudo bem, a Nike talvez veja muito valor nisso. Mas qualquer outra pessoa que compra esse domínio vai ver valor? Vai ter razão pagar 50, 100 mil dólares pelo domínio "Nike.eth" se você não é a Nike? Então, cuidado com isso. Os NFTs são instrumentos que permitem muitas formas de lavagem de dinheiro. E a estratégia mais simples é essa: a pessoa cria e vende NFTs para ela mesma.

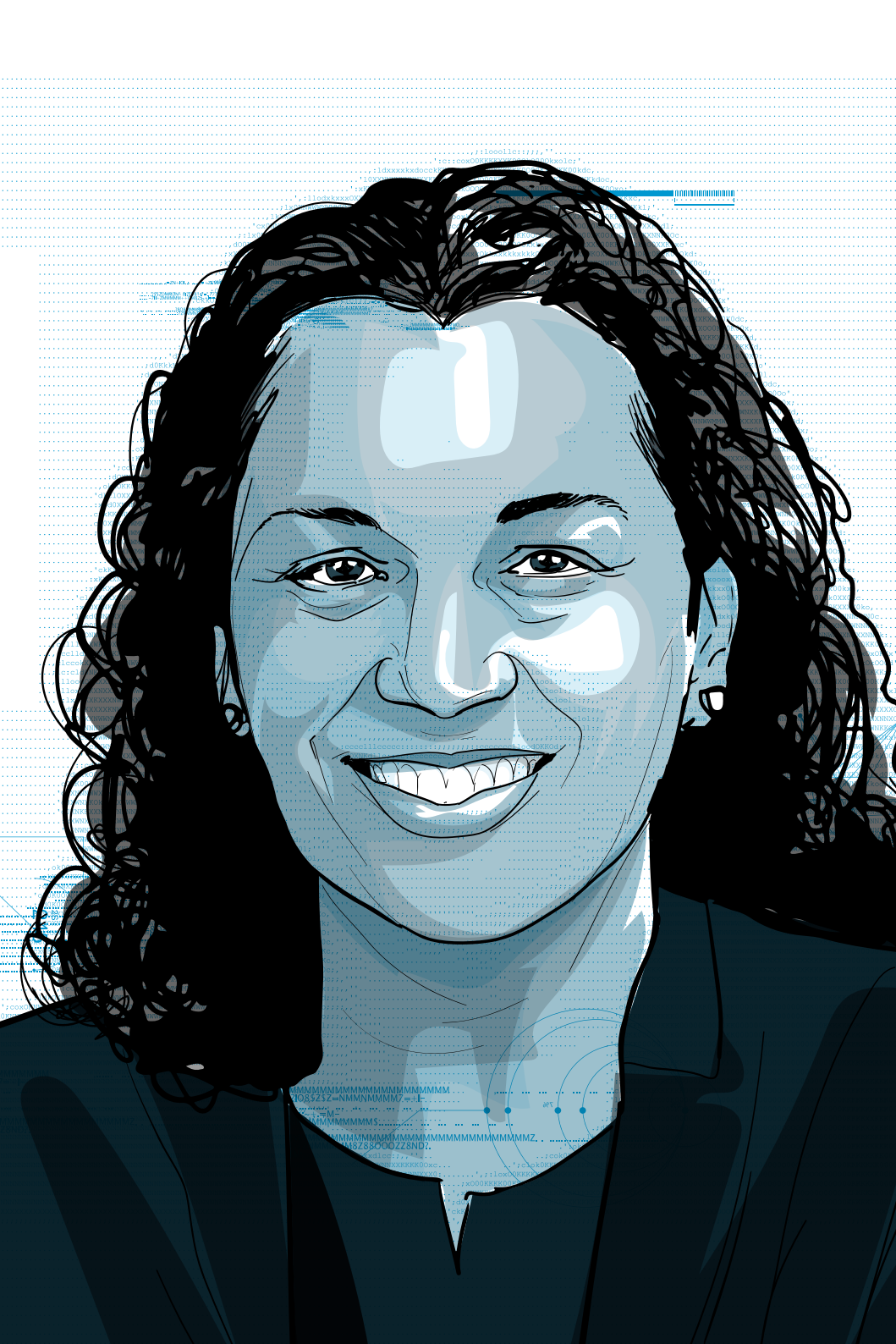
Concluindo, o principal desafio do combate à lavagem de dinheiro com criptoativos, no meu modo de ver as coisas, é o desconhecimento técnico. Não tem como lidarmos com isso se ignorarmos aspectos técnicos fundamentais dessa nova tecnologia.

Obrigado a todos que me acompanharam. 

NOTAS

1. Este artigo foi adaptado a partir de palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022.

2. N/E: Ver: https://shre.ink/l.



09.

REGULAÇÃO DO MERCADO DE CRIPTOMOEDAS[1]

Evelyn Sheehan

Agradeço ao InternetLab pelo convite para estar aqui. É um prazer estar aqui com vocês.

Estou aqui para falar hoje sobre a evolução do cenário jurídico no espaço das criptomoedas sob a perspectiva dos Estados Unidos.

Como vocês ouviram, meu nome é Evelyn. Atualmente sou sócia da Kobre & Kim, em Miami, um escritório de advocacia internacional dos Estados Unidos. Mas antes disso, fui procuradora federal por 10 anos. E a razão pela qual destaco esse ponto novamente é porque, ao longo da minha carreira, vi essa questão de muitas perspectivas diferentes, certo? Durante os dez anos em que estive no Departamento de Justiça (DOJ),[2] vi como era importante aplicar de forma justa as leis criminais e de confisco que estão nos livros, e agora, na prática privada, percebi a importância do tema principal que vou discutir com vocês hoje: o tema do equilíbrio e da clareza.

Agora estou do lado da defesa, mas também represento vítimas de crimes e também represento administradores de *exchanges* (câmbios) de criptomoedas insolventes. Portanto, realmente vi muitos pontos de vista diferentes e muitos desafios diferentes que cada um desses grupos enfrenta.

Como mencionei hoje, quero realmente focar nesse tema do equilíbrio. Equilibrar a necessidade de permitir espaço para a inovação no espaço das criptomoedas com a necessidade de aumentar a regulamentação tem sido um assunto muito discutido em muitos países da América Latina.

Especificamente, vimos diversos atores soberanos caminhando para extremos opostos: de um lado está El Salvador, que tornou o *bitcoin* sua moeda nacional e meio legal de pagamento, e do outro vemos um país como a Guiana, que proibiu completamente o *bitcoin* ou qualquer criptomoeda.

O ponto ideal, é claro, está em algum lugar no meio: com proteções de mercado prospectivas claras para reduzir a pre-

valência de invasões, golpes, fraudes, lavagem de dinheiro por corrupção e crime organizado, mas com espaço para inovação dentro da indústria - é por isso que essa questão é tão fascinante no momento.

Um possível obstáculo para alcançar esse ponto ideal é a tendência recente que observamos nos Estados Unidos, que é a *regulamentação por meio de aplicação da lei* (*regulation by enforcement*). O conceito se refere a indivíduos e empresas sendo mirados como alvo de várias agências governamentais relacionadas a alegações de irregularidades, mas sem um quadro regulatório ou criminal prospectivo que forneça clareza.

Em outras palavras, os supostos infratores descobrem que cometeram um erro pela primeira vez quando recebem uma intimação ou são contatados por um órgão regulador - ou pior, quando estão enfrentando um mandado de prisão, uma acusação ou sanções - o que vimos recentemente no espaço dos *mixers* de criptomoedas.

Além de tornar difícil a alguém saber se está realmente violando a lei antes de tomar decisões comerciais, essa tendência é particularmente preocupante porque sufoca a inovação e o investimento - sem mencionar que ameaça a liberdade, a reputação e os ativos das pessoas envolvidas nas supostas ações criminosas.

Como mencionei antes, outro exemplo recente de regulamentação por meio de aplicação está relacionado a acusações criminais e sanções referentes aos *mixers* que mencionamos anteriormente. *Mixers* são empresas que criam uma desconexão entre a criptomoeda que um usuário envia e o que o destinatário recebe, e tornam sua regulamentação muito confusa.

Por um lado, torna-se muito difícil para as autoridades rastrearem os ativos. Portanto, eles são essencialmente uma ferramenta projetada para tornar as transações de criptomoedas mais privadas, o que, por um lado, permite que os usuários desfrutem de privacidade por motivos válidos - especialmente

no contexto de terem que se proteger de governos opressivos. É aí que vimos muitos desses *mixers* sendo usados de forma positiva. Como você ouviu, a recente prisão em Amsterdã do desenvolvedor de um *mixer* de criptomoedas realmente chocou a comunidade porque esses *mixers* estão sendo cada vez mais usados para atividades ilícitas.

Agora, os administradores de criptomoedas estão enfrentando sanções sem clareza suficiente sobre quais são as regras aplicáveis no setor. Não existe uma lei que diga que os *mixers* são, por si só, ilegais, mesmo que seja amplamente entendido que eles possam ser usados por terceiros para facilitar transações ilegais.

Compreensivelmente, como mencionei, a comunidade de criptomoedas ficou indignada, pois as pessoas e empresas só são informadas *posteriormente* de que ações como desenvolver *software* podem ser consideradas violações da lei e até mesmo resultar em sanções. Para complicar ainda mais, algumas dessas leis são antigas e nem sequer foram projetadas para abranger as criptomoedas. Portanto, é realmente importante fornecer mais clareza ao mercado.

Como eu disse, a clareza para o mercado é extremamente importante. É importante para todos os inovadores, muitos de vocês, talvez até mesmo aqui, que estão interessados em participar do impulso à inovação. Você não quer se encontrar acidentalmente com sua vida, liberdade e reputação em perigo sem clareza sobre as regras. Em um mundo ideal, os reguladores também apoiariam avanços tecnológicos que promovam o desenvolvimento e uso responsável de ativos digitais, mas também protegeriam o mercado, especialmente porque estamos vendo tantos investidores inexperientes entrarem no mercado, certo?

Portanto, uma regulamentação clara não apenas uma regulamentação clara protegerá os consumidores e os praticantes de criptomoedas, mas, do ponto de vista comercial,

empreendedores inteligentes, inovadores e investidores ganharão confiança e entrarão e impulsionarão o mercado e a inovação tecnológica.

No entanto, apesar da falta de clareza regulatória, mesmo nos Estados Unidos, estamos vendo reguladores competindo entre si para ver quem será o primeiro a realmente regular e fazer cumprir essas leis. Por exemplo, a disputa entre a Comissão de Valores Mobiliários (SEC) e a Comissão de Negociação de Futuros de Commodities (CFTC) destacou o debate sobre se uma criptomoeda é um título de crédito, ou uma mercadoria ou ambos.

Começando com essa pergunta básica, o que seria mais útil é que as tentativas de regulamentação promovessem uma maior clareza, como mencionei, e isso está recebendo cada vez mais atenção da Casa Branca. Eles recentemente divulgaram declarações e diretrizes políticas que buscam encontrar o equilíbrio adequado entre os aspectos positivos das criptomoedas (ou seja, eficiência financeira, inclusão liderança e finanças globais) com seus aspectos negativos, ou seja, potencial de financiamento ilícito, fraudes contra consumidores e empresas e, é claro, lavagem de dinheiro.

Então, quais foram as tendências recentes que aumentaram a pressão para que o governo acertar a regulamentação e que serão enfrentadas por todos os países que lutam para legislar e realmente trazer clareza aos mercados?

Bem, primeiro, vimos uma recente volatilidade incrível que deixou o universo das criptomoedas em alerta. As criptomoedas são obviamente altamente voláteis. No auge em novembro do ano passado, a capitalização de mercado do *bitcoin* estava em torno de 1,2 trilhão de dólares americanos. Hoje, isso caiu para menos de 400 bilhões. Certo. Então, enquanto a turbulência no mercado está causando quedas de preços de capa de jornal chamativas para os grandes nomes das criptomoedas

como o *Bitcoin* e o Ethereum, também é um fato que está sendo sentido em outros lugares.

A volatilidade de mercado é quase certamente uma forma de eliminar muitas das moedas fraudulentas, fracas e instáveis. Além disso, a volatilidade já começou a eliminar *exchanges* e fundos com estratégias ruins ou excessivamente alavancadas no mercado de criptomoedas. Eu mencionei antes que a Kobre & Kim representa casos de insolvência, e eles estão aumentando. Essa volatilidade do mercado levou a grandes insolvências de *exchanges* importantes, pois o mercado de criptomoedas está lutando para atender às demandas de saques.

O professor Renato de Mello Jorge Silveira mencionou a falta de requisitos para a garantia dos saldos reais nas *exchanges* de criptomoedas, o que veio à tona de forma muito dolorosa para muitos investidores. Então, muitas plataformas estão enfrentando problemas de liquidez e diversos *exchanges* têm declarado falência.

A questão-chave para os proprietários de criptomoedas nesse contexto é o modo como a lei os tratará em um contexto de insolvência. E , com o resultado provável é sendo que a maioria dos clientes comerciais das *exchanges* de criptomoedas insolventes será considerada apenas como credores gerais quirografários (sem qualquer garantia sobre a propriedade) não garantidos, no final da fila nos processos de insolvência - o que significa que eles seriam os últimos a receber qualquer pagamento e, portanto, seriam os que mais têm a perder.

Portanto, mais uma vez, a proteção do mercado, especialmente com investidores inexperientes, é extremamente importante. Recentemente, a Voyager Digital, uma corretora de criptomoedas, entrou com um pedido de falência no Capítulo 11[3] nos Estados Unidos e, em Singapura, a Three Arrows Capital pediu falência em julho e agora enfrenta reivindicações

/ [A] PROTEÇÃO DO MERCADO, ESPECIALMENTE COM INVESTIDORES INEXPERIENTES, É EXTREMAMENTE IMPORTANTE /

/ O ASPECTO
MAIS IMPORTANTE,
COMO EU DISSE
HOJE: EQUILÍBRIO.
EQUILÍBRIO
E CLAREZA /

de credores no valor de 3,5 bilhões. Estamos falando de uma escala massiva de perdas.

Lá em maio, quando seu valor havia despencado quase 90%, a Coinbase afirmou que, se eles pedissem falência - exatamente o que eu disse antes -, seus clientes seriam apenas credores não garantidos.

Esse risco não é novo. Voltando a 2014, a Mt. Gox, que na época era a maior *exchange* de criptomoedas do mundo, pediu falência no Japão depois que a maior parte de seus *bitcoins* desapareceu misteriosamente. Então, obviamente, quase oito anos depois e cada vez mais disso, veremos cada vez mais situações semelhantes.

Apesar da volatilidade do mercado, como você ouviu antes também, houve um aumento maciço no número de usuários legítimos de criptomoedas ingressando no mercado. A Chainalysis, uma empresa líder em análise de *blockchain*, relatou recentemente um aumento de 500% no uso legítimo de criptomoedas em relação ao ano anterior. Muitas vezes, investidores inexperientes que não conhecem o básico sobre criptomoedas estão arriscando grande parte de seu patrimônio líquido.

Infelizmente, além da volatilidade do mercado que mencionei, os consumidores também estão enfrentando um aumento incrível nos crimes envolvendo criptomoedas. O mesmo relatório que mencionei antes (da Chainalysis) estimou que, em 2021, mais de 14 bilhões de dólares em criptomoedas foram recebidos por carteiras criminosas de criptomoedas - um aumento em relação aos sete bilhões de dólares em 2020, ou seja, o dobro do valor.

Enquanto os otimistas apontarão para o fato de que o volume percentual de transações ilícitas nunca foi tão baixo, a verdade é que o volume de transações ilícitas aumentou em 79%. Isso é um aumento incrível, independentemente de ser proporcional ou não às outras tendências do mercado.

No entanto, não estou aqui apenas para desanimá-los. Existem pontos positivos nesse espaço. Há algo que pode ser feito se o pior acontecer, mesmo no caso de grandes crimes e *hacks* ocorrerem e indivíduos e empresas inocentes forem prejudicados significativamente.

A combinação de tecnologia de análise de *blockchain* e fortes parcerias público-privadas fortes nos Estados Unidos pode realmente permitir o rastreamento e a recuperação de ativos, mesmo em casos em que os alvos são fugitivos, o que muitas vezes é o caso. Então, não vou me aprofundar na tecnologia de rastreamento, mas a análise de *blockchain* deu passos gigantescos desde o tempo em que eu estava trabalhando no governo. Existem parcerias público-privadas muito poderosas com empresas de tecnologia que estão constantemente desenvolvendo a tecnologia para nos permitir rastrear efetivamente transações de criptomoedas.

Muitos de vocês aqui estão familiarizados com o fato de que existe uma transparência inerente às criptomoedas, porque toda essa tecnologia e os dados da *blockchain* podem ser usados em conjunto com ferramentas forenses para agrupar endereços sob controle comum, exibindo graficamente as conexões entre os endereços e, em muitos casos, identificar quais entidades controlam esses ativos.

Fundamentalmente, rastrear criptomoedas não é muito diferente do que eu costumava fazer no Departamento de Justiça. Você segue o dinheiro. Mas, em vez de ter que emitir intimações onerosas e examinar extratos bancários de muitos e muitos anos de transações, você realmente tem a capacidade de fazer isso de imediato e em tempo real com a nova tecnologia. Isso é uma oportunidade incrível para que as autoridades policiais tenham sucesso significativo.

A má notícia, como mencionei antes, é que *mixers* e outras novas tecnologias criam maneiras inovadoras de ocultar a

identidades no mundo real e frustrar as autoridades policiais, apesar de todos esses avanços tecnológicos.

Os *mixers* tornam muito difícil desemaranhar quais fundos foram para onde, e vimos que endereços ilícitos representam 23% dos fundos enviados para *mixers* até agora em 2022. O que mais se destaca é o enorme volume de fundos movendo-se para *mixers* de endereços associados a entidades sancionadas, e isso realmente tem chamado a atenção das autoridades policiais em todo o mundo e aumentado a cooperação entre as fronteiras como resultado.

Por exemplo, o mercado russo na *darknet* Hydra, que foi sancionado em abril de 2022, representa aproximadamente 50% de todos os fundos movendo-se para *mixers* de entidades sancionadas este ano, e quase todos os outros fundos provenientes de entidades sancionadas estão associados ao governo norte-coreano, ao grupo Lazarus e ao Blender.io.

Portanto, obviamente, as questões de sanções são de alto risco neste mês. Obviamente, como mencionei antes, as sanções para um dos primeiros *mixers*, Tornado Cash, e apenas quatro meses antes disso, para o Blender.io em maio de 2022, foram as primeiras. E o que realmente causou impacto com a designação do Tornado Cash foi a prisão de um desenvolvedor em Amsterdã, que discutimos aqui hoje, sinalizando que, além de sanções, os indivíduos podem enfrentar responsabilidade criminal simplesmente pelo desenvolvimento de tecnologia que pode ser usada ilegalmente por terceiros. Ou seja, indivíduos sendo responsabilizados por criar tecnologia que facilita o crime - o que é uma visão muito agressiva da lei. Mas, novamente, a boa notícia é que os *mixers* não são o fim da históriado caminho.

As mesmas empresas privadas que estão constantemente desenvolvendo tecnologia agora o fizeram para desfazer as transações envolvendo *mixers*. Embora os criminosos muitas

vezes estejam avançando em relação às autoridades policiais o mais rapidamente possível, muitas vezes, se permitirmos que o setor privado floresça, eles tentarão acompanhar os novos desafios que os criminosos apresentam.

Em geral, embora os *mixers* representem um desenvolvimento tecnológico fascinante para a privacidade na *blockchain*, a inovação tecnológica avançada permitiu que o aspecto transparente da *blockchain* triunfasse quando necessário, e estou ansiosao para vivenciar isso cada vez mais.

Apesar de todos esses desafios que mencionei, um dos temas que são próximos e queridos ao meu coração é a recuperação de ativos? Eu fazia isso no Departamento de Justiça. Eu faço isso agora na prática privada em nome das vítimas. E apesar de todos esses desafios, estamos vendo que a tecnologia da *blockchain* agora está disponível para as autoridades policiais por meio de parcerias público-privadas, bem como empresas privadas, e é evidente que o governo dos Estados Unidos começou a tratar os crimes relacionados a criptomoedas com a mesma abordagem que usam para qualquer outro crime. Eles estão rapidamente aplicando as leis existentes aos crimes relacionados a criptomoedas, não estão esperando por legislação específica.

Nos Estados Unidos, os perpetradores de fraudes envolvendo criptomoedas podem ser responsabilizados criminalmente por roubar ativos, lavar dinheiro, distorcer a natureza de tudo isso, e violações de fraude eletrônica e lavagem de dinheiro têm sido amplamente utilizadas.

Além disso, a legislação criminal e de confisco civil dos Estados Unidos tem sido rapidamente aplicada para visar e apreender grandes quantidades de ativos de criptomoedas. Somente em 2021, as agências federais dos Estados Unidos apreenderam mais de 5 bilhões de dólares em criptomoedas em nome das vítimas de crimes. Os Estados Unidos continuam

sendo líderes nessa área, também utilizando sob as disposições tradicionais de confisco de ativos segundo a lei dos Estados Unidos. Qualquer propriedade que possa ser rastreada como produto de fraude eletrônica ou fraude eletrônica está sujeita à confiscação, e nada disso exigiu nova legislação.

Além disso, se um ativo de criptomoeda for considerado envolvido em um delito de lavagem de dinheiro, até mesmo ativos misturados são considerados perdidos para os Estados Unidos. Essa é uma ferramenta incrivelmente poderosa que as agências dos Estados Unidos têm utilizado.

Importante e próximo de muitos de nós é o fato de que o governo pode usar os vastos recursos investigativos à sua disposição, incluindo tratados de cooperação internacional. Vimos isso recentemente, em novembro de 2020, em um dos casos - que acredito que a NPF também tenha lidado - de acordo com um MLAT oficial, eles conseguiram recuperar 24 milhões de dólares que estavam localizados nos Estados Unidos.

Portanto, não são apenas os Estados Unidos solicitando assistência, mas também outros governos. Esse foi um dos principais temas em termos de equilíbrio. É incrivelmente importante que, apesar da cooperação e da inovação, seja elementar fundamental para as autoridades internacionais continuarem a seguir as regras, mesmo quando a tecnologia em questão é muito diferente do que era no passado.

Por exemplo, vou dar uma versão anonimizada de um dos meus clientes. Temos um caso nos Estados Unidos em que nosso cliente, o réu, enfrenta uma acusação de esquema de pirâmide Ponzi de 2 bilhões de dólares, e o governo obteve uma ordem de restrição de bens e, de acordo com um MLAT, solicitou assistência de um país europeu. E, em vez de obter um mandado de apreensão e cumprir, de acordo com o MLAT, o país europeu simplesmente usou documentos recebidos durante a execução de um mandado de busca para alterar a

senha da conta do cliente e transferir um milhão de dólares em criptomoedas sem seguir os procedimentos criminais.

O fato de a inovação tecnológica permitir fazer isso não significa que as garantias do devido processo legal devam ser ignoradas. Portanto, esses são os tipos de desafios para as autoridades que serão incrivelmente importantes para equilibrar com a inovação.

Por último, e vou abordar isso muito rapidamente, você ouve falar de todas essas apreensões e pode se perguntar: o que acontece com os ativos confiscados de acordo com a lei dos Estados Unidos? Todos esses ativos acabam eventualmente nas mãos das vítimas que estão dispostas a se apresentar. E isso já aconteceu nos últimos anos. O programa de confisco de ativos do Departamento de Justiça devolveu mais de cinco bilhões de dólares em fundos confiscados civil e criminalmente para as vítimas de crimes desde 2002. Portanto, esse é um benefício significativo para os cidadãos dos Estados Unidos, ou de qualquer lugar, porque as vítimas não precisam ser americanas.

Também é uma ótima notícia que outros países estejam rapidamente tentando desenvolver suas leis para acompanhar os desafios tecnológicos (como o Reino Unido, Hong Kong e, é claro, como discutimos antes, o Brasil também está tentando se atualizar).

Para resumir, aqui estão algumas das principais conclusões. Infelizmente, sabemos que cada agência reguladora de aplicação da lei tem recursos limitados, então é incrivelmente importante apoiar os esforços para fornecer mais financiamento e recursos para promotores especializados, como o presente hoje, agências de investigação, etc. Além disso, como uma das 10 maiores economias do mundo, o Brasil tem uma oportunidade incrível de fomentar a inovação responsável e a criação de riqueza dentro da indústria de criptomoedas.

O aspecto mais importante, como eu disse hoje: equilíbrio. Equilíbrio e clareza.

Como mencionei antes, a disposição das instituições públicas de trabalhar com empresas tecnológicas privadas para apoiar seus esforços também pode ser um recurso tremendo (e isso tem funcionado muito bem nos Estados Unidos com poucas dificuldades).

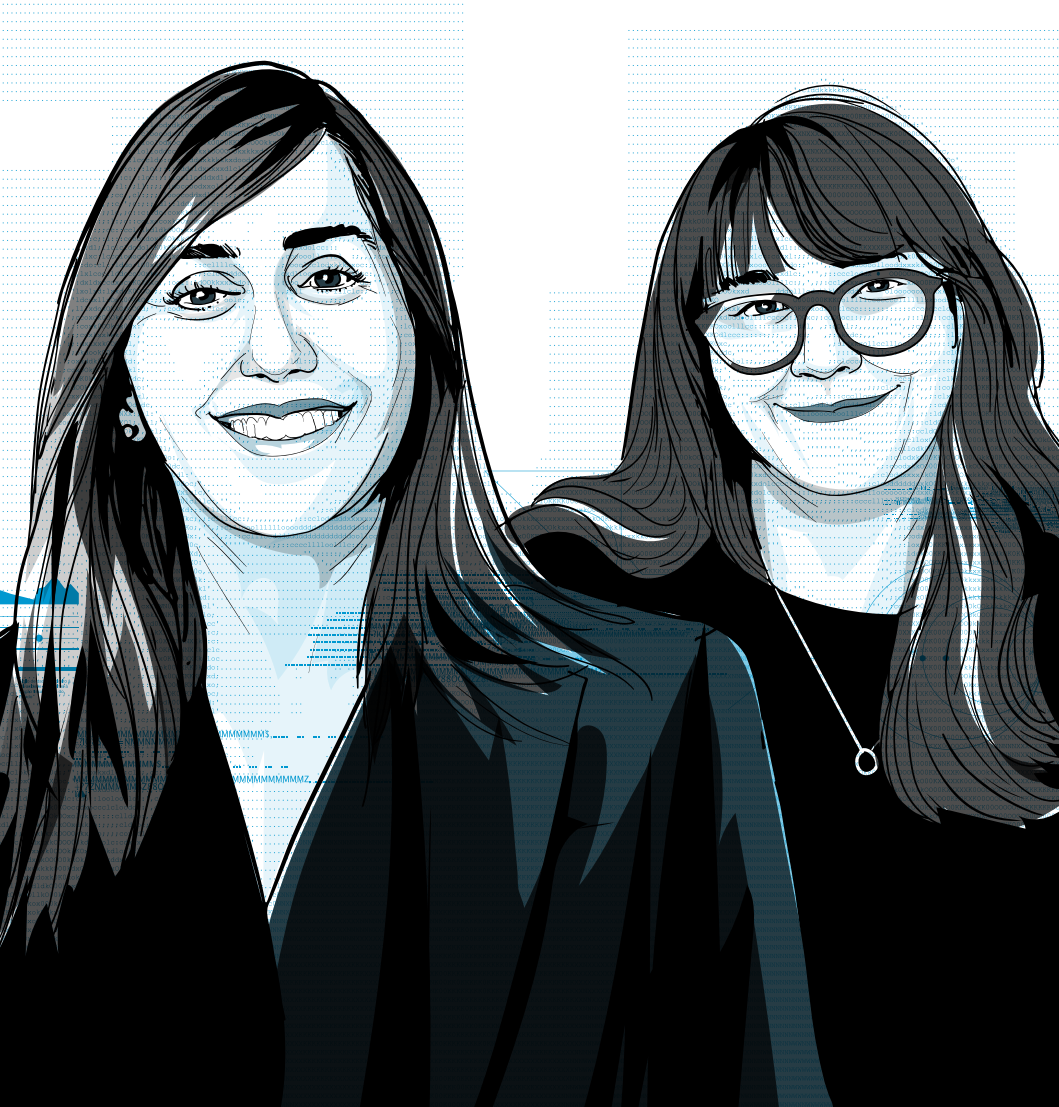
Por fim, é importante expandir, se necessário, e aprimorar as leis de confisco de ativos para permitir que os promotores que estão fazendo todo o trabalho não apenas busquem justiça contra os réus criminosos, mas também auxiliem na recuperação dos ativos relacionados a essas questões. E com isso, passo adiante. Muito obrigada.

NOTAS

1. Este artigo foi adaptado a partir de palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022.

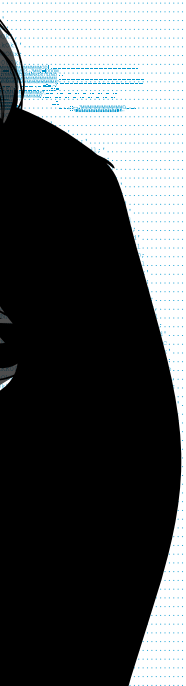
2. N/E: The Department of Justice is a federal executive department of the United States government tasked with the enforcement of federal law and administration of justice in the United States.

3. According to the official United States Courts website: "A case filed under chapter 11 of the United States Bankruptcy Code is frequently referred to as a "reorganization" bankruptcy. Usually, the debtor remains "in possession," has the powers and duties of a trustee, may continue to operate its business, and may, with court approval, borrow new money." Access in: https://shre.ink/lend



10.

INVESTIGAÇÕES PRIVADAS E CADEIA DE CUSTÓDIA DA PROVA DIGITAL



Juliana Sá de Miranda
e Nathália Corrêa
Leiser Tamer

INTRODUÇÃO

Investigar é inerente ao ser humano, curioso por natureza, instigado por desvendar os fatos ocorridos até se chegar a um determinado resultado.

Por esse motivo, costum a haver um certo fascínio em torno de qualquer investigação, sendo grande a expectativa de dar cabo ao suspense, se revelar a grande descoberta e como se chegou até ela.

Em princípio, qualquer pessoa pode fazer uma investigação, pois as investigações em geral não demandam uma técnica específica a ser observada pelo investigador.

Essa afirmação não é válida, contudo, para as chamadas investigações defensivas, que são aquelas em que se buscam provas para formar, corroborar ou robustecer a defesa de um determinado indivíduo ou empresa.

Apesar de não haver previsão legal de um procedimento a ser seguido na sua condução, toda a investigação defensiva deve observar os direitos fundamentais assegurados pela Constituição.

Essa premissa também se aplica às chamadas investigações internas, que são investigações privadas conduzidas nos ambientes corporativos.

Outro ponto de convergência entre as duas modalidades de investigação é a coleta de dados digitais, com preservação da cadeia de custódia, visando a assegurar a integridade da prova.

O presente artigo irá abordar as semelhanças e diferenças entre investigações internas e defensivas, a necessidade de assegurar direitos fundamentais nessas investigações e a cadeia de custódia de provas eletrônicas.

1. INVESTIGAÇÕES INTERNAS

Não obstante sua – razoavelmente - recente utilização no país, as investigações internas iniciaram no início dos anos 1970, quando empresas norte-americanas começaram a realizá-las

para averiguar suspeitas de suborno para autoridades estrangeiras em troca de benefícios comerciais, que culminou na promulgação do Foreign Corrupt Practives Act (FCPA) em 1977.

Desde então, o uso dessas investigações tem crescido significativamente em âmbito global, especialmente após escândalos financeiros que ocorreram a partir de 2001,[1] quando a descoberta de fraudes contábeis nas empresas Enron e WorldCom culminou na queda de uma grande empresa de auditoria e, posteriormente, na promulgação da Lei Sarbanes-Oxley, que visa aprimorar a governança corporativa e a transparência nas demonstrações financeiras.

No Brasil, as investigações internas se tornaram mais comuns após a promulgação da Lei Federal n. 12.846/2013 ("Lei Anticorrupção") e posteriores repercussões, como grandes operações para apuração de atos contra a Administração Pública e integração da ética como pilar da operação empresarial e expectativa social.

Após a entrada em vigor da Lei Anticorrupção, a criação de um "sistema de gestão" ou "programa" de *compliance* passou a ser recomendada visando, principalmente, a prevenção de atos ilícitos e a determinação de valores e diretrizes que orientarão a pessoa jurídica.

Investigações internas são contempladas dentro deste sistema como uma peça-chave ao real funcionamento e efetividade dos programas de integridade corporativos.

Trata-se de um procedimento técnico e com metodologia que, por meio da verificação aprofundada e ordenada de suspeitas e indícios, visa, primordialmente esclarecer e remediar[2] comportamentos indevidos ou em desacordo com diretrizes da empresa ou com a legislação.

Em vista da abrangência e sensibilidade deste mecanismo, se mostra fundamental a definição de critérios, regras e procedimentos específicos e transparentes, que orientem a prática,

de modo a garantir respaldo e controle adequados sobre a condução das averiguações, inclusive para preservação das garantias e valores inerentes ao devido processo legal.

O estabelecimento prévio de regras para a condução do procedimento e a necessária preservação da cadeia de custódia são essenciais para que fatos verificados e evidências eventualmente coletadas possam ser utilizados de forma legítima. Antes disso, visa também garantir que, ao tentar prevenir desvios de conduta por seus colaboradores, que as pessoas jurídicas não institucionalizem uma cultura de persecuções infundadas, violando direitos fundamentais dos envolvidos e/ou incorrendo, elas mesmas, em atos reprováveis legal e socialmente.

2. INVESTIGAÇÕES DEFENSIVAS

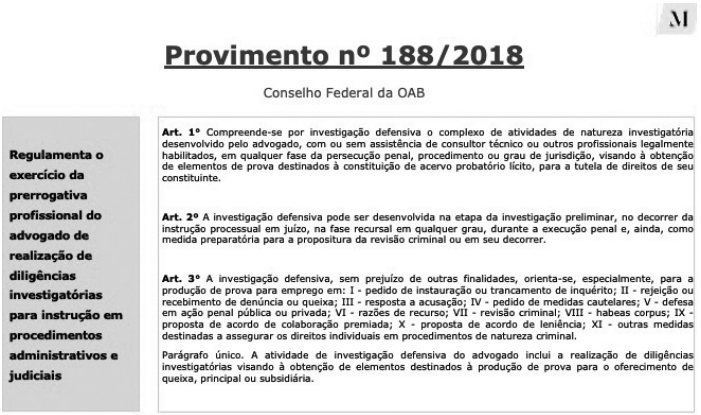
Com perfil diferenciado e objetivos mais específicos se comparadas às investigações internas, as investigações defensivas são realizadas como meio de defesa, desde muito antes da Lei Anticorrupção.

Amplamente reconhecidas no Direito Italiano, tendo sido formalizadas pela Lei n. 397/2000 neste país, e nos Estados Unidos da América, como consequência do regime jurídico estado-unidense e de seu modelo processual penal "adversarial", no Brasil, as investigações defensivas se apresentam, assim como em tais países, com o principal objetivo de levantamento de provas em contraposição à investigação pública e ao poder acusatório do Estado.[3]

Embora inexista regulamentação no Direito Processual Penal nacional ou outra norma específica sobre o procedimento para realização de investigações defensivas, a prática encontra seu embasamento nas normas do devido processo legal, na ampla defesa, no contraditório e, adicionalmente, na presunção de inocência.

Em dezembro de 2019, o Conselho Federal da Ordem dos Advogados do Brasil ("OAB") publicou o Provimento n. 188/2018[4] ("Provimento"), regulamentando o exercício da prerrogativa do advogado na realização de investigações defensivas.

O Provimento descreve a prática como "o complexo de atividades de natureza investigatória desenvolvido pelo advogado, (...), em qualquer fase da persecução penal, procedimento ou grau de jurisdição, visando à obtenção de elementos de prova destinados à constituição de acervo probatório lícito, para a tutela de direitos de seu constituinte".



M

Provimento nº 188/2018

Conselho Federal da OAB

Regulamenta o exercício da prerrogativa profissional do advogado de realização de diligências investigatórias para instrução em procedimentos administrativos e judiciais

Art. 1º Compreende-se por investigação defensiva o complexo de atividades de natureza investigatória desenvolvido pelo advogado, com ou sem assistência de consultor técnico ou outros profissionais legalmente habilitados, em qualquer fase da persecução penal, procedimento ou grau de jurisdição, visando à obtenção de elementos de prova destinados à constituição de acervo probatório lícito, para a tutela de direitos de seu constituinte.

Art. 2º A investigação defensiva pode ser desenvolvida na etapa da investigação preliminar, no decorrer da instrução processual em juízo, na fase recursal em qualquer grau, durante a execução penal e, ainda, como medida preparatória para a propositura da revisão criminal ou em seu decorrer.

Art. 3º A investigação defensiva, sem prejuízo de outras finalidades, orienta-se, especialmente, para a produção de prova para emprego em: I - pedido de instauração ou trancamento de inquérito; II - rejeição ou recebimento de denúncia ou queixa; III - resposta a acusação; IV - pedido de medidas cautelares; V - defesa em ação penal pública ou privada; VI - razões de recurso; VII - revisão criminal; VIII - habeas corpus; IX - proposta de acordo de colaboração premiada; X - proposta de acordo de leniência; XI - outras medidas destinadas a assegurar os direitos individuais em procedimentos de natureza criminal.

Parágrafo único. A atividade de investigação defensiva do advogado inclui a realização de diligências investigatórias visando à obtenção de elementos destinados à produção de prova para o oferecimento de queixa, principal ou subsidiária.

No entanto, o Provimento inova apenas ao colocar o advogado como condutor das investigações defensivas, determinando expressamente, em seu artigo 7º[5], que as atividades descritas no Provimento são privativas da advocacia, mas não traz muitas novidades sobre a técnica e metodologia necessárias para a condução do procedimento, preservação da cadeia de custódia ou poderes atribuídos aos seus condutores.

Apesar da especificação no provimento da OAB de que serão conduzidas em qualquer fase da persecução penal, as investigações defensivas podem ser empregadas em caráter preventivo a qualquer tempo a partir do momento de conhecimento

do eventual fato de risco[6]. Nesse sentido, as investigações defensivas também terão o objetivo de entender contextos, fluxos e buscar definir quem são os responsáveis pelo ato, mas com o propósito de preparar a defesa das partes – verificando-se, portanto, a necessidade de atuação do advogado em todo o processo, conforme apontado pelo Provimento.

No entanto, diferentemente das investigações internas, que têm como objetivo apurar irregularidades e infrações com o propósito de melhorias no "sistema de gestão" de *compliance*, as investigações defensivas partem de outra premissa – a de reação, seja para complementação ou contraposição de aspectos já levantados pela acusação (como a indicação de fatos que possam demonstrar causas de excludentes de ilicitude ou de culpabilidade), seja para avaliação da melhor estratégia de defesa.

As investigações defensivas, nesse sentido, propõem o papel ativo da defesa[7] na produção de provas e na eventual verificação de lacunas, erros ou omissões, por exemplo, cometidos em investigações públicas conduzidas paralelamente e de forma independente.

Ao considerar o aspecto processual penal presente nas investigações defensivas, destaca-se como exemplo de dificuldade a inexistência de poderes coercitivos no exercício das atividades investigatórias, de modo que se depende da cooperação voluntária e espontânea das pessoas envolvidas e do consentimento expresso do titular do direito para obtenção de certas informações.

Além das diferenças que decorrem das perspectivas histórica, conceitual e de expectativa de regulação, a metodologia utilizada também apresenta características de perfil diferenciado, de modo que a conservação de evidências e a preocupação com o tempo da investigação serão muito mais presentes na investigação defensiva quando comparada à investigação interna.

Mais um exemplo de diferença é o peso das possíveis consequências decorrentes das evidências constatadas. Enquanto nas investigações internas normalmente as evidências são utilizadas para fins diretivos e de pontos de melhoria interna,[8] nas investigações defensivas a não localização de evidências ou trabalhos probatórios frágeis podem resultar em consequências bem mais gravosas, como sanções administrativas, penas aos indivíduos (e pessoas jurídicas em caso de crimes ambientais), responsabilidade civil e riscos reputacionais.

Também se aponta a necessidade de que todas as atividades conduzidas sejam, a todo tempo, registradas em espécie de "dossiê" da investigação defensiva, com a devida explicação e garantia de observância da cadeia de custódia, que poderá posteriormente ser entregue às autoridades. Diferentemente de um relatório de investigação interna, no entanto, que trará, como regra, contexto sobre os fatos para registro imparcial, o "dossiê" de registro das atividades das investigações defensivas será construído de acordo com a utilidade das informações para a defesa da parte, tendo em vista que o papel do advogado – dentro dos limites da legalidade – é de representar os interesses de seus constituintes.

Contextualizadas, percebe-se que as investigações defensivas são aquelas realizadas com o propósito de defesa e obtenção de provas úteis para a defesa, diferentemente das investigações internas que visam ao esclarecimento dos fatos.

Além disso, destaca-se que, apesar das discrepâncias anteriormente mencionadas, tanto as investigações defensivas quanto as investigações internas compartilham dois pontos fundamentais, explorados a seguir: (i) a salvaguarda dos direitos fundamentais das pessoas envolvidas e (ii) a importância da manutenção da integridade da cadeia de custódia das evidências colhidas.

3. RESPEITO AOS DIREITOS FUNDAMENTAIS

Durante a condução de investigações privadas - internas ou defensivas – se deve assegurar a observância aos direitos fundamentais das pessoas envolvidas.

Por esse motivo, é fundamental que sejam tomadas as devidas precauções não somente para uma melhoria contínua do "sistema de gestão" de *compliance* ou para desenvolvimento de método de defesa mais sólido e alinhado ao devido processo legal, mas também para que as investigações, independentemente do foco principal, estejam conforme os valores e premissas do Estado Democrático de Direito.

Inclusive, é importante ressaltar que, embora não sejam investigações oficiais (conduzidas por autoridades públicas), as pessoas jurídicas têm a responsabilidade de manter vigilância constante na proteção de direitos fundamentais no seu papel esperado de agente social e de forma coerente com a eficácia horizontal de tais direitos.

Conforme destacam Fábio André Guaragni e Douglas Rodrigues da Silva[9] sobre as investigações internas, mas também perfeitamente aplicável às investigações defensivas: "a empresa, na condução das investigações internas, não está submetida de modo simétrico aos mesmos regramentos impostos ao Estado, pois está amparada em premissas distintas. Todavia, isso não torna as investigações corporativas imunes aos limites de admissão da prova, especialmente se existir o interesse de colaborar com o Estado na cessão de elementos para formação do processo penal. Nesse caso, é imprescindível a proposição de uma solução que contemple o direito individual dos trabalhadores, acolha as prerrogativas da empresa e afaste o risco do proveito estatal de provas obtidas com violação a direitos fundamentais".

Esta ideia de que as pessoas jurídicas no âmbito das investigações privadas – internas e defensivas - devam respeitar os

/ A INVESTIGAÇÃO DEFENSIVA DEVE OBSERVAR OS DIREITOS FUNDAMENTAIS ASSEGURADOS PELA CONSTITUIÇÃO /

/ A PRESERVAÇÃO DA CADEIA DE CUSTÓDIA GANHA AINDA MAIS RELEVÂNCIA CONSIDERANDO O ATUAL CENÁRIO TECNOLÓGICO /

direitos fundamentais dos envolvidos, apesar de não terem as mesmas premissas impostas ao Poder Público, encontra respaldo na jurisprudência brasileira, como no precedente histórico da decisão do Supremo Tribunal Federal no Recurso Extraordinário n. 201.819/RJ, que indicou que a autonomia privada não pode ser exercida em detrimento ou com desrespeito aos direitos de terceiros, especialmente aqueles positivados em sede constitucional.[10]

Nas investigações privadas reinará a presunção de inocência dos indivíduos, sendo que as partes envolvidas em uma investigação sempre deverão ter a oportunidade de serem ouvidas e de apresentarem suas versões dos fatos.

Em suma, é essencial estabelecer e respeitar limites de até onde uma investigação pode ir, considerando os contextos e objetivos da situação em pauta, sempre garantindo a licitude dos atos e a observância e respeito aos direitos fundamentais.

4. PRESERVAÇÃO DA CADEIA DE CUSTÓDIA DAS PROVAS DIGITAIS

As investigações defensivas e as evidências digitais possuem uma relação de utilidade profunda e cada vez mais evidente, à medida que as organizações ampliam o uso das tecnologias da informação e que o sucesso e a validade das provas extraídas das investigações defensivas, naturalmente, dependem da correta preservação das evidências. Falar em correta preservação, significa garantir a cadeia de custódia, sob pena de invalidade e consequente inutilidade dos trabalhos, a exemplo das decisões judiciais e precedentes citados adiante.

A preservação da cadeia de custódia, nesse sentido, implica criar um histórico de formação da prova, de modo a assegurar sua integridade e autenticidade desde o momento de identificação do fato investigado até a sua apresentação documen-

tada no procedimento de destino[11], evitando contaminações, adulterações e até mesmo perda de elementos de evidência ao longo de toda esta trajetória procedimental. A falta da gestão especializada de fontes e fatos é um dos maiores entraves nesta tarefa, conforme a jurisprudência tem confirmado, comprometendo estratégias, conclusões, fundamentos de defesa e até mesmo a sustentação de legalidade das evidências.

Conceito há muito tempo recorrente na prática forense, a cadeia de custódia só veio a ser definida legalmente, de forma específica, pelo Código de Processo Penal brasileiro em seu artigo 158-A, introduzido pela Lei n. 13.964/2019. Segundo a lei, a cadeia de custódia é "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

A definição acerta em dois pontos. Primeiro, a definição corretamente atrela a cadeia de custódia à ideia de "conjunto de práticas", de modo que a preservação da evidência não depende de um ato só, mas da reunião de procedimentos e tarefas a serem executadas de forma coordenada, como o engajamento de profissionais técnicos e jurídicos especializados, a utilização das ferramentas adequadas de *e-discovery* (ferramentas técnicas de levantamento de evidências digitais) etc. Em segundo lugar, o conceito trabalha o objetivo da tarefa de forma evidente: documentar a história cronológica da prova. O objetivo principal é certificar a real e segura fotografia dos fatos, sem qualquer risco de adulteração ou manipulação da identificação do fato até a coleta, documentação e apreciação administrativa ou judicial da evidência.

Deste modo, preserva-se a evidência e o registro de seu histórico, garantindo maior segurança jurídica em relação aos fatos nela contidos. A "ideia é que se alguém seguir os mesmos passos já dados na produção da prova, o resultado será

exatamente o mesmo", de modo que "é importante sinalizar datas, horários, quem teve acesso, onde o acesso foi feito e até quaisquer alterações inevitáveis relacionadas".[12]

Conforme entendimento da 6ª Turma do Superior Tribunal de Justiça ("STJ"), a "história cronológica dos vestígios" é relevante, pois "o instituto da quebra da cadeia de custódia refere-se à idoneidade do caminho que deve ser percorrido pela prova até sua análise pelo magistrado e, caso haja qualquer interferência durante o trâmite processual, poderá implicar a sua imprestabilidade".[13] Igualmente, é o precedente da 5ª Turma do STJ sobre a afirmação da preservação da idoneidade no caminho probatório.[14]

A inclusão da definição de cadeia de custódia no Código de Processo Penal, nesse sentido, documentou um importante conceito prático e, em especial, vinculou os órgãos persecutórios à maior transparência e segurança na condução das investigações.

Entende-se que o principal foco da cadeia de custódia da prova, portanto, é preservar sua utilidade a partir da segurança técnico-jurídica de seu histórico de formação – do fato à documentação do seu registro. Adicionalmente, aponta-se que, seja em investigações internas seja em investigações defensivas, a preservação da cadeia de custódia é requisito que se impõe mesmo antes do texto legal incluído no Código de Processo Penal, tendo em vista a necessidade de evitar qualquer dúvida sobre a origem e a integridade das evidências, garantindo a imparcialidade e a transparência do processo, além de contribuir para a proteção dos direitos e garantias individuais dos envolvidos no caso. Ao estabelecer um rastro documentado e ininterrupto do manuseio das provas, é possível evitar a possibilidade de adulterações maliciosas ou acidentais, bem como contestações futuras sobre a validade das evidências apresentadas.

Importante destacar, conforme ensina Gustavo Badaró, que "a documentação da cadeia de custódia é de responsabilidade das pessoas que têm contato com a fonte de prova custodiada".[15] Depreende-se, portanto, que a preservação da cadeia de custódia também é de responsabilidade da parte privada, principalmente em seus procedimentos investigatórios, independentemente de sua natureza.

A preservação da cadeia de custódia ganha ainda mais relevância considerando o atual cenário tecnológico no qual as interações, arquivos, elaboração de documentos e registro de informações são realizados majoritariamente por meios eletrônicos, *e-mails* ou outras comunicações telemáticas, mensagens de textos, registros de chamadas, registros de navegação na *internet*, registros de transações financeiras e registros em mídias sociais.

As mudanças associadas às tecnologias, neste contexto, têm potencializado a complexidade das tarefas de preservação da cadeia de custódia, uma vez que trazem elementos que podem dificultar a coleta probatória. Importante lembrar que os pilares de autenticidade e integridade não são aspectos inerentes às evidências eletrônicas e digitais, mas da prova em si, ainda que analógica. O que as tecnologias da informação fazem é agregar ainda mais complexidade a esta tarefa.

A tecnologia pode agregar ainda mais complexidade à cadeia de custódia ao tornar os fatos menos visíveis, exigir discussões jurídicas mais profundas em decorrência do perfil técnico do que foi feito e impor exigências legais específicas, a exemplo do previsto na Lei n. 12.965/2014 (Marco Civil da Internet), que regula a guarda e fornecimento de registros eletrônicos de conexão e acesso. Todos esses fatores devem ser levados em consideração na preservação da cadeia de custódia para garantir que as provas coletadas sejam admissíveis

em procedimentos administrativos e/ou judiciais e que não levantem dúvidas quanto à sua autenticidade e integridade.

A jurisprudência traz muitos exemplos da invalidação e inutilidade das evidências digitais pela falha na preservação da cadeia de custódia. Essas decisões são diretrizes para aceitação da prova no processo penal.

Neste contexto, destaca-se decisão proferida também pela 5ª Turma do STJ,[16] em que foi discutido o conceito de cadeia de custódia e apontada a responsabilidade da parte acusatória (no caso, o Estado) em preservar a integridade das fontes de prova arrecadadas durante uma investigação. Nesta decisão, a cadeia de custódia foi ressaltada como fundamental para constatar a integridade e a confiabilidade das fontes de prova apresentadas pela acusação, de forma que, sem ela, não seria possível verificar se os dados apresentados são íntegros e idênticos aos originais, o que resultaria na inadmissibilidade das provas apresentadas e das que delas derivam. Segundo voto-vista do Min. Ribeiro Dantas, "A documentação da cadeia de custódia é essencial no caso da análise de dados digitais, porque permitirá assegurar a autenticidade e integridade dos elementos de prova e excluirá que tenha tido alterações indevidas do material digital". Neste caso, como ressaltou a Corte, esperava-se que as autoridades policiais tivessem documentado as decisões e o passo a passo na coleta dos dados e evidências, de modo que, segundo outro trecho do voto-vista, foi destacado o desconhecimento de como a polícia fez estas tarefas e de que cabe ao "Judiciário controlar a atuação do Estado-acusação a partir do Direito, e não a partir de autoproclamada confiança que o Estado-acusação deposita em si mesmo".

Em outro caso julgado pelo STJ, a 5ª Turma decidiu que "são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preser-

vação da integridade, da autenticidade e da confiabilidade dos elementos informáticos".[17]

Neste cenário, é importante que as pessoas jurídicas adotem regras formais sobre a documentação e registro de toda prova coletada, independentemente de sua natureza, enfatizando a importância do registro de informações sobre quem coletou a evidência, quando e onde foi coletada, como foi armazenada, quem teve acesso a ela e eventuais alterações realizadas.

A formalização deste processo, bem como o treinamento de todas as partes envolvidas, se mostra crucial para evitar falhas ou irregularidades em qualquer fase de apuração dos fatos e formação da evidência, mitigando riscos de inadmissibilidade por má qualidade de formação ou mesmo violação à norma jurídica (princípio da vedação à prova ilícita). Inclusive, repisa-se o conceito e necessidade de "dossiê" mencionado no tópico sobre investigações defensivas, em que, por função própria do documento, a parte poderá incluir todos as atividades probatórias realizadas (com detalhamento, por exemplo, de informações sobre a coleta, armazenamento, manuseio e transporte das evidências, bem como a identificação dos responsáveis por cada etapa do processo).

NOTAS

1. "*La reciente aparición de las investigaciones internas em este escenario lleva muchas veces a pensar que se trata de una temática absolutamente novedosa. Sin embargo, el moderno uso de las investigaciones internas tuvo sus inicios entre las empresas norteamericanas a comienzos de los setenta ante la sospecha de sobornos pagados a autoridades de Bélgica, Japón, Holanda, Honduras e Italia para obtener contratos públicos. A mediados de los años ochenta se convirtieron en algo muy común en los Estados Unidos, hasta llegar al máximo de popularidad en todo el mundo con los escándalos financieros iniciados en el año 2001.*" (MONTIEL, Juan Pablo. Autolimpieza Empresarial: Compliance Programs, Investigaciones Internas y Neutralización de Riesgos Penales *In* KUHLEN, Lothar [et. al] *Compliance y teoría del Derecho Penal*. Madrid: Marcial Pons, 2013, p. 221-242).

2. "*Los objetivos perseguidos con una investigación interna, en función de los cuales debe enjuiciarse la adecuación de las medidas de indagación disponibles son acertadamente agrupados por Moosmayer como sigue (...): (i) Evitación de la responsabilidade (...); (ii) Esclarecimiento, interrupción y sanción de comportamientos irregulares: (...); (iii) Obtención de información sobre deficiencias en el sistema de control interno de la empresa: (...); (iv) Prevención: las investigaciones internas muestran a los trabajadores y colaboradores de forma explícita que los órganos directivos de toman en serio los indicios de comportamientos defectuosos y que los persiguen de forma consecuente*." (MOOSMAYER, Klaus. Compliance: Praxisleitfaden für Unternehmen, 2. Ed., Munique, C.H.Beck, 2011, p. 99 Apud SAHAN, Oliver. Investigaciones empresariales internas desde la perspectiva del abogado *In* KUHLEN, Lothar [et. al] Compliance y teoría del Derecho Penal. Madrid: Marcial Pons, 2013, p. 221-242).

3. Os autores definem a investigação defensiva como: "*[...] o complexo de atividades de natureza investigatória desenvolvido, em qualquer fase da persecução criminal, inclusive na antejudicial, pelo defensor, com ou sem assistência de consultor técnico, tendente à coleta de elementos objetivos, subjetivos e documentais de convicção, no escopo de construção de acervo probatório lícito que, no gozo da parcialidade constitucional deferida, empregará para pleno exercício da ampla defesa do imputado em contraponto à investigação ou acusação oficial.*" (AZEVEDO, André Boiani e BALDAN, Édson Luís. A preservação do devido processo legal pela investigação defensiva (ou do direito de defender-se provando) In INSTITUTO DE CIÊNCIAS CRIMINAIS, Boletim do Instituto de Ciências Criminais n. 137, abril/2004, Disponível em: https://shre.ink/le1x, Acesso em 18.04.2023).

4. ORDEM DOS ADVOGADOS DO BRASIL, Provimento n. 188/2018, Disponível em: https://shre.ink/le1B, Acesso em 18.04.2023.

5. Art. 7º As atividades descritas neste Provimento são privativas da advocacia, compreendendo-se como ato legítimo de exercício profissional, não podendo receber qualquer tipo de censura ou impedimento pelas autoridades. Disponível em: https://shre.ink/le1B, Acesso em 18.04.2023).

6. "Tal tarefa, não adstrita a ritos ou formas, pode ser desenvolvida em qualquer fase ou grau da persecução penal ou, ainda, em caráter meramente preventivo, isto é, diante da possibilidade de instauração de eventual procedimento criminal". (AZEVEDO, André Boiani e BALDAN, Édson Luís. Ibidem).

7. Sobre a adoção do instrumento de investigações defensivas, os autores apontam que seria esperado que a adoção deste instrumento tivesse algumas consequências imediatas, como "*a) aprimoramento da investigação policial*

como contraponto eficaz às provas produzidas pelo defensor, obrigando a polícia judiciária e o ministério público à busca de contínuo aperfeiçoamento técnico-científico; b) criação (ou desenvolvimento) de uma categoria profissional, a dos investigadores privados; c) estímulo ao culto das ciências afins ao Direito Penal, como a Criminalística, Criminologia, Medicina Legal, com a consequente necessidade de adequação do ensino técnico e superior; d) redimensionamento da estatura jurídica do Advogado (dentro e fora do processo), transmudando-o da condição de mero espectador inerme e inerte para a posição de ativo protagonista na formação da prova criminal; e) obrigação da motivação judicial na admissão da acusação, criando-se verdadeiro juízo de prelibação que arredaria a instauração da instância judicial quando insuficientes os elementos indiciários; f) maior proximidade do processo penal com a verdade real pelo fortalecimento da prova criminal, com a consequente serenidade do magistrado ao proferir seu decisum, pois com ouvidos às razões produzidas por acusação e defesa em perfeita égalité des armes." (AZEVEDO, André Boiani e BALDAN, Édson Luís. Ibidem).

8. Neste aspecto, aponta-se atividades que estejam estão dentro do âmbito decisório da própria organização e dentro de sua liberdade de condução dos negócios, sem repercussões externas negativas – como, por exemplo, a realização de treinamentos de conscientização sobre políticas e procedimentos internos ou até mesmo temas específicos relacionados a eventuais suspeitas de infração.

9. GUARAGNI, Fábio André; DA SILVA, Douglas Rodrigues. A proteção da privacidade no processo penal e investigações corporativas: uma análise sobre o monitoramento de smartphones In Revista Brasileira de Ciências Criminais, vol. 186, dez/2021, versão eletrônica, p. RR-6.2. grifo nosso

10. SOCIEDADE CIVIL SEM FINS LUCRATIVOS. UNIÃO BRASILEIRA DE COMPOSITORES. EXCLUSÃO DE SÓCIO SEM GARANTIA DA AMPLA DEFESA E DO CONTRADITÓRIO. EFICÁCIA DOS DIREITOS FUNDAMENTAIS NAS RELAÇÕES PRIVADAS. RECURSO DESPROVIDO. I. EFICÁCIA DOS DIREITOS FUNDAMENTAIS NAS RELAÇÕES PRIVADAS. As violações a direitos fundamentais não ocorrem somente no âmbito das relações entre o cidadão e o Estado, mas igualmente nas relações travadas entre pessoas físicas e jurídicas de direito privado. Assim, os direitos fundamentais assegurados pela Constituição vinculam diretamente não apenas os poderes públicos, estando direcionados também à proteção dos particulares em face dos poderes privados. II. OS PRINCÍPIOS CONSTITUCIONAIS COMO LIMITES À AUTONOMIA PRIVADA DAS ASSOCIAÇÕES. (...) **A autonomia privada, que encontra claras limitações de ordem jurídica, não pode ser exercida em detrimento ou com desrespeito aos direitos e garantias de terceiros, especialmente aqueles positivados em sede constitucional**, pois a autonomia da vontade não confere aos particulares, no domínio de sua incidência e atuação, o poder de transgredir ou ignorar as restrições postas e

definidas pela própria Constituição, cuja eficácia e força normativa também se impõem, aos particulares, no âmbito de suas relações privadas, em tema de liberdades fundamentais. (STF, Tribunal Pleno, Recurso Extraordinário n. 201.819/RJ, Min. Rel. Gilmar Mendes, j. 11.10.2005, grifo nosso)

11. O procedimento de destino da investigação defensiva seria justamente aquele para o qual a investigação é realizada. Existindo utilidade na construção da defesa, há um procedimento de destino a ser considerado. O Provimento da OAB traz bons exemplos neste sentido: "Art. 3º A investigação defensiva, sem prejuízo de outras finalidades, orienta-se, especialmente, para a produção de prova para emprego em: I - pedido de instauração ou trancamento de inquérito; II - rejeição ou recebimento de denúncia ou queixa; III - resposta a acusação; IV - pedido de medidas cautelares; V - defesa em ação penal pública ou privada; VI - razões de recurso; VII - revisão criminal; VIII - habeas corpus; IX - proposta de acordo de colaboração premiada; X - proposta de acordo de leniência; XI - outras medidas destinadas a assegurar os direitos individuais em procedimentos de natureza criminal. Parágrafo único. A atividade de investigação defensiva do advogado inclui a realização de diligências investigatórias visando à obtenção de elementos destinados à produção de prova para o oferecimento de queixa, principal ou subsidiária.".

12. TAMER, Mauricio. Provas no Direito Digital, 2. Ed., São Paulo: Thomson Reuters, 2022, versão eletrônica, p. RB-1.4.

13. STJ, 6ª T., Agravo Regimental no Habeas Corpus n. 147.885/SP, Min. Rel. Olindo Menezes, j. 07.12.2021.

14. STJ, 5ª T., Agravo Regimental no Habeas Corpus n. 615.321/PR, Min. Rel.

15. BADARÓ, Gustavo Henrique. Processo penal, São Paulo, Thomson Reuters Brasil, 9. Ed., 2023, versão eletrônica, p. 10.34.

16. PENAL E PROCESSUAL PENAL. (...)CADEIA DE CUSTÓDIA. INOBSERVÂNCIA DOS PROCEDIMENTOS TÉCNICOS NECESSÁRIOS A GARANTIR A INTEGRIDADE DAS FONTES DE PROVA ARRECADADAS PELA POLÍCIA. FALTA DE DOCUMENTAÇÃO DOS ATOS REALIZADOS NO TRATAMENTO DA PROVA. CONFIABILIDADE COMPROMETIDA. PROVAS INADMISSÍVEIS, EM CONSEQUÊNCIA. AGRAVO REGIMENTAL PARCIALMENTE PROVIDO PARA PROVER TAMBÉM EM PARTE O RECURSO ORDINÁRIO. (...)2. A principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo. 3. Embora o específico regramento dos arts. 158-A a 158-F do CPP (introduzidos pela Lei 13.964 (2019) não retroaja, a necessidade de preservar a cadeia de custódia não surgiu com eles. Afinal, a

ideia de cadeia de custódia é logicamente indissociável do próprio conceito de corpo de delito, constante no CPP desde a redação original de seu art. 158. Por isso, mesmo para fatos anteriores a 2019, é necessário avaliar a preservação da cadeia de custódia. 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado. 6. É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle; isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo. 7. No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º , do CPP . 9. Agravo regimental parcialmente provido, para prover também em parte o recurso ordinário em habeas corpus e declarar a inadmissibilidade das provas em questão. (STJ, 5ª T., Agravo Regimental no Recurso em Habeas Corpus n. 143.169/RJ, Min. Rel. Messod Azulay Neto, j. 07.02.2023)

17. O caso está sob segredo de justiça, mas referências oficiais estão disponíveis em: https://shre.ink/QqBP. Acesso em: 09.06.2023.

REFERÊNCIAS BIBLIOGRÁFICAS

AZEVEDO, André Boiani e BALDAN, Édson Luís. A preservação do devido processo legal pela investigação defensiva (ou do direito de defender-se provando) *In* INSTITUTO DE CIÊNCIAS CRIMINAIS, *Boletim do Instituto de Ciências Criminais n. 137*, abril/2004, Disponível em: https://shre.ink/le1x, Acesso em 18.04.2023.

BADARÓ, Gustavo Henrique. Processo penal, São Paulo, Thomson Reuters Brasil, 9. Ed., 2023, versão eletrônica.

GUARAGNI, Fábio André; DA SILVA, Douglas Rodrigues. A proteção da privacidade no processo penal e investigações corporativas: uma análise sobre o monitoramento de smartphones *In Revista Brasileira de Ciências Criminais*, vol. 186, dez/2021, versão eletrônica.

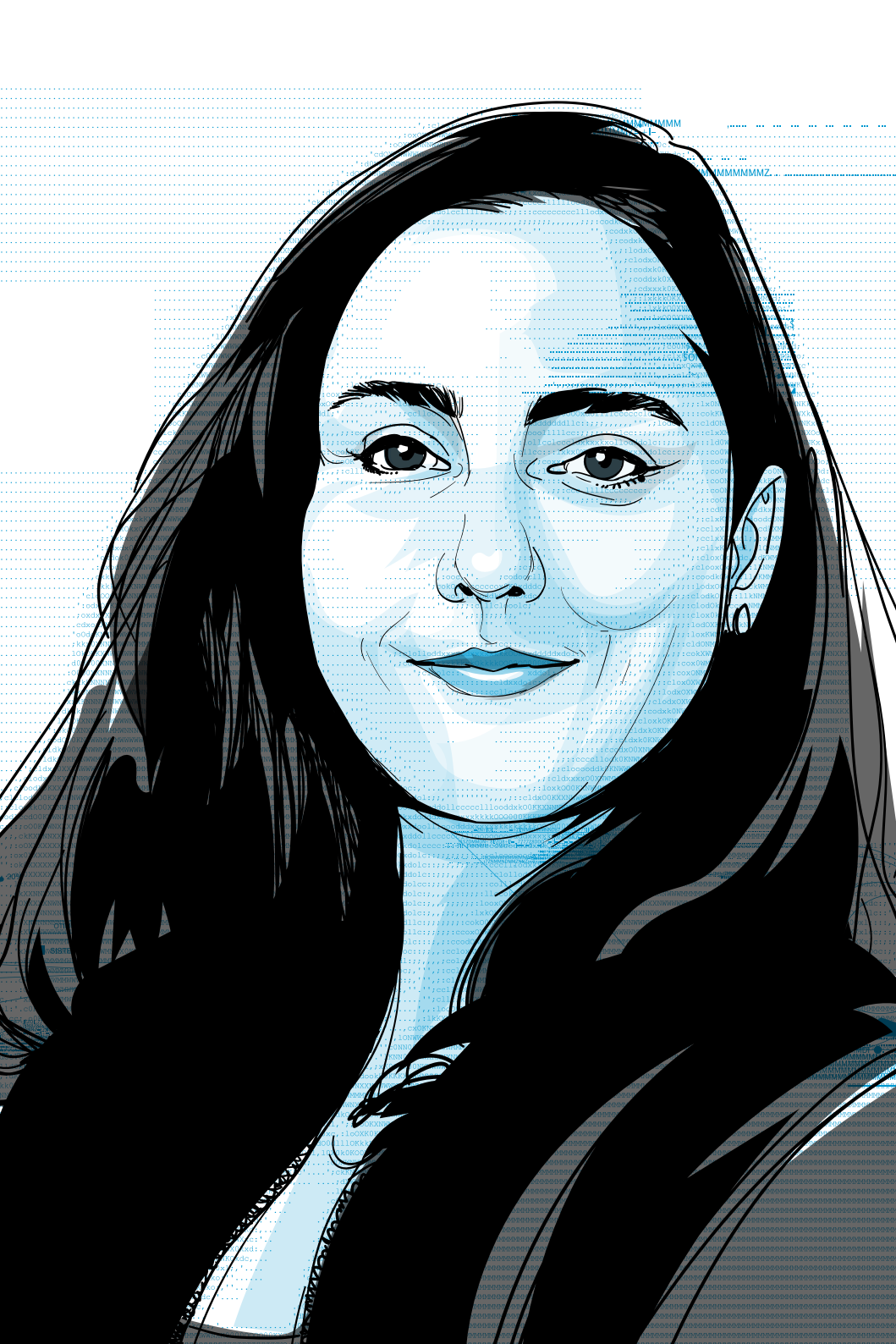
MONTIEL, Juan Pablo. Autolimpieza Empresarial: Compliance Programs, Investigaciones Internas y Neutralización de Riesgos Penales *In* KUHLEN, Lothar [et. al] *Compliance y teoría del Derecho Penal*. Madrid: Marcial Pons, 2013.

MOOSMAYER, Klaus. *Compliance: Praxisleitfaden für Unternehmen*, 2. Ed., Munique, C.H.Beck, 2011, p. 99 *Apud* SAHAN, Oliver. Investigaciones empresariales internas desde la perspectiva del abogado *In* KUHLEN, Lothar [et. al] *Compliance y teoría del Derecho Penal*. Madrid: Marcial Pons, 2013.

ORDEM DOS ADVOGADOS DO BRASIL, *Provimento n. 188/2018*, Disponível em: https://shre.ink/le1B. Acesso em 18.04.2023.

STF, Tribunal Pleno, Recurso Extraordinário n. 201.819/RJ, Min. Rel. Gilmar Mendes, j. 11.10.2005.

TAMER, Mauricio. *Provas no Direito Digital*, 2. Ed., São Paulo : Thomson Reuters, 2022, versão eletrônica.



11.

DADOS ESTÁTICOS, PROPORCIONALIDADE E VIGILANTISMO, UMA ANÁLISE DO RE 1301250[1]

Clarissa Borges

Bom dia a todas e a todos, inclusive aos colegas que estão remotamente. Gostaria de iniciar agradecendo não só o convite para que o Instituto de Defesa do Direito de Defesa (IDDD) pudesse expor a tese que está em elaboração a respeito do Recurso Extraordinário 1301250, mas também pela oportunidade de estar depois de mais de dois anos num evento presencial.

O IDDD é uma associação de advogados criminalistas que tem sua maior preocupação na garantia do direito de defesa em seu sentido mais amplo. E tem olhado para as questões das provas - e das provas digitais - com bastante cuidado e cautela diante dos incontáveis documentados e conhecidos abusos, que formam o tratamento que o judiciário e a polícia dão sobre as provas, pode acarretar. E é essa, então, a nossa inserção num tema que é bastante delicado porque chega ao Supremo Tribunal Federal a partir de um caso que foi tratado pelo próprio Superior Tribunal de Justiça como um caso difícil.

Um caso difícil porque traria ali uma contraposição entre o direito à privacidade, à intimidade e direitos decorrentes dessa própria garantia, e o direito à segurança e a necessidade de investigação de um caso que chocou a todos nós, que é o duplo homicídio contra Marielle Franco e Anderson Gomes, o motorista, em março de 2018. Vou trazer aqui para vocês: são 1625 dias desde que o crime aconteceu e eu sei disso porque diariamente a Eliane Brum e a Laerte Coutinho publicam no Twitter a pergunta "*Quem matou?*" e "*Quem mandou matar Marielle Franco e Anderson?*".

Essa é, de fato, uma pergunta que deve ser respondida pelas autoridades. Já existem indícios de autoria que apontariam para dois autores que estão presos desde 2019 que seriam executores, autores imediatos do delito. Mas a pergunta a respeito da autoria mediata, de quem seriam os mandantes, ainda se encontra em aberto. Nós não temos, de fato, informações a respeito dessa investigação, do que leva até esses dois suspei-

tos e das dúvidas que pairam a respeito da autoria mediata. Essas informações, elas são essencialmente sigilosas porque contidas no inquérito. Então, o que nós temos hoje é o que a imprensa pode nos proporcionar.

Portanto, o raciocínio da autoridade de polícia judiciária e do Ministério Público que culmina naquela decisão que autoriza a quebra do sigilo com relação às buscas feitas no Google num período de cinco dias - buscas por termos que parecem até inofensivos, a princípio: "*Marielle Franco*", "*Agenda Marielle Franco*", o endereço "*Rua dos Inválidos*", "*Casa das Pretas*", o local onde já se encontrava antes que o delito fosse cometido. Esses dados que foram solicitados num período de cinco dias antes do delito parecem, então, bastante etéreos.

No entanto, a quebra que foi determinada – que foi autorizada pelo STJ e agora está sob exame do STF –, tem o condão de atingir uma quantidade indeterminada de pessoas, uma vez que, segundo a própria argumentação do recurso, isso diz respeito à popular vereadora no Rio de Janeiro, uma rua muito comum no centro do Rio de Janeiro na Lapa, às vésperas do Carnaval, e é um local frequentado por ativistas. Esses dados, quando desdobrados, podem revelar muitas outras informações para além daquilo que foi precisamente solicitado pela polícia, e esta é a nossa primeira preocupação. Os endereços de IP que são solicitados e aqueles que acessaram aquelas buscas no Google, a partir desses dados é possível extrapolar para preferências religiosas, políticas, hábitos de consumo e hábitos de deslocamento. Enfim, uma série de informações que são tão privadas que, indiferente da discussão a respeito do que se tratam os dados e a natureza dos dados, elas, por si só, mereceriam a tutela da privacidade, a garantia inafastável da privacidade.

De outro lado, quando nós pensamos nos dados, existe essa discussão que está em jogo a respeito dos dados em fluxo de

comunicação e que, portanto, estariam protegidos por um sigilo especial na Constituição ou se trataria de dados estáticos. Essa questão eu considero bastante sensível, porque tem sido relativizada pela jurisprudência a proteção aos dados estáticos. Esses dados estáticos podem ser acessados de diversas formas.

A controvérsia diz respeito ao flagrante, mas nós sabemos que abordagens policiais, outra forma de diligência probatória com alvos incertos, já mostram um direcionamento para esse tipo de abuso. O acesso do policial sem ordem judicial aos dados estáticos contidos em aparelhos celulares - também é algo que já foi tratado aqui na exposição anterior, que não é nem um risco, é um fato - é uma medida marcada pelo racismo institucional das polícias.

Uma pesquisa que foi publicada essa semana a respeito, no contexto do Jacarezinho no Rio de Janeiro, mostra que 70% das pessoas respondentes que foram alvo de abordagens policiais tiveram seus telefones revistados. Quer dizer, os policiais entram procurando a autoria delitiva ou indícios de autoria delitiva. E isso tem uma marcação racial muito séria neste país, ou até mesmo o caso de um celular que seja apreendido e a polícia vai lá e vasculha. A quantidade de informação que é obtida dali - desses dados estáticos - chega a ser assustadora. E revela a intimidade do proprietário, ou do usuário, daquele dispositivo para muito além do objeto da própria investigação criminal. Em razão disso, também é necessária a proteção especial às buscas. Elas revelam muito a respeito de nós mesmos.

De uma forma quase anedótica: eu não conhecia Marielle Franco até aquele momento do crime. E aí, eu vejo a internet implodir. A primeira coisa que eu fiz: fui ao Google e pesquisei "*Marielle Franco*". E a partir disso, a gente passa a acompanhar essas informações que nós estamos cedendo para os provedores, de que eles estão nos fornecendo. Elas podem mostrar

/ A PARTIR DESSES DADOS É POSSÍVEL EXTRAPOLAR PARA PREFERÊNCIAS RELIGIOSAS, POLÍTICAS, HÁBITOS DE CONSUMO E HÁBITOS DE DESLOCAMENTO /

muito a respeito de quem nós somos e o Estado não deveria ter acesso a isso.

Além disso, é importante mostrar a ausência de proporcionalidade nessa medida para averiguar e investigar este homicídio, o que é algo realmente necessário. A polícia está se valendo dessa medida probatória, mas em momento algum nos autos está justificada a proporcionalidade, o sacrifício de direitos e garantias de uma quantidade inestimável de pessoas, considerando que ali não existe justificativa a respeito do prazo, não existe justificativa a respeito dos próprios termos de busca e sequer indicativo da forma como os dados serão tratados. Nós temos dúvidas, inclusive, a respeito da cadeia de custódia daquilo tudo. Ou seja, nós não temos, enquanto institucionalidade, a experiência para o tratamento dessas informações de forma que seja correta, que seja fidedigna e até mesmo a forma como esses dados poderão ser extrapolados.

Pesquisando para esta fala, eu vi entrevista de um dos suspeitos de ser o autor do homicídio. Ele fala para a revista Veja. A polícia conseguiu quebrar o sigilo daquele sujeito determinado e teria constatado que ele passou três meses fazendo buscas a respeito de Marielle, de Freixo. E nos dias que antecediam ao crime, a respeito de uma arma em específico, que seria do mesmo modelo que teria sido utilizado no delito. Essa é uma informação que está na imprensa. Mas ele tem outra justificativa para aquilo. E estou dizendo isso porque presumidamente inocente, mas ele tem outra justificativa: "*Sou colecionador de armas, estava buscando para...*", enfim, a forma como a informação é utilizada, inclusive para construção de narrativas, é um risco que não pode ser desprezado ali no tratamento desses dados.

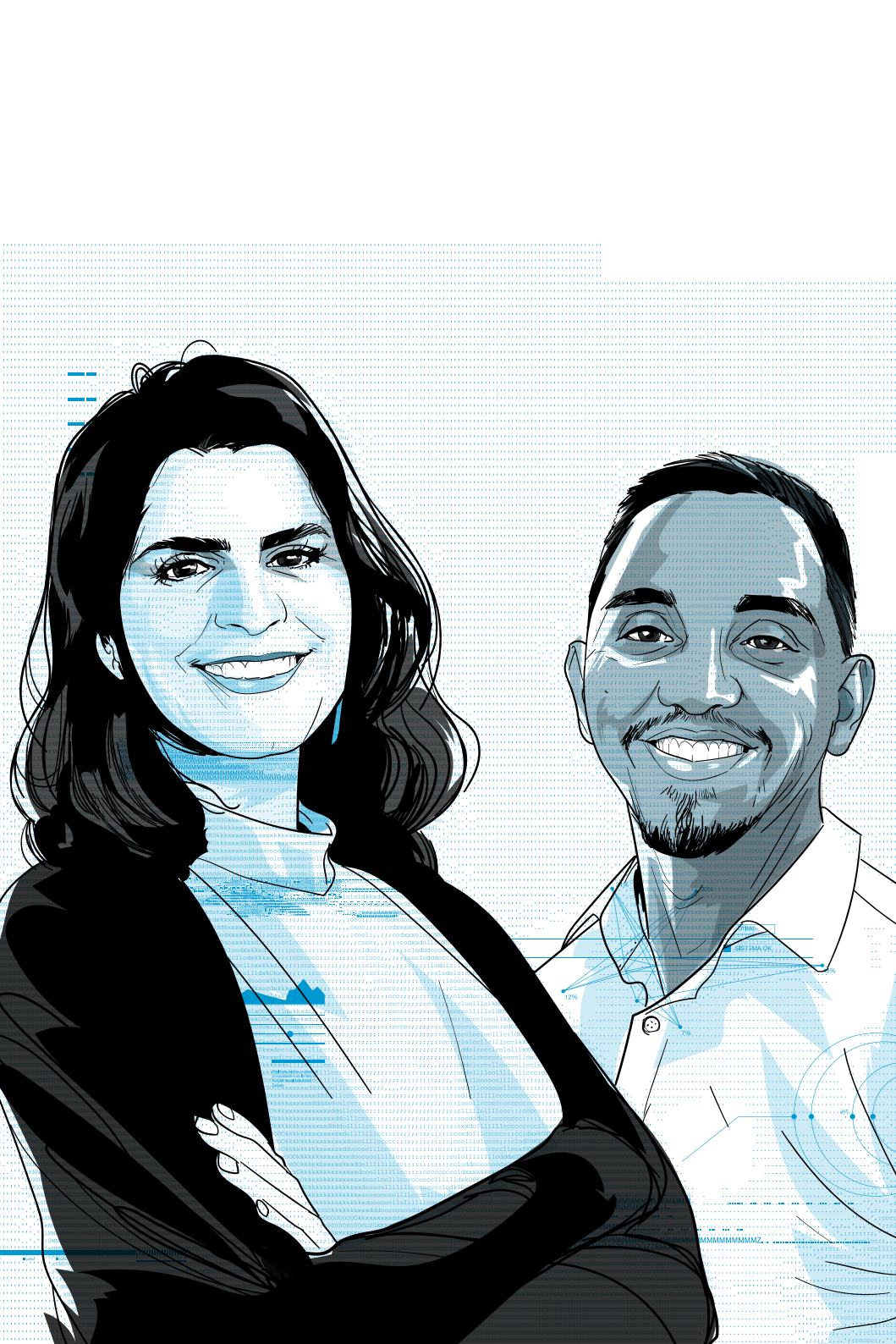
Aí surge a questão final, que para nós é muito séria também, que é a criação de arcabouços tecnológicos pelo Estado que se

prestam aos vigilantismo. A criação de mecanismos de vigilância social, a pretexto do combate ao crime. Grupos vulneráveis, grupos políticos, grupos dissidentes - no sentido de uma dissidência intelectual com relação à forma como o Estado tem se organizado - podem passar a ser alvo de investigações com esse pretexto, de uma forma indeterminada. Imagine se a polícia resolve determinar, a pretexto de combater o terrorismo, a quebra de sigilo sobre a pesquisa de alguns conceitos e termos que poderiam ser utilizados e um pesquisador, que faça pesquisa sobre esses temas, também estaria sendo desprotegido naquele momento. Podemos criar várias outras hipóteses a respeito de como isso poderia ter um destino abusivo.

Enfim, sem me alongar mais, é necessário ter em conta que essa investigação é, sim, necessária, no sentido de descobrir quem é o autor mediato deste delito. Não obstante, não podemos, com isso, sacrificar direitos de uma quantidade indeterminada de pessoas. E é com isso que eu finalizo. Obrigada.

NOTAS

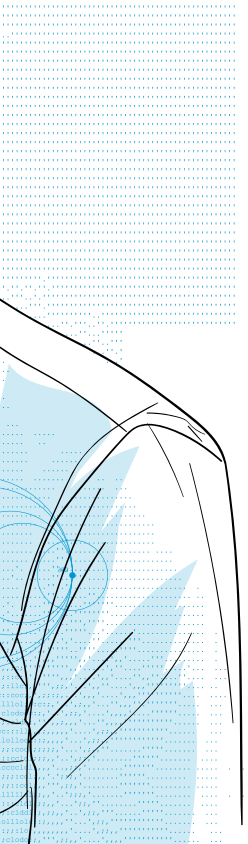
1. Este artigo foi adaptado a partir de uma palestra realizada no VI Congresso Direitos Fundamentais e Processo Penal na era digital, promovido pelo InternetLab em agosto de 2022.



12.

O ACESSO A DADOS DE GEOLOCALIZAÇÃO DE PESSOAS INDEFINIDAS: UMA ANÁLISE SOBRE A PRÁTICA DE BUSCA REVERSA[1]

Bárbara Simão e Vitor Vilanova



Hoje, os dispositivos eletrônicos utilizados por uma pessoa ao caminhar na rua - sejam telefones celulares, computadores pessoais, ou ferramentas vestíveis como *smartwatches* — são capazes de oferecer informações com precisão razoável sobre a localidade em que se esteve durante determinado período de tempo. A obtenção do dado de geolocalização, assim, tem sido considerada valiosa por agentes de investigação para determinar se pessoas estiveram presentes na região em que um crime ocorreu.

A prática consiste na "busca reversa" a partir de dados de geolocalização em investigações criminais. Isto é: quando pedidos genéricos, sem definição de suspeitos, são feitos por órgãos de investigação em relação a um determinado espaço geográfico em que um crime ocorreu, verificando quais dispositivos eletrônicos – e, consequentemente, pessoas – estavam presentes naquele local, em um determinado espaço de tempo. Embora tenha se tornado um método recorrente no âmbito de investigações criminais, a prática levanta dúvidas importantes em torno de sua legalidade e constitucionalidade, por impactar severamente os direitos à privacidade de pessoas atingidas pela medida.

Na busca reversa, são obtidas informações sobre a localização de um conjunto indeterminado de indivíduos em um determinado momento. Isso pode ser feito por meio de diversas fontes, como redes Wi-Fi, torres de celular, sensores GPS e Bluetooth. Com base nesses dados, é possível traçar um perfil de movimentação de uma pessoa, identificar lugares frequentados e estabelecer conexões entre suspeitos e eventos criminais. A prática, por consequência, pode afetar pessoas que não tenham qualquer relação com o crime investigado, o que se questiona com relação à proteção constitucional garantida à intimidade e vida privada das cidadãs/ãos, uma vez que dados de geolocalização podem exprimir hábitos de vida, consumo, e padrões de comportamento.

Neste artigo, iremos abordar os aspectos legais e constitucionais envolvidos na prática da busca reversa de dados de geolocalização. Em um primeiro momento, serão examinadas as legislações pertinentes à obtenção de dados de geolocalização no contexto do processo penal brasileiro, como o Código de Processo Penal e a Lei de Interceptação Telefônica, além do Marco Civil da Internet e a Lei Geral de Proteção de Dados. Na sequência, serão explorados os limites impostos pelo direito constitucional à privacidade e à intimidade, bem como as garantias processuais fundamentais, como o direito à presunção de inocência e à vedação à autoincriminação compulsória.

A BUSCA REVERSA A PARTIR DE DADOS DE GEOLOCALIZAÇÃO

Os mandados de coleta de dados de localização via "busca reversa" envolvem técnicas de investigação utilizadas para tentar identificar um suspeito. A forma tradicional desse método se refere à busca de dados de localização a partir de alguém. Ou seja, tem-se o indivíduo, sobre o qual recai uma quebra de sigilo de seus dados de localização (BROCK, 2023, p. 667). A busca reversa visa descobrir, em determinado espaço e horário, quais pessoas estavam presentes em um determinado local. Assim, no método tradicional, parte-se da pessoa e chega-se no lugar, enquanto na busca reversa parte-se do lugar para se chegar à(s) pessoa(s).

Ou seja, os dados de localização de todos os dispositivos que se encontravam em determinada área geográfica durante um período específico são solicitados.[2] Aparelhos móveis como smartphones, computadores e tablets conectam-se a redes WiFi ou às Estações Rádio Base para que possam acessar à internet ou à rede telefônica, e a localização física de tais pontos de acesso, conjuntamente com o acesso a novos pontos, mais

próximos, quando da movimentação do usuário, permitem que se estime sua localização ao longo do tempo. Dispositivos móveis possuem, ainda, outros sensores capazes de estimar a sua localização, como GPS e Bluetooth.

Frequentemente, requisitam-se também dados identificadores dos referidos aparelhos, tal como IMEIs, nome de titulares, contas de e-mail e até senhas de acesso aos celulares. A técnica permite que as autoridades policiais examinem os dados pessoais de diversos indivíduos não relacionados ao crime para, então, tentar identificar dispositivos que possam ter relação com a investigação. A busca reversa tem como objetivo, portanto, encontrar alguém, a pessoa alvo de uma investigação, por meio de uma determinada região geográfica.

Há, no entanto, um problema significativo com o método: em geral, outras pessoas que não tenham qualquer relação com o crime investigado estarão na mesma região e horário aproximado. Sendo assim, a técnica inevitavelmente pode gerar quebra de sigilo de dados de pessoas que não tenham relação com os fatos investigados. Em prol da eficiência da investigação, há riscos de invasão à privacidade das/os detentoras/es dos dispositivos rastreados. Ordens genéricas de quebra de sigilo de dados telemáticos por geolocalização abrangem um conjunto não identificado de pessoas, contra as quais não há qualquer indício de envolvimento em crime e que estão unidas tão somente pela circunstância aleatória de terem transitado, em certo lapso de tempo, por certas localidades (SAKAMOTO, 2023, p. 14).

Trata-se de uma forma de "fishing *expedition*", prática empregada quando os investigadores pesquisam informações, sem causa prévia e sem finalidade específica, sobre um alvo. A prática, portanto, se aplica a qualquer processo de obtenção de provas que não derivou de uma informação prévia na investigação e/ou que não delimita um alvo específico.

Assim, inevitavelmente a aplicação da busca reversa vai de encontro ao direito à privacidade. Embora parte da doutrina argumente que a violação da privacidade, nesses casos, seria justificada pelo interesse público na eficiência da investigação criminal (MAIA e PAULINO, 2020, p. 775), questiona-se quanto a medida pode equilibrar-se com direitos fundamentais, considerando-se a falta de individualização de suspeitos em sua aplicação.

Nos EUA, casos relacionados têm sido discutidos sob a aplicação da 4ª Emenda da Constituição do país. A 4ª Emenda visa evitar a violação desnecessária da privacidade das/os cidadãs/ãos por parte das autoridades públicas, estabelecendo medidas de proteção que incluem: i. prevenir o uso arbitrário do poder policial; ii. restringir a extensão exagerada de uma busca inicialmente justificada; iii. salvaguardar os direitos constitucionalmente protegidos contra intrusões; iv. minimizar a exposição a informações sensíveis; e v. proteger contra possíveis danos físicos causados por agentes policiais (FERGUSON, 2023, p. 5). De acordo com Owsley (2022, p. 883-4), a ausência de justificativa e "causa provável" (*probable cause*) para a emissão dos *geofence warrants* resulta em sua potencial inconstitucionalidade, em confronto com as exigências estabelecidas pela 4ª Emenda. Isso por serem naturalmente mais abrangentes, uma vez que identificam indivíduos criminalmente apenas com base em sua proximidade geográfica a um local de crime (BROCK, 2023, p. 673), o que os colocaria em situação similar à dos mandados genéricos, que também são considerados inconstitucionais (Idem, p. 682).

O caso *United States v. Chatrie*[3] emerge como exemplo desse debate. Neste caso, as autoridades policiais utilizaram um mandado *geofence* para solicitar ao Google informações sobre dispositivos móveis localizados em um raio específico próximo a uma cena de crime (OWSLEY, 2022, p. 852). A corte

distrital aprovou os pedidos de quebra feitas pelas autoridades policiais, sugerindo que a doutrina da 4ª Emenda poderia não estar adequadamente adaptada às rápidas transformações tecnológicas (BROCK, 2023, p. 684). Por sua vez, a juíza federal Hannah Lauck reconheceu a inconstitucionalidade da utilização do mandado, mas concluiu que as provas obtidas não deveriam ser anuladas devido à existência de boa-fé em sua obtenção (OWSLEY, 2022, p. 852). Conforme a decisão:

> As autoridades policiais tentaram justificar o mandado alegando que uma busca tão abrangente "poderia levar à identificação de testemunhas potenciais e/ou suspeitos". Mesmo que este Tribunal assumisse que um mandado seria justificado com base no fato de que uma busca poderia revelar testemunhas (algumas das quais já tinham sido entrevistadas) em vez de perpetradores, o Mandado de Geofence está completamente desprovido de qualquer sugestão de que todas - ou mesmo a maioria - das pessoas investigadas tenham participado ou testemunhado o crime. É certo que poderia existir uma probabilidade razoável de que o Mandado de Geofence revelasse informações sobre a localização do suspeito. No entanto, o mandado, em sua essência, também abrangeu dados de localização irrestritos de cidadãos privados que não tinham motivo para serem submetidos ao escrutínio governamental.[4]

No próximo tópico, iremos avaliar as possibilidades de obtenção de dados de geolocalização de acordo com o ordenamento jurídico brasileiro, examinando a compatibilidade dos mandados sem especificação de suspeitos com os direitos e princípios previstos na Constituição Federal e nas legislações infraconstitucionais.

/ [A BUSCA REVERSA] INEVITAVELMENTE PODE GERAR QUEBRA DE SIGILO DE DADOS DE PESSOAS QUE NÃO TENHAM RELAÇÃO COM OS FATOS INVESTIGADOS /

/ QUANTO
MAIS INVASIVA
A SOLICITAÇÃO
[...], MAIOR
DEVE SER A
SUSPEITA SOBRE
O INDIVÍDUO
INVESTIGADO
OU A GRAVIDADE
DO CRIME /

AS POSSIBILIDADES DE OBTENÇÃO DE DADOS DE GEOLOCALIZAÇÃO NO ÂMBITO DO PROCESSO PENAL BRASILEIRO

O Direito brasileiro conhece diferentes e específicas maneiras para acesso a dados pessoais por autoridades públicas para fins de investigações criminais. A Lei das Interceptações Telefônicas (LIT) autoriza a quebra de sigilo e "interceptação do fluxo de comunicações em sistemas de informática e telemática" em determinadas hipóteses, proibindo-a caso não haja "indícios razoáveis de autoria ou participação em infração penal" (Art. 2, I, LIT). Já o Código de Processo Penal (CPP) admite buscas pessoais apenas mediante fundada suspeita de que alguém oculte consigo arma proibida ou material que constitua corpo delito (art. 240, §2º). Isto é: a abordagem policial sobre pessoas que simplesmente transitam em ruas ou estão em certos lugares apenas pode ocorrer mediante justa causa.

Em seu art. 13-B, o CPP estabelece ainda que "se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso", prescindindo da autorização judicial, conforme §4º desse mesmo artigo, caso não haja manifestação judicial dentro de 12 horas.

Em suma, no caso previsto no CPP, existe a possibilidade de obtenção de dados de localização referentes a crime de tráfico de pessoas em curso, de forma que se permita a localização da vítima e dos suspeitos, e, no caso da LIT, a possibilidade de interceptação de comunicações em determinados casos, contanto que haja indícios razoáveis de autoria do crime que se quer investigar.

O Marco Civil da Internet (MCI), por sua vez, estabelece mecanismos para acessos a dados cadastrais e registros de IP. Seu art. 10, *caput*, estabelece que a disponibilização de dados pessoais associados a comunicações deve atender à preservação da intimidade e da vida privada das partes envolvidas. Neste sentido, o Decreto nº 8.771/2016, que regulamenta o Marco Civil, explicita a proibição de pedidos coletivos "genéricos ou inespecíficos" de dados cadastrais (art. 11, § 3º). Vê-se, assim, que em nenhum momento se planejou conferir uma prerrogativa ampla de acesso a qualquer dado no MCI, muito menos de coletividades de pessoas; pelo contrário: a proteção da privacidade na internet e através de aplicações é um dos pilares fundamentais da legislação.

Essas maneiras de obtenção de dados devem ainda ser vistas em conjunto com outros diplomas infraconstitucionais que tocam a matéria e que buscam conter novos tipos de ameaças decorrentes do processamento, compartilhamento e gerenciamento de bases de dados pessoais. A despeito de o regime estabelecido pela Lei Geral de Proteção de Dados (LGPD) não se aplicar em sua integralidade ao processamento de dados pessoais para fins de segurança pública (Art. 4º, III, a, LGPD), impõe, também para essa finalidade, a aplicação de seus princípios e os direitos dos titulares de dados previstos na referida lei (Art. 4º, §1º, LGPD), bem como admite requisição de relatório de impacto à proteção de dados (Art. 4º, §3º, LGPD). O direito à proteção de dados pessoais possui também fundamento constitucional - instituído pela Emenda Constitucional nº 115, de 2022 -, de onde já decorre diretamente sua eficácia, inclusive no campo penal. Não se podem afastar, assim, de nenhuma maneira, princípios como a proporcionalidade, adequação, necessidade, transparência etc., inclusive nas atividades voltadas à segurança pública e a investigações criminais.

Vale frisar que os dados de geolocalização são particularmente sensíveis entre os dados associados às comunicações se comparados aos dados cadastrais e aos registros diretamente citados no art. 22 do Marco Civil, que, em geral e de forma agregada, possuem o potencial de revelar aspectos relevantes do comportamento, relacionamentos e preferências de uma pessoa. Em análise sistemática com outros diplomas infraconstitucionais, com o paradigma constitucional e com compromissos assumidos pelo Brasil no âmbito da proteção de direitos humanos, deve-se interpretar tais formas de obtenção de dados à luz da vedação de pedidos genéricos, do princípio da necessidade no tratamento de dados pessoais, segundo o qual somente os dados efetivamente necessários para determinada finalidade podem ser utilizados, o princípio da proporcionalidade, dentre outros relevantes. Ressalte-se que o Marco Civil da Internet deixa claro a proteção de dados pessoais, na forma da lei, como um de seus princípios no art. 3º, III, em complemento à proteção à privacidade.

O DIREITO À PRESUNÇÃO DE INOCÊNCIA E A VEDAÇÃO À AUTOINCRIMINAÇÃO COMPULSÓRIA

Uma análise cuidadosa deve ser exercida ao serem sopesados os direitos fundamentais em jogo. Quanto mais invasiva a solicitação em relação à privacidade, maior deve ser a suspeita sobre o indivíduo investigado ou a gravidade do crime, em conformidade com a proteção constitucional à privacidade. Além disso, em respeito à presunção de inocência, a autoridade policial deve ser capaz de comprovar uma suspeita razoável em relação à pessoa cujos dados serão coletados.

Nos casos de busca reversa, o acesso aos dados pessoais ocorre para determinar quem será o suspeito, o que inverte

esse sistema. Não há previsão legal quanto à possibilidade de que pessoas estejam sujeitas a abordagens e inquirições apenas porque seu dispositivo celular informa que habitam, trabalham, estudam ou de qualquer outro modo transitaram em certa localidade. Tampouco, que isso as torne pessoas de interesse em investigação, expostas a ter seu sigilo levantado de forma oculta, sem oportunidade de defesa ou ciência.

Pode-se considerar também que o acesso indiscriminado aos dados de inúmeras pessoas não relacionadas ao crime investigado constituiria violação à presunção de inocência. Isso, principalmente, porque as pessoas alvo da medida não têm conhecimento da coleta de dados em andamento e, portanto, podem inadvertidamente produzir provas contra si mesmas. Lembrando que, de acordo com o Código de Processo Penal e a Lei de Interceptações Telefônicas, toda interceptação, requisição, compartilhamento e quebra de sigilo de dados deve ter fundamentação clara, respeitando tanto a letra da lei quanto a justificativa que resulta de um equilíbrio efetivo entre o interesse público na investigação criminal e os sensíveis riscos que se apresentam aos direitos e liberdades fundamentais da pessoa titular dos dados pessoais.

Além disso, vale ressaltar que o Brasil aderiu à Convenção Americana sobre Direitos Humanos, conhecida como Pacto de São José da Costa Rica, e ao Pacto Internacional de Direitos Civis e Políticos (PIDCP) – tratados que proíbem a autoincriminação compulsória. Ambos os tratados também garantem defesa contra interferências arbitrárias e abusivas na vida privada.[5] Essa proteção abrange não apenas as comunicações privadas, mas também os dados relacionados a essas comunicações, como informações de geolocalização e outros dados utilizados para identificar dispositivos, que podem ser solicitados às operadoras de telefonia móvel ou provedores de aplicativos de Internet.

A privacidade, ainda, é porta de entrada para o exercício de outros direitos, especialmente a liberdade de opinião e expressão,[6] o que também se aplica à proteção de dados pessoais. Por exemplo, houve casos de realização de "buscas reversas" para identificar pessoas no contexto de protestos sociais. Em maio de 2020, durante as manifestações em reação ao assassinato de George Floyd nos EUA, a polícia de Minneapolis acessou informações de todas as pessoas próximas a uma loja que foi vandalizada em 27 de maio.[7] De fato, os dados de geolocalização são reveladores em sua relação com a divulgação de informações sensíveis associadas ao exercício de outros direitos humanos e fundamentais. Além dos direitos de associação e reunião, eles podem inferir informações sobre religião, orientação sexual, estado de saúde, entre outros.

Essa interpretação é necessária ao se analisar a profunda intimidade relacionada aos dados de localização, bem como o fato de que os pedidos de geolocalização raramente se limitam apenas aos dados de localização. Com a ubiquidade e o uso constante de dispositivos móveis, especialmente smartphones, o rastro contínuo de informações pessoais deixado pelo seu uso pode revelar aspectos íntimos da identidade digital de sua/eu proprietária/o, desde sua residência até seus hábitos, renda, pessoas com quem interage, etc. Portanto, é de suma importância que seja garantida a proteção ao acesso aos dados gerados nessas situações, sem que se abra mão de avaliação cuidadosa das garantias e proteções fundamentais do Estado de Direito diante da necessidade pública de investigação criminal.

O TEMA NO SUPREMO TRIBUNAL FEDERAL

No Brasil, discussões acerca da busca reversa também têm chegado aos tribunais. Em decisões recentes do Superior Tribunal de Justiça, tem sido recorrente o entendimento de que o Marco Civil

da Internet não exige individualização das pessoas alcançadas na decisão que requisita dados armazenados em provedores de internet. É o caso do Recurso em Mandado de Segurança nº 59716 - RS (2018/0342755-1), do Recurso em Mandado de Segurança nº 65242 - SP (2020/0325548-2) e do Recurso em Mandado de Segurança nº 61.302-RJ. Apesar disso, trata-se de medida restritiva a direitos fundamentais, com pontos que devem ser melhor debatidos à luz da Constituição Federal (SMANIO, 2021).

Recentemente, o Supremo Tribunal Federal admitiu a Repercussão Geral do Recurso Extraordinário 1.301.250 (Tema 1.148). Nesse caso, com o intuito de se investigar a morte da vereadora Marielle Franco e seu motorista Anderson Gomes, autoridades de investigação solicitaram a quebra de sigilo de dados telemáticos de um número indefinido de pessoas que tenham pesquisado, num período de cinco dias, por termos como "Marielle Franco", "Agenda Marielle Franco", "Rua dos Inválidos", e "Casa das Pretas" na plataforma do Google. Trata-se de pedido que foge ao escopo de "dado de geolocalização", abrangendo pesquisas feitas por usuárias/os na plataforma de busca. No entanto, o caso estabelecerá precedente importante sobre o acesso a dados de pessoas indefinidas, sem especificação de suspeitos, no processo penal.

Até esse momento, o STF se debruçou sobre o tema de maneira lateral, em poucas ocasiões. Em pesquisa em que filtramos casos analisados pelo Supremo,[8] foram encontrados 11 casos em que o tema tenha sido tangenciado pela Corte. Além disso, chama atenção como a discussão é recente. Não foram encontrados casos antes de 2019, sendo o primeiro referente a fevereiro de 2019. Já os temas específicos de cada decisão variaram dentre os seguintes: quebra de sigilo de dados, nulidade de prova, busca genérica, encontro fortuito, além de assuntos correlatos.

Em um dos casos, o Mandado de Segurança nº 38.061, o ministro Ricardo Lewandowski argumenta que o tema da quebra de sigilo de dados de geolocalização ainda seria objeto de debate no, aqui já referido, RE 1.301.250 RG/RJ, de relatoria da Ministra Rosa Weber. Assim, a constitucionalidade das medidas ainda estaria sujeita ao escrutínio definitivo do STF, o que o impediria de julgar sobre o tema nesse momento.

Em outro grupo de decisões, os temas debatidos eram a ocorrência de "buscas genéricas" e a possível prática de "*fishing expedition*". Os ministros, de maneira geral, rechaçam a prática. Seja afastando a tese de que houve *fishing expedition* em determina ação de autoridade pública (HC 181.719 AgR), exigindo controle judicial prévio, de modo a evitar a prática (HC 163.461), ou considerando a ilegalidade de buscas por consistirem *fishing expedition* (Rcl 43.479). Em outra decisão (RHC 219.193), do ministro Luiz Fux, é afastada a ideia de que houve *fishing expedition* com base na argumentação de que na verdade se tratava de "encontro fortuito de prova", sendo a busca, portanto, legal. Já quando o Tribunal considerou que houve a prática de *fishing expedition*, decidiu pela nulidade das provas, como no caso do *Habeas Corpus* nº 201.965, de relatoria do ministro Gilmar Mendes.

Há, no entanto, dois casos dentre os pesquisados que chamaram a atenção por serem ambos pedidos de quebra de sigilo de dados de localização feitos pela própria defesa do acusado. Como temos aqui um indivíduo, não se tratam de casos em que houve solicitação de dados de pessoas indefinidas. Em vez disso, a pessoa solicita o acesso a seus dados como manobra de defesa.

O primeiro desses casos é a Reclamação nº 57.683. O caso aborda a possível violação da Súmula Vinculante nº 14 do Supremo Tribunal Federal, que prevê o direito do defensor de

ter acesso a todos elementos de provas em um procedimento investigatório. O defensor, aqui, peticiona para que seja disponibilizado acesso à íntegra das provas digitais coletadas pela autoridade acusatória e argumenta que seria "importante registrar que ao analisar a prova digital será provado através da geolocalização do aparelho celular que o acusado não estava na cena do crime, prova esta crucial até mesmo para o Juiz não condenar um inocente". Teria-se, aqui, portanto, uma utilização pró-defesa do dado de geolocalização. O ministro Alexandre de Moraes, por sua vez, negou provimento ao pedido por compreender que o caso não se tratava de recusa ao direito de acesso a provas, mas um pedido para rever a análise de um requerimento de produção de provas.

Do mesmo modo, no HC nº 222.949, também de relatoria do ministro Alexandre de Moraes, houve indeferimento do pedido, feito pela defesa, de acesso a dados de localização do réu. O caso tratava de suposta falta grave cometida por reeducando. A defesa solicitou a intimação do Google para que a empresa fornecesse os dados de localização do reeducando no período em que ele supostamente teria cometido a falta grave. A solicitação se contrapõe ao método baseado no testemunho de agentes públicos - os policiais que teriam ido na casa do reeducando durante sua saída temporária e não o teriam encontrado. Em todas as instâncias e tribunais, nesse caso, o entendimento foi de que o "novo" método de obtenção dos dados como fonte de prova seria desnecessário, uma vez que os testemunhos, imbuídos de fé pública, seriam provas suficientes da determinação da localização do réu.

Os argumentos utilizados em ambos os casos revelam a dificuldade de que o acesso aos dados seja mobilizado pela defesa da parte ré no âmbito de uma acusação. Embora o escopo desses achados não permita a conclusão definitiva a respeito,

espera-se que o Tribunal, à luz do princípio do contraditório e da ampla defesa, também evite assimetrias ao considerar o acesso a dados apenas como prerrogativa de órgãos de investigação, passando a largo dos casos em que poderia ser mobilizado como estratégia de defesa.[9]

CONSIDERAÇÕES FINAIS

A prática da busca reversa de dados de geolocalização em investigações criminais tem suscitado debates acerca de sua legalidade e implicações. Trata-se de situação com claros riscos de invasão à privacidade dos detentores dos dispositivos rastreados. Sendo o celular o ponto focal da vida moderna, onde toda atividade encontra algum rastro – das mais íntimas às mais profissionais, especial cuidado deve ser tomado com as possibilidades de acesso a suas informações por agentes estatais, em especial sem a ciência do atingido.

No contexto jurídico brasileiro, espera-se que essa questão seja abordada com base nos limites processuais penais e nas garantias constitucionais estabelecidas. É necessário estabelecer critérios objetivos para determinar quando o acesso a dados de geolocalização é admissível, levando em consideração a gravidade do crime em questão e a existência de suspeitas razoáveis em relação aos indivíduos envolvidos.

Além disso, é fundamental que sejam estabelecidas salvaguardas adequadas para evitar o acesso indiscriminado aos dados de geolocalização de pessoas não relacionadas ao crime investigado. A coleta e a utilização dessas informações devem ser realizadas com base em fundamentação sólida, exigindo-se uma justificativa clara e detalhada que demonstre a necessidade e a proporcionalidade da medida, assim como a delimitação de suspeitos que sejam alvo da prática.

NOTAS

1. Este artigo foi elaborado com base em tese institucional elaborada pelo InternetLab e pela Electronic Frontier Foundation para apreciação das Defensorias Públicas dos Estados de São Paulo e do Rio de Janeiro. Agradecemos especialmente a Veridiana Alimonti pela colaboração neste tema.

2. Em inglês, chama-se esse tipo de mandado de "geofence warrant", considerando-se que geofence seria um perímetro virtualmente definido ao redor de um certo ponto no globo terrestre, uma espécie de "cerca virtual" (MAIA e PAULINO, 2020, p. 770). Um Geofence warrant é, portanto, um mandado de quebra de dados referentes a determinado geofence. Pela similaridade, muitas vezes os geofence warrants são referidos como mandados de busca reversa (BROCK, 2023, p. 652).

3. United States v. Chatrie. Disponível em: https://www.rcfp.org/briefs-comments/united-states-v-chatrie/.

4. Idem.

5. Cf. Art. 11.2 do Pacto de São José da Costa Rica: "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação", e Art. 17 do PIDCP: "Ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação. Toda a pessoa tem direito a proteção da lei contra essas ingerências ou esses ataques"

6. Ver resolução 68/167 da Assembleia Geral, A/HRC/13/37 e resolução 20/8 do Conselho de Direitos Humanos

7. https://bit.ly/3JtJdSz

8. A pesquisa foi feita em maio de 2023. Os termos utilizados como chave de pesquisa foram "geolocalização", "busca reversa" e "fishing expedition", além de outras chaves que não foram frutíferas, como "geofence warrant", ou combinações das chaves que resultaram nos mesmos casos. O resultado foi de 44 casos.Os casos foram filtrados com base em sua pertinência ou não ao tema do presente artigo. O resultado final para a análise foi de 11 casos.

9. Nesse sentido, ver WEXLER, Rebecca. Assimetrias de Privacidade. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara(eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. V. SãoPaulo. InternetLab, 2022.

BIBLIOGRAFIA

BROCK, Matthew L. **"If You Build It, They Will Come": Reverse Location Searches, Data Collection, and The Fourth Amendment**. University of Richmond Law Review, v. 57, 2023, pp. 650-682. Disponível em: https://shre.ink/9PKy.

MAIA, Tiago Dias; PAULINO, Galtiênio da Cruz. **A quebra de sigilo de dados baseada em coordenadas geográficas e o princípio da proporcionalidade** *in* **Direitos fundamentais em processo: estudos em comemoração aos 20 anos da Escola Superior do Ministério Público da União**. Escola Superior do Ministério Público da União, Brasília, 2020, pp. 769-788.

FERGUSON, Andrew Guthrie. **Digital Rummaging**. Washington University Law Review, v. 101, n. 5, 2023. Disponível em SSRN: https://ssrn.com/abstract=4377633 ou https://shre.ink/lezDOWSLEY, Brian L. **The best offense is a good defense: fourth amendment implications of geofence warrants**. Hofstra Law Review, v. 50:813, 2022, pp. 829-894. Disponível em: https://shre.ink/leA2

SAKAMOTO, Maria Laura Grisi. **A constitucionalidade das ordens judiciais de quebra de sigilo telemáticos, de um conjunto não identificado de pessoas, por geolocalização à luz dos direitos à privacidade de intimidade**. Revista Foco, Curitiba, v. 16, n. 1, 2023, pp. 01-43. Disponível em: https://shre.ink/leAV.

SMANIO, Gianluca Martins. **A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ**. Revista Brasileira de Ciências Criminais, Brasília, v. 12, n. 5, mai/ago, 2021, pp. 49-76. Disponível em: https://shre.ink/9PK8.

ESTE LIVRO FOI COMPOSTO COM AS FAMÍLIAS TIPOGRÁFICAS *DECIMA MONO* E *FF META*. PARA O MIOLO FOI UTILIZADO O PAPEL OPALINA ENVENGLOW DIAMON 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*. FORAM IMPRESSAS 250 CÓPIAS PELA *GFK COMUNICAÇÃO* EM 2023.