DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.4 >

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / CAROLINA RICARDO / DIOGO MALAN / ELOÍSA MACHADO / FERNANDA TEIXEIRA SOUZA DOMINGOS / GUSTAVO BADARÓ / JAQUELINE ABREU / MAURÍCIO DIETER / MELISSA GARCIA BLAGITZ DE ABREU E SILVA / NEIDE MARA CARDOSO DE OLIVEIRA / ORLANDINO GLEIZER / SARAH LAGESON / TERCIO SAMPAIO FERRAZ JR. / YURI LUZ

INTERNETLAB
pesquisa em direito e tecnologia

SÃO PAULO, 2021

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. IV. São Paulo. InternetLab, 2021.

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

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

Direitos fundamentais e processo penal na era digital / [editores] Bárbara Simão, Francisco Brito Cruz. 1. ed. São Paulo : InternetLab, 2021. (Doutrina e prática em debate; 4)

Vários autores.
Bibliografia.
ISBN 978-65-88385-09-8

1. Direito processual penal **2.** Direitos fundamentais **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação **I.** Simão, Bárbara. **II.** Cruz, Francisco. **III.** Série.

21-89300 **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 /

< CAROLINA RICARDO >

Advogada e socióloga. Mestre em Filosofia do Direito pela Faculdade de Direito da Universidade de São Paulo. Foi assessora de projetos no Instituto São Paulo Contra a Violência, consultora do Banco Mundial e do BID em temas de segurança pública e prevenção da violência. Foi fellow no programa Draper Hills Summer Fellows (2018) oferecido pelo CDDRL da Universidade de Stanford, CA e fellow na Residência em Capital Humano do Instituto República (2018/2019). Atualmente é Diretora Executiva do Instituto Sou da Paz.

< DIOGO MALAN >

Pós-doutor em Democracia e Direitos Humanos pela Universidade de Coimbra. Doutor em Processo Penal pela USP. Professor da UERJ e FND/UFRJ. Advogado.

< ELOÍSA MACHADO >

Professora da FGV Direito SP. Doutora em Direito e mestre em Ciências Sociais. Fundadora do Coletivo de Advocacia em Direitos Humanos – CADHu. Conselheira do Instituto Pro Bono, do Instituto Alana e do Fiquem Sabendo. Coordenadora do centro de pesquisa Supremo em Pauta FGV Direito SP. Membro da Comissão de Constitucional da Ordem dos Advogados do Brasil – SP. Ganhadora do Outstanding International Woman Lawyer Award, dado pela International Bar Association (IBA) 2018-2019.

< FERNANDA TEIXEIRA SOUZA DOMINGOS >

Procuradora da República em São Paulo. Coordenadora do Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão Criminal do MPF. Coordenadora do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo. Graduada em Direito na Universidade de São Paulo, especialista em direitos difusos e coletivos pela Escola Superior do Ministério Público/SP e em direitos humanos e trabalho pela ESMPU e mestranda em Direito Transnacional na Faculté de droit, de sciences politique et de gestion da Université de Strasbourg.

< GUSTAVO BADARÓ >

Professor Associado de Direito Processual Penal da Universidade de São Paulo, nos cursos de graduação e pós-graduação. Livre-Docente (2011), Doutor (2002) e Mestre (1998) em Direito Processual Penal pela Universidade de São Paulo. Graduado em Direito pela Universidade de São Paulo (1993). Advogado Criminalista. Membro do Instituto Ibero-americano de Direito Processual (IIDP), Instituto Brasileiro de Direito Processual (IBDP), Instituto Brasileiro de Ciências Criminais (IBCCRIM), Instituto Brasileiro de Direito Processual Penal (IBRASPP) e Instituto dos Advogados de São Paulo (IASP). É membro do Conselho Consultivo do Instituto Brasileiro de Ciências Criminais (IBCCRIM) (2013/2015) e da Diretoria do Instituto Brasileiro de Direito Processual. Membro do Conselho Científico do Centro de Estudos de Direito Penal e Processual Penal La-

tino-americano, do Instituto de Ciências Criminales, da Georg-August de Göttingen, na Alemanha. Advogado sócio do escritório Badaró Advogados.

< JAQUELINE ABREU >

Doutoranda em Direito na Faculdade de Direito da Universidade de São Paulo e advogada no Barroso Fontelles, Barcellos, Mendonça & Associados. Mestra em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Graduada em direito pela Universidade de São Paulo. Durante a graduação, foi bolsista de iniciação científica da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Programa de Estímulo ao Ensino de Graduação (PEEG) nas áreas de Filosofia e Teoria Geral do Direito e membro do Núcleo de Direito, Internet e Sociedade da USP. Realizou intercâmbio acadêmico de graduação também na LMU, período em que foi bolsista do Serviço Alemão de Intercâmbio Acadêmico (DAAD). Foi pesquisadora-júnior na FGV DIREITO SP e assistente de pesquisa visitante do Berkman Klein Center for Internet and Society da Harvard University. Participou do Summer Doctoral Programme do Oxford Internet Institute e coordenou a área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em direito e tecnologia.

< MAURÍCIO DIETER >

Professor do Departamento de Direito Penal e Criminologia da Faculdade de Direito da Universidade de São Paulo. Pós-Doutor pela Universidade do Estado do Rio de Janeiro. Mestre e Doutor pela Universidade Federal do Paraná. Professor-con-

vidado das Universidades San Carlos de Guatemala, Westminster e da Universidade Autonoma Latinoamericana, em Medellín. Coordenador do Departamento de Amicus Curiae do IBCCRIM. Advogado Criminalista.

< MELISSA GARCIA BLAGITZ DE ABREU E SILVA >

Procuradora da República em São Paulo. Membro do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo. Ex- coordenadora do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo. Graduada em direito pela Universidade de São Paulo. Mestre em Direito pela Universidade de Chicago (LL.M.).

< NEIDE MARA CAVALCANTI CARDOSO DE OLIVEIRA >

Procuradora Regional da República da Procuradoria Regional da República na 2ª Região. Procuradora Regional Eleitoral Substituta no Estado do Rio de Janeiro. Coordenadora adjunta do Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão Criminal do MPF. Graduada em Direito pela Universidade do Estado do Rio de Janeiro. Especialista em Direitos Humanos nas Relações de Trabalho pela Universidade Federal do Rio de Janeiro.

< ORLANDINO GLEIZER >

Assistente científico na Universität Würzburg, Alemanha. Doutorando pela Humboldt Universität zu Berlin, Alemanha. Mestre em Direito pela Universität Augsburg, Alemanha. Mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro, UERJ.

< SARAH LAGESON >

Professora Assistente na School of Criminal Justice at Rutgers University of Newark, em New Jersey, nos Estados Unidos. Socióloga com pesquisa em direito penal, privacidade, vigilância e tecnologia. Seu livro, Digital Punishment: Privacy, Stigma and the Harms of Data-Driven Criminal Justice, foi publicado pela Oxford University Press em junho deste ano.

< TERCIO SAMPAIO FERRAZ JR. >

Professor titular aposentado da Faculdade de Direito da USP, professor emérito da Faculdade de Direito da USP – Ribeirão Preto, Doutor em Filosofia pela Universidade de Mainz-Alemanha, Doutor em Direito pela Universidade de São Paulo, advogado militante, Procurador Geral da Fazenda Nacional (1991-93), secretário executivo do Ministério da Justiça (1990).

< YURI LUZ >

Bacharel em Direito e doutor em Direito Penal pela USP (2015), com período de pesquisa na Ludwig-Maximilians-Universität de Munique, Alemanha. É Procurador da República desde 2014, atualmente integrante da Força-Tarefa Lava Jato de São Paulo. É também pesquisador do Núcleo Direito e Democracia do Cebrap.

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).

A quarta edição do Congresso, que ocorreu online entre os dias 25 de agosto e 04 de setembro de 2020, teve como mote a proteção de dados pessoais no âmbito da segurança pública e em investigações criminais, abordando desafios que legisladores, profissionais e pesquisadores enfrentam diante do de-

senvolvimento e absorção de novas tecnologias na prevenção, repressão, processamento de delitos, e nas próprias dinâmicas de incidência criminal.

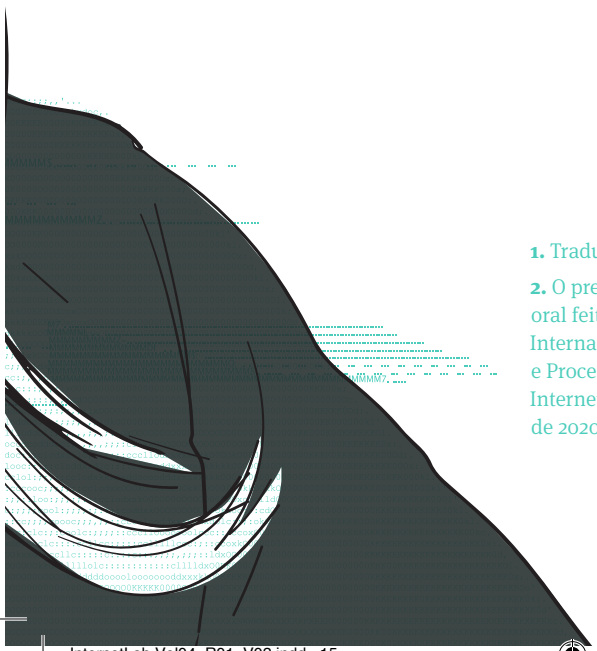
As contribuições aqui compiladas abordam o debate constitucional sobre a privacidade e a proteção de dados, o impacto de sistemas de vigilância em massa e de técnicas de big data sobre investigações e o compartilhamento de dados com agências penais. Todas elas estão também registradas em vídeo e disponíveis para acesso online. Com isso, pretendemos 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, agosto de 2021

01.

PUNIÇÃO DIGITAL[1]

Sarah Lageson[2]



1. Tradução de Flora Gil.

2. O presente texto se baseia em apresentação oral feita como Keynote Speaker do IV Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

Muito obrigada pelo generoso convite do InternetLab. É uma honra estar aqui, compartilhar meu trabalho com vocês e discutir o que está realmente se tornando um fenômeno global de uso de informação no sistema de justiça de novas maneiras, e, frequentemente, por agentes internacionais que estão expandindo o uso dessas tecnologias.

Estou aqui hoje para falar a vocês da pesquisa que fiz nos Estados Unidos sobre o fenômeno que tenho chamado de "punição digital", e minha apresentação se encaixa bem na questão mais ampla desse congresso: o que a justiça processual significa na era digital? O que a presunção de inocência e o devido processo legal significam? O que ocorre com os direitos processuais fundamentais e com os direitos de privacidade onde existem oportunidades tão vastas para que as informações pessoais sejam usadas de formas variadas por plataformas digitais?

A punição digital é uma consequência das operações legais orientadas por dados, do esforço para usar mais dados para organizar o sistema legal. Nos Estados Unidos, isso surgiu como uma combinação de leis permissivas sobre registros públicos e do sistema de encarceramento em massa. O resultado é essa permanente estigmatização e discriminação de milhões de pessoas a cada ano nos Estados Unidos, pessoas que são apenas acusadas de crimes. Um problema adicional é que, na medida em que cada órgão do sistema judiciário – a polícia, os tribunais, as penitenciárias e as prisões – expande suas práticas de coleta e disseminação de dados, muitos erros e informações incorretas começam a aparecer. Assim, esses registros desatualizados e incorretos se tornaram não só um problema interno ao sistema de justiça, mas um problema externo a ele, pois esses dados se tornaram um produto valioso no setor privado. E o que isso acaba por fazer é incentivar empresas a criar produtos de vigilância para coletar informações

pessoais, que essas mesmas empresas depois podem agregar e vender para consumidores de registros criminais.

Para ilustrar, vou compartilhar algumas anedotas do meu livro. Elas vieram de entrevistas com moradores de New Jersey, onde fiz parte de minha pesquisa. Primeiro, vou falar de Cindy, que foi presa em 2010, depois de tentar apresentar uma receita falsa em uma farmácia. Ela sofria de uma adição grave na época. O farmacêutico recusou a receita e Cindy saiu da farmácia, entrou em um carro, e se envolveu em um pequeno acidente de carro com o policial que foi chamado à cena. Foi uma situação terrível. Ela foi acusada e detida por falsificação de receita, e então foi também detida por tentativa de homicídio e lesão corporal qualificada ao policial. Quando ela foi julgada, as outras queixas foram retiradas, e ela enfim cumpriu um ano de pena pela condenação de falsificação. Todo o resto foi retirado, mas uma busca no Google por seu nome, dez anos depois, revela sua foto com as palavras "tentativa de homicídio de um agente de polícia" abaixo de sua imagem. E, estando nos Estados Unidos, ela não consegue que seus resultados de pesquisa sejam removidos do Google.

Há, também, o caso de Carl, um jovem que foi condenado por posse de arma em 2005, pelo qual ele passou dois anos em liberdade condicional. Em 2015, ele estaria legalmente apto a ter sua ficha criminal excluída, ou resguardada do conhecimento do público. Ele precisa fazer isso para manter seu emprego atual. Ele trabalha como segurança em uma escola local. Então, seus empregadores disseram: "você deve limpar seu registro para manter seu emprego". Há um erro material em um de seus registros: alguns números foram trocados e ele não pôde, por cinco anos, descobrir como resolver esse erro para possibilitar que ele conseguisse a exclusão, mesmo ele tendo passado de tribunal em tribunal no estado de New Jersey para tentar encontrar o arquivo.

Enfim, temos o caso de Alan, um pai de New Jersey que foi preso às cinco horas da manhã em sua casa por não ter comparecido ao tribunal. Após não ter comparecido a uma audiência, foi emitido um mandado de prisão e a polícia o prendeu. Ele passou o fim de semana inteiro na cadeia, apresentou-se à juíza na segunda-feira de manhã, e ela percebeu rapidamente que as intimações a comparecer ao tribunal foram enviadas ao seu endereço antigo, assim, ele nunca soube da data da audiência. Ele foi liberado da cadeia e teve seu registro criminal devidamente excluído. Sua foto de rosto, no entanto, aparece nos resultados de busca por seu nome no Google e, por conta disso, ele tem desistido de oportunidades de emprego, devido a esses resultados no Google. Ele teme que sua detenção, mesmo que tenha sido anulada, possa aparecer numa verificação de perfil de consumidor.

Assim, uma distinção importante que quero fazer é a de que a punição digital não inclui apenas o que tradicionalmente pensamos ser um registro criminal, que seria o registro de uma condenação. Ao contrário, eu argumento no livro que todo e qualquer contato com o sistema de justiça cria novas formas digitais de registro criminal, inclusive as detenções que nunca levaram a uma condenação. E acredito que isso toca o ponto central deste congresso ao pensar sobre quais são nossos direitos diante de uma condenação.

Falarei hoje sobre as características da punição digital que acho relevantes para os avanços relativos à política de dados que vemos atualmente no Brasil, explicarei os contextos social e legal que permitiram sua emergência nos Estados Unidos e, por fim, fecharei com vários pontos de discussão sobre intervenções políticas ou de pesquisa.

Depois de anos de trabalho de campo em muitos estados americanos, cheguei a quatro características centrais da punição digital. A primeira, é que ela é "desordenada". Como disse, esse tipo de estigmatização pode se estender de uma detenção poli-

cial até uma condenação; há registros públicos, como registros oficiais de tribunal, e há versões privadas desses registros que são mantidas por comerciantes de dados ou por empresas de dados pessoais. Mas processos judiciais mudam ao longo do tempo – conforme o caso passa pela justiça, os registros antigos automaticamente se tornam obsoletos. Dessa forma, quando empresas recolhem registros cruzados de fontes do governo, elas automaticamente estão recolhendo informações defasadas. Essas informações, no entanto, persistem no mercado privado e as pessoas têm pouca possibilidade de administrar esses tipos diferentes de registros. Esses registros são então mercantilizados como um produto de big data; eles são garimpados, polidos, combinados com outros registros e vendidos no mercado privado.

Esses registros são monitoráveis, portanto uma forma de se pensar sobre punição digital ou marketing digital é aquilo que Margaret Hu chama de "lista obscura de big data": isso significa que sequer é necessário ter uma suspeita razoável, como seria requerido para prender ou vigiar alguém nos Estados Unidos; agora, pode-se ter um nível bastante baixo de suspeita para rastrear alguém em um banco de dados. Isso leva a rotular pessoas como criminosas, como suspeitas ou perigosas muito antes de elas terem exibido tais comportamentos ou de terem sido legalmente condenadas por tais comportamentos. E, assim, quando esses pontos de dados são criados, eles se tornam um circuito retroalimentado de injustiça algorítmica; dessa forma, uma prisão equivocada pode entrar em seu registro e, então, justificar uma próxima prisão equivocada, simplesmente baseada no fato de que já há dados de detenção a seu respeito. O sistema todo se torna uma prisão digital retroalimentada.

Por fim, as disparidades e o racismo que vemos no sistema de justiça criminal americano são estendidos, sem dúvida, para a versão digital do sistema jurídico. Com isso quero dizer que as pessoas que têm mais probabilidade de se tornarem

alvo da polícia ou de promotores zelosos demais são frequentemente pessoas pobres, pessoas negras, ou pessoas que sofrem de adições ou de problemas de saúde mental. Então, não só é mais provável que sejam essas as pessoas a lidar com a estigmatização da punição digital, como são elas as que menos têm recursos para remediar ou para reagir à situação.

Então, podemos pensar nisso como um capital de privacidade, no sentido em que a estratificação social exacerba o capital de privacidade, e em que pessoas com menos recursos não conseguem remediar sua reputação digital.

Então, de onde vêm esses registros nos Estados Unidos? Começarei com a origem desses registros e, então, mostrarei como eles realmente aparecem na internet, como eles existem no mundo digital. Há dois tipos principais de registros que são produzidos na fase pré-condenação. Primeiro, o registro de detenção: a pessoa é detida pela polícia, seu nome é inserido no cadastro que muitos departamentos de polícia postam em seus sites. Então, membros da família, o público, ou talvez o advogado de alguém podem ver qual é sua situação de custódia. No entanto, há uma série de sites que virão rastrear os cadastros e escavar todos os dados que estão sendo publicados gratuitamente. Eles serão repostados em sites de interesse público, em mídias sociais, ou em agregadores de registros públicos, e então eles serão frequentemente indexados nos resultados de pesquisa do Google.

Os registros também vêm da fase de acusação criminal. Assim, se você for acusado judicialmente, esse registro digital fará parte de um grande banco de dados. Esses bancos de dados são comprados e vendidos no mercado privado, são mesclados com outros tipos de dados de consumo e de registros públicos, e depois são revendidos como um novo pacote de dados pessoais para a indústria de checagem de perfil.

Da perspectiva da justiça criminal, o que se vê são departamentos de polícia e tribunais trabalhando para modernizar suas

práticas de dados, apesar de terem recursos muito limitados para isso. Eles também estão tentando com bastante empenho manter o controle institucional sobre suas práticas e sobre seus dados, mas não estão desenvolvendo seus próprios softwares: eles estão contando com empresas privadas e terceiros para fazer isso por eles. Ao mesmo tempo, eles estão tentando responder às requisições da Lei da Liberdade de Informação ou aos esforços de notificação pública, mas estão progressivamente perdendo o controle sobre os dados em si. Tudo isso se torna ainda mais complicado quando se tem um esforço de síntese dos dados entre órgãos; as polícias estão tentando trabalhar com os tribunais, que estão tentando trabalhar com as condicionais, mas porque todos esses órgãos têm objetivos e atribuições diferentes, o que se tem é um ambiente de dados bastante desordenado.

O resultado é que vemos esses esforços para modernizar as operações internas da justiça criminal e para modernizar investigações por meio de abordagens orientadas por dados, mas, nesse processo, todos esses órgãos também produzem uma massiva e valiosa mercadoria de dados. E assim, é claro, isso significa que o público agora tem amplo acesso a dados arquivados, desatualizados e incorretos.

TYPE TIPO	N	%	ANNUAL ANUAL	5 – YEAR 5 ANOS
ARREST RECORD REGISTRO DE DETENÇÃO	41	82%	10.160.728	50.8 MILLION MILHÕES
BOOKING PHOTO FOTO DE PERFIL	21	42%	4.574.740	22.8 MILLION MILHÕES
COURT RECORD* REGISTRO JUDICIAL	41	82%	19.508.593	97.5 MILLION MILHÕES
PRISION INMATES PRESIDIÁRIOS	50	100%	1.316.205	–
PRISION RECORD REGISTRO DE PRISÃO	18	36%	–	6.5 MILLION MILHÕES
RAP SHEET* FICHA CRIMINAL	29	58%	–	13 MILLION MILHÕES

Essa é uma análise que fizemos sobre o número de registros criminais que o governo dos Estados Unidos coloca em sites de órgãos locais. O "N" refere-se ao número de estados americanos que publicam diferentes tipos de registros em seus sites, geralmente disponíveis sem custo algum. Mas, se pensarmos no escopo do sistema de justiça americano, no número de pessoas que são detidas e fichadas a cada ano, os números se tornam de fato surpreendentes. Assim, a cada ano, cerca de 10 milhões de registros de detenção são postos na internet pela polícia sem custo algum, e 19 milhões de registros de tribunais. Então, se multiplicarmos essas contagens anuais por um período de cinco anos, veremos quão grande esse problema pode rapidamente se tornar.

Qual é o enquadramento jurídico aqui? A primeira emenda da constituição dos Estados Unidos protege a republicação de informações obtidas de fontes acessíveis ao público. Assim, se o governo torna algo público, é perfeitamente legal que outras pessoas republiquem a informação, que gerem lucro a partir dela ou que a usem da forma que quiserem. Se um jornal quiser publicar minha foto de rosto, mesmo que eu nunca tenha sido condenada por um crime, eu não posso processar esse jornal, porque eles divulgaram legitimamente uma informação pública sobre minha detenção.

Aí também estão abarcadas as detenções que foram lacradas ou excluídas. Em um caso particular (*Martin v. Hearst Corporation*, 2015), a foto de rosto de uma pessoa aparecia em um site. Seu registro de detenção foi lacrado depois das acusações terem sido julgadas improcedentes, mas o tribunal argumentou que eles não podiam processar um site por manter a foto online. A opinião da corte era a de que, embora seja possível entrar em um tribunal e dizer ao juiz "Eu nunca fui preso" porque seu registro foi resguardado da vista pública, o jornal é legalmente autorizado a divulgar sua foto de rosto, porque ela é evidência de um

evento histórico. Dessa forma, para a corte americana, a exatidão histórica da prisão é diferente da versão legal do registro.

A regulação que efetivamente temos nos Estados Unidos cobre apenas as agências de informações de consumidores, que são agências de checagem que fazem um tipo de pesquisa que empregadores podem usar para recusar um emprego a um candidato, e que devem cumprir normas de privacidade e veracidade. A grande maioria desses sites privados, no entanto, não está na categoria de agência de informações de consumidores.

Então, como se parecem os registros criminais online? Hoje temos dúzias de sites que são considerados agregadores de registros públicos, eles se denominam "serviços de buscas por pessoas" e alegam que "não somos uma organização de proteção ao crédito, fazemos isso só por curiosidade e diversão", então é possível procurar registros criminais neles. Como podem ver, eles realmente gostam de enfatizar a quantidade de informações que eles têm. Isso realmente contribui para o medo dos americanos de ser sempre vitimizados, de que o crime está sempre virando a esquina, ainda que a criminalidade tenha caído nas últimas décadas. Isso de fato legitima a razão de existência desses sites.

Existem vários tipos de sites que usam registros criminais para a construção de perfis de reputação, que buscarão mídias sociais e outros tipos de evidência daquela pessoa na internet e as mesclarão com registros criminais. Temos uma infeliz indústria de extorsão de fotos de rosto "mugshot" nos Estados Unidos, que algumas leis estão tentando enfrentar, mas que continua existindo em muitos estados, onde um site exibe a foto de alguém e então cobra da pessoa milhares de dólares para removê-la. Esses sites fizeram dos registros criminais um *clickbait*. E agora, muitos desses sites que postam fotos de rosto oferecem o serviço de apagamento ou remoção, como

um serviço separado para tentar contornar a nova legislação e parar esse processo.

Uma grande variedade de sites informais ocupa rapidamente os resultados de buscas por pessoas no Google. E então as empresas que tentam compor a versão mais oficial disso, que fornecerão checagens de antecedentes a empregadores e senhorios, também usam a mesma retórica de "vejam quantos registros nós temos". Eles estão usando essa idéia de que registros criminais são difíceis de encontrar nos Estados Unidos porque há 50 estados com milhares de comarcas, e cada uma tem seu próprio banco de dados. Empresas privadas agregam todos esses dados para que o acesso a eles seja mais fácil.

commodified BIG data

Experian Public Records: Repository holds 600 million unique criminal records, covering 90% of the U.S. population

CoreLogic Background Data: 350 million criminal records representing defendant, alias, offense and disposition details

BackgroundChecks.com: 650 million criminal records in database

Data Diver: Criminal index contains nearly 500 million individuals, with over 2 billion criminal records ranging across 1,400+ jurisdictions.

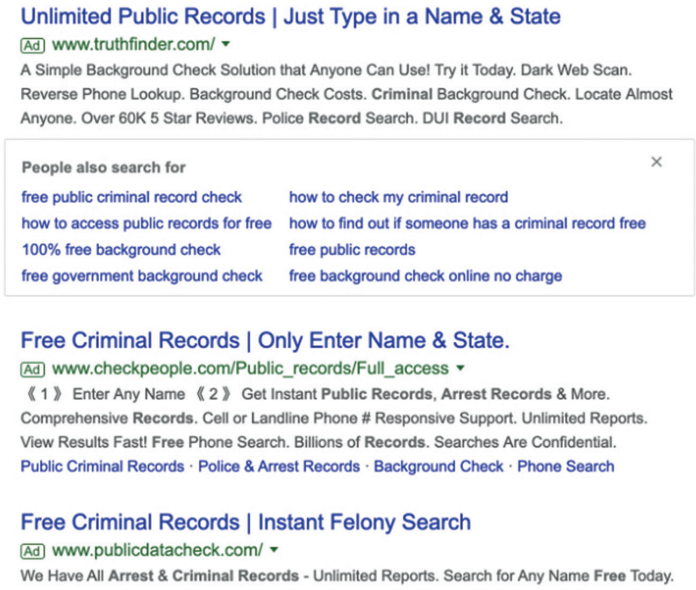
Big data comercializada

Experian Registros Públicos: Repositório contém 600 milhões de registros criminais, abrangendo 90% da população dos Estados Unidos

CoreLogic dados de antecedentes: 350 milhões de registros criminais apresentando detalhes de réu, infração e disposições

Checagem de Antecedentes: Banco de dados com 650 milhões de registros criminais

Mergulhador de dados: Index criminal contém cerca de 500 milhões de pessoas, com mais de 2 bilhões de registros criminais alcançando mais de 1.400 jurisdições



Registros públicos ilimitados | Apenas digite nome e estado
Uma solução simples de checagem de antecedentes que todos podem usar! Tente hoje. Varredura de Dark Web. Busca reversa por telefone. Checagem de antecedentes. Localize quase qualquer pessoa. Mais de 60 mil avaliações de 5 estrelas. Busca por registro policial. Busca por registro de motorista alcoolizado.

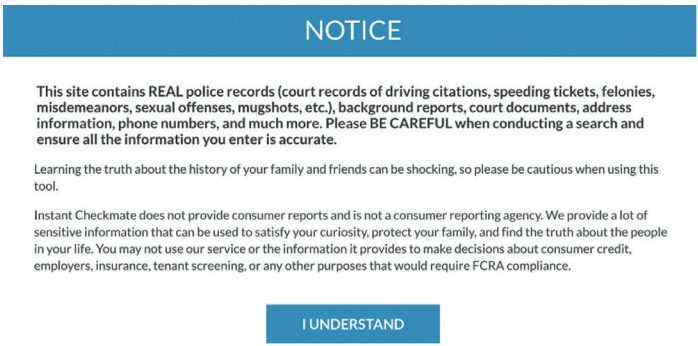
Pessoas também buscaram
Checagem de registro criminal público e gratuito
Como acessar registros gratuitamente
Checagem de antecedentes 100% gratuita
Checagem de antecedentes no governo gratuita
Como checar meu registro criminal
Como descobrir se alguém tem registro criminal gratuitamente
Registros públicos grátis
Registros públicos grátis sem custo

Registros públicos grátis. Apenas insira nome e estado.
< 1 > Insira qualquer nome < 2 > Receba instantaneamente registros públicos, registros de detenção e mais.

Registros abrangentes. Telefone celular ou fixo. Suporte atencioso. Relatórios ilimitados. Veja resultados rápido! Busca gratuita por telefones. Bilhões de registros. Buscas confidenciais.

Registros criminais gratuitos | Busca instantânea por delitos.

Temos todos os registros de detenções e crimes. Relatórios ilimitados. Busque por qualquer nome agora gratuitamente.


NOTICE

This site contains REAL police records (court records of driving citations, speeding tickets, felonies, misdemeanors, sexual offenses, mugshots, etc.), background reports, court documents, address information, phone numbers, and much more. Please BE CAREFUL when conducting a search and ensure all the information you enter is accurate.

Learning the truth about the history of your family and friends can be shocking, so please be cautious when using this tool.

Instant Checkmate does not provide consumer reports and is not a consumer reporting agency. We provide a lot of sensitive information that can be used to satisfy your curiosity, protect your family, and find the truth about the people in your life. You may not use our service or the information it provides to make decisions about consumer credit, employers, insurance, tenant screening, or any other purposes that would require FCRA compliance.

I UNDERSTAND

Advertência

Esse site contém registros policiais reais (registros jurídicos de autuações de trânsito, multas de velocidade, delitos, contravenções, agressões sexuais, fotos de rosto, etc.), relatório de antecedentes, informações sobre endereços, números de telefone, e muito mais. Por favor, TENHA CUIDADO quando realizar uma busca e certifique-se de que toda a informação inserida está correta.

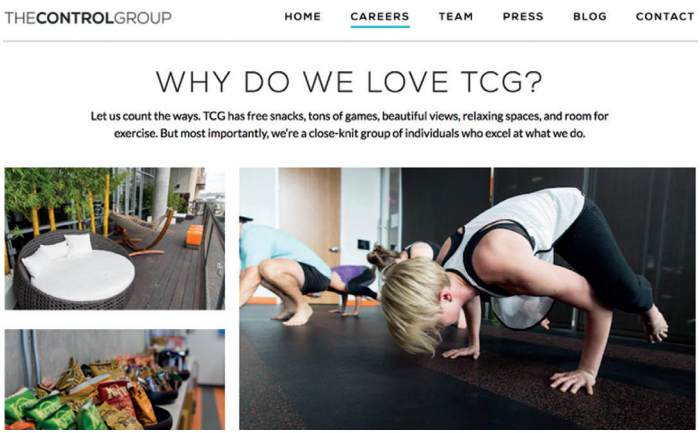
Saber a verdade sobre a história de sua família e amigos pode ser chocante, então, por favor, seja cuidadoso ao usar essa ferramenta.

O Instant Checkmate não fornece relatórios de consumidores e não é uma agência de informações de consumo. Fornecemos informações sensíveis que podem ser usadas para satisfazer sua curiosidade, proteger sua família, e encontrar a verdade sobre pessoas em sua vida. Você não pode usar nosso serviço ou as informações que ele fornece para tomar decisões sobre o crédito de consumidores, empregadores, finanças, locatários ou quaisquer outros propósitos que requeiram conformidade com a Lei de Proteção ao Crédito.

Estou ciente

Esse é o tipo de propaganda que você pode encontrar nesses sites. Vou direcionar a atenção de vocês para o meio da tela, onde se lê "aprender a verdade sobre a história de sua família e amigos pode ser chocante, então, por favor, seja cauteloso ao usar essa ferramenta". Essa é uma janela em que você precisa clicar quando está usando um desses sites de registro criminal. É meio bobo, mas realmente toca naquele ponto em que, vocês sabem, nós sempre queremos saber mais sobre as pessoas e há muitos gatilhos na internet para nos fazer continuar clicando. Esses mecanismos psicológicos usados em publicidade são agora aplicados ao sistema de justiça criminal. Isso realmente criou uma classe de consumo para pessoas que buscam dados de registros criminais para fins de informação, mas também para exposição, para estereotipar, e para justificar a discriminação.

A empresa que postou essa advertência posta fotos de rosto e cria a idéia de que os Estados Unidos são um lugar muito perigoso, e de que é realmente nosso dever ter certeza de que estamos verificando todas as pessoas na internet. Mas este é o site da própria empresa:



Por que amamos o TCG?
Deixem-nos contar as razões. O TCG tem lanches gratuitos, belas vistas, espaços de relaxamento e salas para exercício. Mas, mais importante, somos um grupo de pessoas bem entrosadas com muita competência no que fazemos.

A marca da empresa é bem diferente do serviço de registros criminais. Sua própria marca é ser uma empresa de tecnologia da Califórnia com uma cultura de yoga e surf, que adota integralmente o sistema de valores do Vale do Silicone. A verdade é que o produto que eles vendem é um sistema legal muito desumanizador, que ataca pessoas, que prejudica pessoas, que é confuso e bastante nocivo; e ainda assim essa é a mercadoria que eles vendem, apesar de se entenderem como uma empresa focada em inovação.

Então se pensarmos sobre o ângulo da mercantilização de forma um pouco mais acadêmica e consideramos o que significa a mercadoria em uma acepção marxista, pensaremos em algo que tem forma dupla: há a sua forma natural, e há a sua forma como valor. O sociólogo Dale Rushkoff chamou de mercantilização "a atribuição de um valor a um bem social". Ouvimos muito sobre mercantilização de dados no setor de dados de consumidor: a coleta e agregação de dados pessoais para fins econômicos, dados do tipo que frequentemente compartilhamos com aplicativos. Eu argumentaria que a mercantilização de registros criminais é um uso privado de dados públicos. Temos leis de transparência na constituição para que as pessoas possam monitorar o governo. Antes de tudo, é para isso que temos acesso aos registros criminais. Mas, porque foram digitalizados e disseminados tão rapidamente pelo setor de venda de dados, o que temos visto é o uso de dados públicos para fins comerciais. E o que isso faz é importar a lógica da tecnologia para a punição criminal. A mensagem é que as empresas privadas são melhores em lidar com dados objetivamente, são transparentes e eficien-

/ A PUNIÇÃO DIGITAL É UMA CONSEQUÊNCIA DAS OPERAÇÕES LEGAIS ORIENTADAS POR DADOS, DO ESFORÇO PARA USAR MAIS DADOS PARA ORGANIZAR O SISTEMA LEGAL /

/ ENQUANTO,
TECNICAMENTE,
TEMOS LEIS
PARA EXPANDIR
A TRANSPARÊNCIA
DO GOVERNO,
ESSAS LEIS TÊM
SIDO ALAVANCADAS
PARA ENCORAJAR
A VIGILÂNCIA
ENTRE PARES /

tes de um modo que o governo não é. Assim, há uma expansão dos fatores que causam a punição digital: já não existem apenas os tribunais, mas também esses terceiros.

E o que acontece com as pessoas quando são atingidas por isso? Em meu estudo, entrevistei centenas de pessoas cujos registros aparecem na internet, e foi impressionante o número das que disseram saber que os registros estavam online, mas que simplesmente não queriam vê-los. Os entrevistados realmente expressaram uma noção de desamparo assimilado, ou um tipo de alienação: "Eu sei que está lá, mas nunca fui olhar, se está lá, está lá! Não me interessa".

Digital avoidance

"I've never really looked it up online. **I don't want to know** what's on there." – Sam

"I never look for myself. Not interested. I know who I am. If it's out there, it's out there. Not interested in that. I hope there's not any photos of me floating around. But **I don't go looking for them.**" – Ryan

"Everything just goes onto the computer. **I don't look at it.**" – Kira

"**I've never looked for it.** It's too complicated. What CAN I do – IF I could do anything? And then people see it, and they think you did it, it says you did something, but the truth is I didn't do anything." – Mariah

"No. I deliberately avoid it. It's a horror story I don't want to relive. And what good is my reaction to a website? **What does that accomplish?**" – Albert

Evitamento digital

"Eu nunca procurei [os dados] online. **Não quero saber** o que tem lá." – Sam.

"Eu nunca procuro por mim. Não me interessa. Eu sei quem eu sou. Se está lá, está lá. Não me interesso por isso. Eu espero que não haja fotos minha pairando por lá. **Mas não saio procurando por elas**." – Ryan.

"Tudo entra no computador. **Eu não olho pra isso**" – Kira

"**Nunca procurei por isso**. É muito complicado. O que eu posso fazer – se eu puder fazer alguma coisa? Aí as pessoas vêem, acham que você fez mesmo, lá diz que você fez alguma coisa, mas a verdade é que eu não fiz nada" – Mariah.

"Não. Eu deliberadamente evito olhar. É uma história de terror que não quero reviver. E de que adianta minha reação contra um site? **O que isso resolve**?" – Albert.

Todas essas frases são citações de entrevistas. A última me parece realmente perspicaz. Albert me disse: "Eu deliberadamente evito olhar. É uma história de terror que eu não quero reviver. E de que adianta minha reação contra um site? O que isso resolve?". Anteriormente, quando falei sobre as disparidades na punição digital, pudemos ver de imediato que as pessoas que já estão sob intensa vigilância do governo – não só por conta do sistema de justiça, mas também por receberem benefícios do governo ou usarem o sistema de saúde subsidiado pelo governo –, já estão sob amplos regimes de vigilância. Eles não precisam ir buscar seus registros criminais na internet. Eles sabem que provavelmente estão lá, mas eles não querem lidar com isso.

O problema é: se alguma dessas pessoas com quem falei for se candidatar a um emprego ou a um apartamento, é muito provável que o responsável pela decisão encontre o registro na internet – e essas pessoas jamais vão saber o que diz o registro, já que nunca o consultaram.

Quando pensamos nos danos trazidos por isso, vemos que é um dano difícil de medir, pois as pessoas em meu estudo me falaram repetidamente de afastamentos de escolas, de sua comunidade, da vida pública, de sua intenção de procurar por um emprego ou por um apartamento melhor. Pense em como seria viver sua vida sem que as pessoas jamais pesquisassem você na internet. A internet não é um lugar seguro se você tem um rastro de fotos de rosto ou um registro de detenção, independentemente de sua prisão ter sido correta ou não, ou de as acusações terem resultado em condenação criminal.

Além disso, há esse novo fenômeno no mundo da Covid, em que os procedimentos judiciais – que são abertos, qual-

quer um nos Estados Unidos pode entrar em um tribunal para assistir os procedimentos – migraram para tribunais transmitidos no Zoom e no YouTube. Assim, há milhares de tribunais que estão transmitindo o dia inteiro, e a lógica por trás dessa transmissão é a mesma do início dos anos 1990, quando os registros das cortes começaram a ser digitalizados e postos na internet. A idéia é que, se um dado é tecnicamente um registro público, qualquer um deve ter acesso a ele, em qualquer plataforma em que esteja disponível. Só que, por cem anos, isso significou que você precisaria entrar em um fórum e solicitar os arquivos. No contexto digital, você só precisa ir até o site para acessar a informação. Agora temos esse novo nível de transmissão ao vivo.

Assisti um julgamento na semana passada e vi dois pais disputando a custódia da criança; eles falaram da tentativa de suicídio do pai e de seu alcoolismo, mostraram fotografias do interior da casa do casal, os quartos de seus filhos. Tudo isso foi gravado no Zoom e transmitido ao vivo no YouTube.

Eu diria que, se continuarmos a divulgar as audiências dessa forma, poderá haver um impacto negativo na participação democrática legal, ou seja, testemunhas ou vítimas ficarão apavoradas de dizer a verdade se souberem que seus rostos e seus nomes estão sendo transmitidos por toda a internet.

Há frequentemente louváveis propósitos de transparência nessas iniciativas digitais. Mas o que ocorre é que não estamos obtendo uma transparência real sobre o sistema criminal. Sequer sabemos quantas pessoas são mortas pela polícia a cada ano nos Estados Unidos e, apesar disso, eu poderia contar a vocês detalhes pessoais de muitas pessoas que são presas por essas polícias, suas fotos, seus endereços, todo tipo de informação que pode ser usada contra as pessoas que estão sendo detidas, à custa de saber mais sobre como o governo realmente está funcionando.

Quais são as implicações disso? A primeira é o "efeito raio de sol reverso". Enquanto, tecnicamente, temos leis para expandir a transparência do governo, essas leis têm sido alavancadas para encorajar a vigilância entre pares. Assim, quando pensamos nas implicações dos dados no sistema legal, não é só que a polícia tem coletado dados para o uso na atividade policial, é que o governo está nos levando a observar uns aos outros, a vigiar uns aos outros, ou a levar para a polícia vídeos da entrega da Amazon em nossa porta. Estamos nos comprometendo com o projeto de vigilância sem ao menos perceber, em troca de obter bons dados em massa sobre o próprio sistema de justiça.

Além disso, temos o problema do "entra lixo, sai lixo", a citação famosa frequentemente usada nos tribunais. Se colocarmos dados ruins em um algoritmo, os resultados serão ruins. Nós criticamos os algoritmos por serem racistas, por aprofundarem as desigualdades, sendo que os algoritmos estão apenas replicando o comportamento do próprio sistema de justiça, que frequentemente persegue as pessoas com base em sua aparência ou no local em que vivem.

Então, não só temos injustiças algorítmicas, mas também temos o problema para o indivíduo que sequer sabe quais são ou onde estão seus dados. Realmente precisamos, especialmente nos Estado Unidos, descobrir uma maneira de tratar os registros criminais como tratamos os relatórios de crédito, relatórios médicos, relatórios educacionais. Todos esses são tipos diferentes de registros administrativos que sabemos que podem mudar nossas chances na vida e a forma como somos tratados. Nós deveríamos ter acesso a nossos próprios dados.

Esses rótulos são bastante permanentes; com isso, quero dizer que esse é um tipo de estigmatização que realmente pode permanecer ao longo de uma vida inteira. Isso não termina com uma sentença de prisão ou uma condenação,

mas realmente reforça os estereótipos de que "o crime está em todo lugar", "pessoas que são negras, pessoas que são pardas podem ser criminosas", porque somos repetidamente inundados por essas imagens nas galerias de fotos de perfil nos Estados Unidos. Mais uma vez, esses comportamentos de policiamento se traduzem em cânones digitais, que acabam por legitimar a operação inteira.

Além disso, há a exposição pública. Há as dificuldades sociais e psicológicas com que as pessoas devem lidar após terem sido rotuladas, pois elas ficam com a percepção de que nunca vão superar esse rótulo, de que ele estará sempre lá definindo suas características.

Há também grandes preocupações sobre a discriminação velada. Com isso, quero dizer que temos alguns sistemas regulatórios para verificação de antecedentes, temos parâmetros usados por empregadores para recusar trabalho a alguém com base em seu registro criminal. No entanto, se sou um empregador contratando alguém em um período de recessão, vai haver muita gente se candidatando ao trabalho. Eu vou querer pagar 65 dólares por uma checagem de antecedentes para cada candidato? Provavelmente não. Então, posso fazer uma busca não regulamentada e simplesmente procurar as pessoas no Google, e então retirar determinados nomes da pilha de inscrições e apenas dizendo: "eles não eram adequados, não tinham as qualificações certas". Assim, quanto mais público é o registro criminal disponível nos Estados Unidos, menos importa a regulação, já que as pessoas não precisarão submeter-se a essas regras.

Há também uma grande pressão para aumentar a exclusão e o resguardo dos registros criminais nos Estados Unidos. Essa é uma política muito boa e muito importante, especialmente para pessoas que precisam de licenças profissionais. Se você trabalha com serviços de saúde, por exemplo, se você quer

ser enfermeiro, ter seu registro resguardado da vista pública o ajuda a conseguir esse trabalho. Mas, se esses registros estão disponíveis na internet, se essas versões diferentes de registros existem nesses espaços privados, isso transforma essas políticas em menos efetivas.

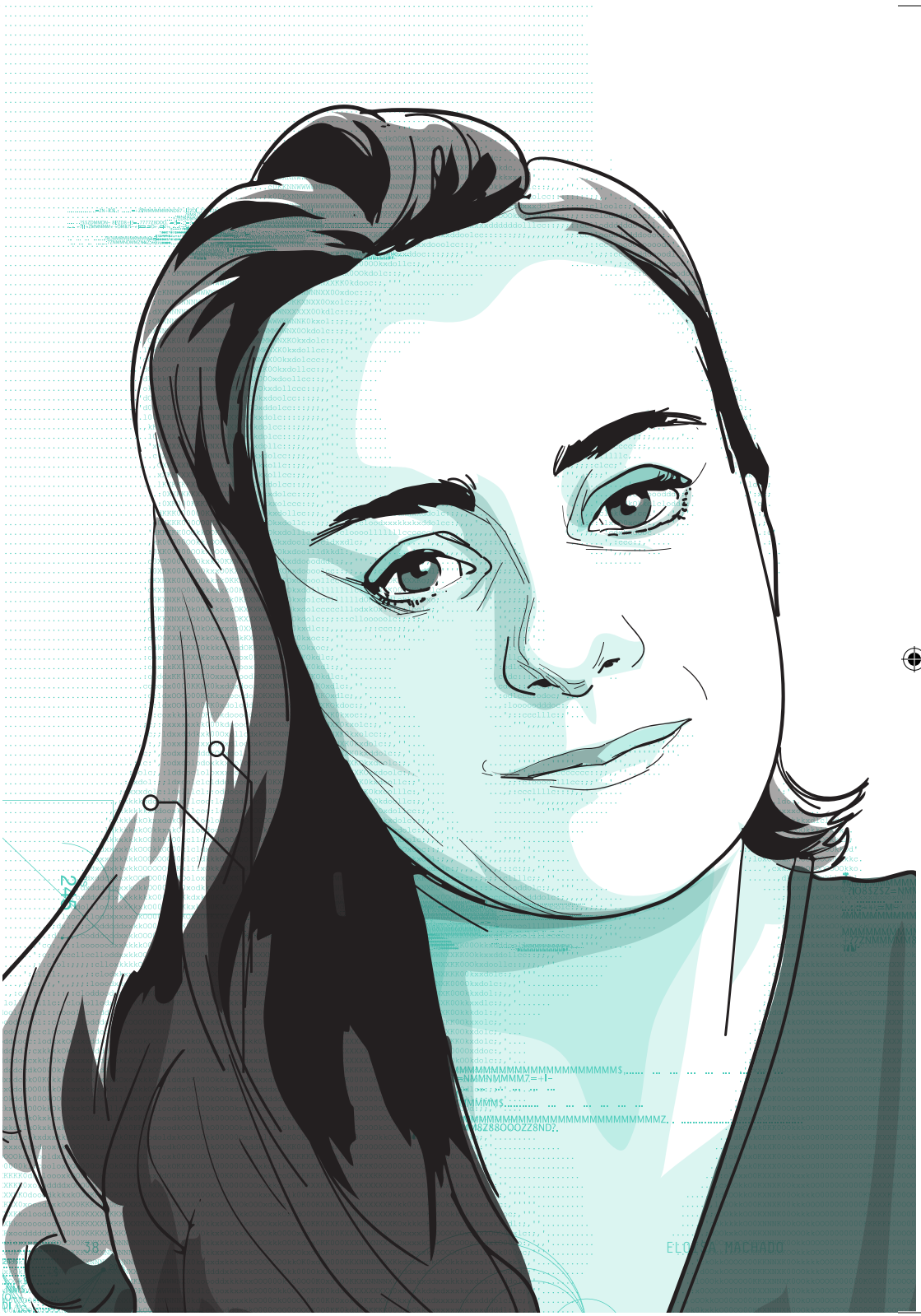
Enfim, há um impacto de disparidade. A probabilidade de ser rastreado nesse sistema já está previamente estruturada. Assim, a possibilidade de solucionar problemas na versão digital do registro também está estruturada por classe social, tecnologia e acesso aos recursos.

Então, para onde vamos, agora que expus o problema? Para o meu estudo, penso que há muitas soluções políticas. A primeira seria reclassificar dados de registro criminal como uma das formas de dados de consumidores. Nos Estados Unidos, existem maneiras de reclassificar dados anteriores à condenação para que sejam tratados como dados de posteriores à condenação, que, ironicamente, recebem maior proteção à privacidade. Há também maneiras de limitar a possibilidade de obtenção de dados em massa. Poderíamos voltar à versão original das leis de transparência, o que significaria dizer: "Eu quero tal arquivo para tal propósito", em vez de simplesmente permitir que usuários baixem uma montanha de dados sobre cada pessoa que já foi processada por um departamento de polícia.

Para o trabalho de vocês, naquilo em que ele se sobrepõe ao meu, acho que é mais importante do que nunca realmente esquadrinhar as parcerias público-privadas, e pensar em seus danos e na direção que elas seguem. Quero dizer: a polícia realmente quer a tecnologia, ou é a empresa de software que está batendo à porta dela? Temos visto fotos dessas grandes conferências de tecnologia e a forma como vendedores e comerciantes trazem suas tecnologias para a esfera pública. Então é realmente hora de esquadrinhar essa relação entre público e privado.

Acredito que precisamos pensar sobre transparência de forma diferente, como uma transparência para os dados do sujeito versus uma transparência para a instituição. Pensar muito criticamente sobre como é esse "efeito raio de sol reverso". E isso significa destrinchar o algoritmo. Então, mesmo que essas empresas se escondam atrás das defesas de proprietário ou de setor privado, ou se elas não quiserem ser transparentes, é mais importante do que nunca entender quais dados estão sendo coletados e para onde estão indo.

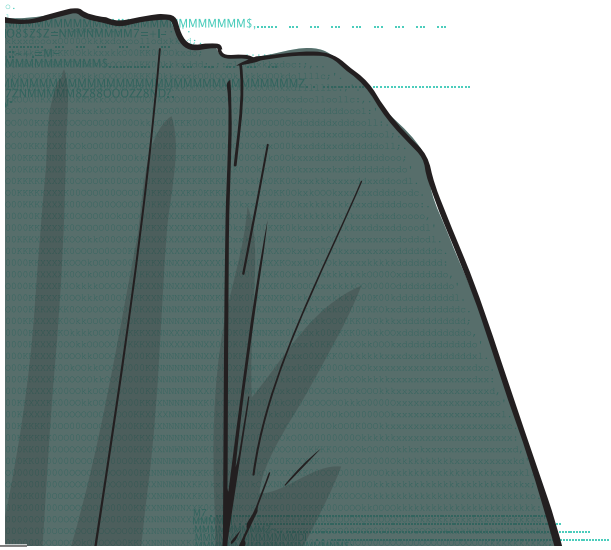
E acredito que haja também um papel do setor privado. Nos Estados Unidos, isso significa pressionar muito para que o Google mude a política da empresa e deixe as pessoas requisitarem a remoção de suas fotos de rosto da internet. Não vejo o direito de ser esquecido ou a Lei Geral de Proteção de Dados sendo importados logo para os Estados Unidos, infelizmente. Então, talvez possamos pressionar essas empresas a pensar sobre como elas estão promovendo e legitimando o sistema de justiça penal com base no papel que elas desempenham na disseminação da informação.Muito obrigada pela atenção e por participarem dessa conversa!



02.

O DEBATE CONSTITUCIONAL SOBRE PRIVACIDADE, INTIMIDADE E PROTEÇÃO DE DADOS NO BRASIL

Eloísa Machado[1]



1. O presente texto se baseia em apresentação oral feita no painel "Do Domicílio aos dados: O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

Olá, boa noite a todos e todas, é um prazer enorme estar aqui com vocês para debater esse tema tão novo, tão instigante, relacionado ao impacto da interpretação da privacidade em termos constitucionais, voltada agora para a proteção de dados nos mais recentes casos do Supremo Tribunal Federal.

Antes de começar essa breve exposição, gostaria de agradecer imensamente o convite feito pelo InternetLab para participar desse Congresso. Eu sou muito fã do trabalho de vocês e mais ainda fico feliz de participar desse congresso com a mediação da minha querida Nathalie Fragoso, uma advogada brilhante, uma grande colega em várias ações, e com a honra enorme de dividir um pouco dessas reflexões com o professor Gustavo Badaró, que vai nos acompanhar essa noite. Então deixo o enorme agradecimento pelo convite e pela possibilidade de trazer alguns desses debates para vocês.

O painel tem um título bastante provocador "do domicílio aos dados" e eu vou sugerir uma inversão: dos dados ao domicílio, para tentarmos nossa fala de maneira otimista, porque me parece que a maneira como o Supremo tem interpretado e encarado a privacidade e a proteção de domicílio traz *standards* melhor definidos do que ele tem dado agora especificamente para proteção de dados.

Eu vou nessa primeira parte da minha exposição tratar de três decisões super recentes do Supremo Tribunal Federal que se referem e tangenciam o tema de proteção de dados e, claro, que essa interpretação pode vir a ter impacto no que se refere à persecução criminal e no uso dessa interpretação pelas instituições de segurança pública.

A primeira decisão que eu gostaria de mencionar, relatada pela Ministra Rosa Weber, refere-se à Ação Direta de Inconstitucionalidade 6.387, a famosa ADI do IBGE, que solicitava o compartilhamento de dados das empresas de telefonia com o

IBGE para fins assumidos - os escusos nunca iremos saber - de realização do Censo populacional.

A segunda decisão se refere a um julgamento também recente, na Ação Direta de Inconstitucionalidade 6529, relatada pela Ministra Carmem Lúcia, sobre o compartilhamento de dados com órgãos de inteligência no âmbito do próprio governo.

E a terceira decisão se refere ao Recurso Extraordinário 1.055.941, relacionado ao compartilhamento de dados fiscais - o caso Coaf, como ficou famoso -, para efeitos também de persecução criminal.

Tanto no caso do IBGE, como no caso da ABIN, o Supremo estabeleceu critérios bem interessantes no que se refere à proteção de dados, ainda que, na minha opinião, insuficientes em termos de proteção jurisdicional, para se averiguar a ilegalidade do acesso a dados pessoais. O que essas decisões têm em comum? O primeiro ponto é de que qualquer compartilhamento de informação tem que se dar de maneira justificada - uma justificativa consistente e legitimada - para que determinado órgão ou pessoa possa ter acesso àquela informação. Gostei muito como o Ministro Ricardo Lewandowski enquadrou essa questão de proteção de dados na perspectiva dos direitos fundamentais. Ele disse o seguinte: "o maior perigo que a gente corre hoje é justamente o controle da vida privada dos cidadãos mediante a coleta massiva de informações pessoais". Me parece que o Ministro Ricardo Lewandowski estava bastante antenado com os problemas e desafios que se colocam em relação à interpretação da possibilidade de coleta massiva de dados e o impacto que isso pode ter para o exercício de direitos fundamentais, inclusive no que se refere à eficácia horizontal, entre particulares, dos direitos fundamentais.

O caso do IBGE teve um papel muito importante, cujo impacto sentimos agora, de antecipar os critérios da LGPD para aquela

decisão. A Ministra Rosa Weber claramente assumiu a LGPD, mesmo antes de sua entrada em vigor, como um parâmetro para a maneira de lidar com proteção e acesso a dados pessoais. O debate sobre entrada ou não em vigor, ou adiamento da entrada em vigor da LGPD, foi de certa maneira esvaziado pela Ministra Rosa Weber ao usar a LGPD para reinterpretar o direito à privacidade, que já estava previsto na Constituição. Esse painel já se torna histórico, porque circula a notícia de que a LGPD vai de fato entrar em vigor agora[2].

As duas decisões falam de reserva de jurisdição. Se estamos falando de informação que não está sujeita à reserva de jurisdição, ou seja, que não são sigilosas, que não compõem o que a gente pode chamar de um núcleo mais duro do direito à privacidade, mesmo assim elas só podem ser compartilhadas de maneira justificada, com uma justificativa consistente, legitimada para explicar exatamente o que vai ser feito com aquela informação. Mas as informações que a Constituição já reserva especificamente ao controle jurisdicional prévio, essas não podem ser compartilhadas, a não ser, claro, com a devida autorização jurisdicional.

Aqui eu acho que vale a pena assentarmos que, quando falamos de interpretação do Supremo, estamos falando de 11 Ministros que decidem não necessariamente de maneira uniforme. Olhando a posição de cada um deles, podemos extrair tendências interessantes para se imaginar o comportamento em casos futuros. Então, ainda que o Supremo tenha por maioria decidido esses dois casos com essas garantias, são os Ministros isoladamente, isto é, são as razões decidir de cada um dos votos que permitem inferir o perfil de votação em casos futuros. Por que eu estou falando isso? O Ministro Toffoli se preocupou, nesses dois julgamentos, com o procedimento de segurança para o fornecimento desses dados. A agenda

2. Nota da autora: A LGPD entrou em vigor em 18 de setembro de 2020 e, no dia 26 de agosto de 2020, o Congresso Nacional decidiu que não mais prorrogaria sua entrada em vigor.

do Ministro Toffoli, no que se refere à proteção de dados, é uma agenda de governança do sistema público de quem vai acessar e de como esse dado vai ser fornecido. É muito clara a maneira como ele focou a sua preocupação nos dois julgamentos em relação a esse ponto. Essas informações sobre o julgamento não estão sendo dadas a partir de análise do acórdão, que ainda não foi publicado, mas a partir do acompanhamento da sessão do julgamento, que é nosso trabalho lá na FGV, no grupo de pesquisa Supremo em Pauta[3].

Falei de IBGE e de ABIN, falta falar de COAF. Quando olhamos o caso do COAF, percebemos que o tribunal decidiu que era possível o compartilhamento de dados, inclusive os dados sob os quais recai uma reserva de jurisdição. Então, se olhamos as recentes decisões do IBGE e da ABIN e compararmos com a decisão um pouco mais antiga de COAF, veremos que é uma posição absolutamente incoerente do tribunal, discordante no que se refere à possibilidade de compartilhamento de dados pessoais dentro da própria estrutura governamental e, sobretudo o que é mais grave no caso COAF, para fins explicitamente de persecução criminal, ou seja, o compartilhamento dessas informações fiscais com o Ministério Público, com a Polícia Federal, para efeitos de criminalização.

O padrão de garantia que o STF usou no caso COAF para estabelecer critérios para o compartilhamento de dados pessoais foi muito baixo. Me parece que talvez seja revisto em breve, justamente pela jurisprudência mais recente, no que se refere aos já mencionados casos ABIN e IBGE.

O que o Supremo falou em linhas gerais sobre o compartilhamento de dados do COAF? Primeiro, que o que importava era o controle de acesso, ou seja, quem teria acesso a essas

3. Nota da autora: o grupo de pesquisa Supremo em Pauta é da FGV Direito SP. Criado em 2014, é atualmente coordenado pela professora Eloísa Machado e pelo professor Rubens Glezer e tem Luiza Pavan Ferraro e Ana Laura Barbosa como pesquisadoras.

informações. Vamos lembrar em que contexto o Supremo decidiu isso: havia uma certa ameaça velada de que dados fiscais de Ministros do tribunal estavam sendo acessados e relatórios sendo produzidos para serem divulgados pelo COAF e pelo Ministério Público Federal. E, de novo, o ministro Dias Toffoli falando em controle de acesso - quem tem acesso? qual é a governança de acesso a essa informação? – para afirmar que não seria possível fazer um relatório por encomenda. Bom, mas como é que você vai averiguar isso, se um determinado relatório de dados foi feito por encomenda ou não? E é isso que estou chamando de *standard* fraco de proteção do compartilhamento e acesso a dados pessoais.

Quando essa informação chega no Ministério Público, há a necessidade de instauração de um procedimento para que a partir daí, da instauração do procedimento, haja o efetivo controle jurisdicional. Então, a noção de reserva de jurisdição aparece no caso do COAF como posterior, a partir da instauração de um procedimento produzido pelo Ministério Público, que não poderia ficar com aquelas informações na gaveta, palavras explícitas aqui usadas pelos Ministros do Supremo nesse julgamento. Além de todo o debate sobre a licitude ou não dessa prova, há toda aquela confusão que o STF fez em relação aos termos de colaboração premiada, que reaparece agora também em relação a esses relatórios e esses dados pessoais. Os relatórios não seriam provas, seriam meio de obtenção de prova. E você não consegue diferenciar uma coisa da outra e permite um espaço muito menor de fiscalização sobre a atividade de persecução criminal.

Bom, eu falei que iria tratar dos dados ao domicílio. Quando vamos para decisões relativas a domicílio, ainda que saibamos que essa interpretação é difícil de ser colocada em prática, que temos violações sistemáticas e institucionais em relação à inviolabilidade do domicílio, ainda que saibamos tudo isso,

/ A CONSTRUÇÃO DA PROTEÇÃO ANALÓGICA, DA PROTEÇÃO DE DOMICÍLIO, SERVE MUITO [...] PARA CONSTRUIR MELHORES INTERPRETAÇÕES PARA A PROTEÇÃO DE DADOS /

/ O TEMA É NOVO, MAS O DIREITO À PRIVACIDADE JÁ ESTÁ RECONHECIDO NA CONSTITUIÇÃO HÁ UM TEMPÃO /

é imperioso reconhecer que são decisões muito mais robustas no que se refere ao direito à privacidade, em termos estritos de standard protetivo da decisão. Me parece que o Supremo, quando foi interpretar casos de proteção de dados, escolheu o caminho mais difícil, como se precisasse fazer isso do zero, sendo que o que estamos fazendo é uma reinterpretação do direito à privacidade, que é uma coisa que o Supremo faz há muitas décadas e faz de maneira muito interessante, especialmente no que se refere à proteção da privacidade para efeitos de uma futura investigação ou no curso de uma investigação criminal. A construção da proteção analógica, da proteção de domicílio, serve muito e pode servir muito para construir melhores interpretações para a proteção de dados, a partir do feixe, é lógico, da privacidade. Vou citar dois casos do STF que são relevantes para entendermos essa estandardização.

O primeiro é um Habeas Corpus 138.565, que foi relatado pelo Ministro Ricardo Lewandowski, estabelecendo parâmetros muito claros de como e quando se ingressar ou não em domicílio. E o Recurso Extraordinário 603.616, que me parece um caso pouquíssimo explorado em termos do impacto para a proteção de direitos fundamentais e também para a proteção de dados. Qual foi a decisão? O Supremo disse o seguinte: mesmo em caso de flagrante, onde a Constituição expressamente autoriza a entrada em domicílio, sem a devida autorização judicial, é preciso que o agente policial demonstre ter fundadas e prévias razões para ingresso em domicílio. Então, aquela famosa "pescaria" (que se aplica tanto a domicílio como pode servir para dados pessoais), onde se procura a esmo até encontrar algo, é ilegal. Neste Recurso Extraordinário, portanto, houve um aumento enorme no de proteção ao domicilio. Essas razões fundadas e prévias têm que ser formalizadas, oficializadas, para posterior possível responsabilização do agente e já há indicação da jurisprudência de que a prova se torna

ilícita. Se não havia fundada razão, se não explicou como você chegou naquele domicílio, a prova é ilícita. Então, me parece que se usarmos esse parâmetro da proteção de domicílio, conseguimos aprimorar também a proteção de dados.

Quais são as conclusões que conseguimos derivar, olhando a jurisprudência dos dados ao domicílio, ambas voltadas à caracterização do âmbito de proteção do direito à privacidade?

Primeiro, que o Supremo poderia se aproveitar muito melhor da construção histórica e muito mais robusta que ele faz em relação à proteção do domicílio, pelo viés de limitação inclusive do poder de investigação para analisar casos de proteção de dados, sem precisar da impressão de que é uma coisa absolutamente nova. O tema é novo, mas o direito à privacidade já está reconhecido na Constituição há um tempão.

A segunda conclusão incontornável é que o Supremo está agora convivendo com decisões absolutamente incoerentes, o que eles falaram no caso do IBGE, mas sobretudo no caso da ABIN, não se coaduna com o que eles falaram no caso do COAF. Sim, são os mesmos Ministros falando coisas absolutamente opostas no que se refere, sobretudo, à reserva de jurisdição para acesso e compartilhamento de dados pessoais.

O terceiro ponto é de que talvez a explicação para essa incoerência é da influência que a agenda de combate ao crime ainda exerce sobre o tribunal. Entender o contexto do caso do COAF é importante, porque o caso do Coaf virou o caso Flávio Bolsonaro. O caso COAF virou aquele caso de terrorismo persecutório, de que se não fosse mantida a forma de compartilhamento de dados, todas as investigações do Ministério Público seriam arquivadas. Parece que o Supremo tomou a decisão bastante acuado por essa agenda de combate ao crime e, agora, em outros casos, onde ficou evidente o perigo de se permitir o acesso dessas instituições a dados pessoais, sobretudo submetidos à reserva jurisdicional, o Supremo parece recuar.

Não podemos nos esquecer de que o caso ABIN, tratava especificamente de um decreto, e logo depois se tornou um caso de elaboração de um dossiê ilegal, inconstitucional, um dossiê de polícia política. E aí me parece que a ficha do Supremo caiu: se eu permitir o compartilhamento de informações, talvez eu esteja alimentando um tipo de perseguição política nesse governo que, todos sabemos, é refratário à lógica dos direitos humanos e fundamentais.

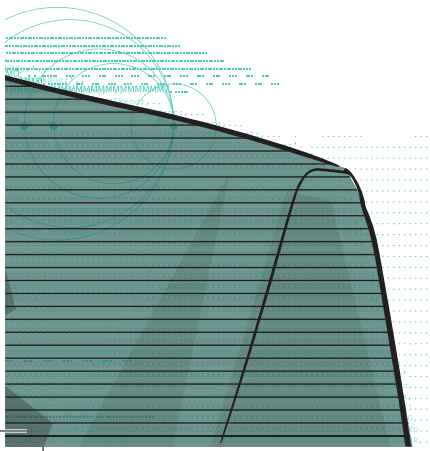
Feitas essas considerações, eu já me calo aguardando aqui as perguntas do debate ao final do painel.

Muito obrigada!

03.

O DEBATE CONSTITUCIONAL SOBRE PRIVACIDADE, INTIMIDADE E PROTEÇÃO DE DADOS NO BRASIL

Gustavo Badaró[1]



1. O presente texto é baseado na transcrição da exposição feita no IV Congresso Internacional, sobre "Direitos Fundamentais e Processo Penal na Era Digital – Proteção de Dados em Segurança Pública e Investigações Criminais", promovido pelo InternatLab, no painel "Do domicílio aos dados: o debate constitucional sobre a privacidade, intimidade e proteção de dados no Brasil". Houve pequenas alterações e acréscimos para tornar mais compreensível a exposição, mas mantido o estilo de uma narrativa oral. Foram acrescentadas notas de rodapé, com dados jurisprudenciais e bibliográficos, para que o leitor interessado possa aprofundar a análise, nos temas mais relevantes abordados na exposição.

Boa noite. Gostaria de cumprimentar a Nathalie Fragoso e, em seu nome, saudar InternetLab, por mais esse evento, o IV Congresso Internacional, sobre "Direitos Fundamentais e Processo Penal na Era Digital". Também desejo parabenizar a professora Eloísa Machado, que me antecedeu com uma brilhante exposição e sua detalhadíssima análise sobre a posição - ou a falta de posição - do Supremo Tribunal Federal.

Além de gostar muito da exposição da Eloísa, isso me libera para falar do modo que eu mais gosto, que eu chamo de efeito Julia Roberts. Explico o que é o "efeito Julia Roberts". Para quem assistiu "Dossiê Pelicano", ela está assistindo aula na faculdade e o professor faz uma exposição sobre uma decisão tomada pela Suprema Corte dos EUA, que decidiu não ser inconstitucional a lei do estado da Georgia que classificava certas condutas como crime.[2] Diante de tal informação, ela afirma: "A Suprema Corte está errada"! Eu gosto de usar esse fator Julia Roberts, pois muitas vezes digo: o Supremo Tribunal Federal está errado! Ou, o que seria o outro lado da moeda, não é porque o Supremo Tribunal Federal decidiu algo, que sua decisão está certa.

Agradeço aos organizadores do evento, pelo título da palestra. Considero extremamente oportuno analisar a questão da proteção dos dados pessoais sob a ótica "do domicílio aos dados".

Na primeira parte da exposição, muito rapidamente, pretendo mostrar como há uma insuficiência legislativa para proteção dos dados pessoais, do ponto de vista da lei de execução penal e da utilização desses dados para fins de investigação criminal. Mas, a ideia do direito à privacidade, e a noção de inviolabilidade do domicílio, sempre

2. Tratava-se do precedente firmado no caso *Bowers* vs. *Hardwick*, do ano de 1986 em que por cinco votos a quatro, à luz do direito à privacidade, a Suprema Corte decidiu que não era inconstitucional a lei da sodomia do estado da Geórgia, que criminalizava os sexos oral e anal consensuais feitos em ambiente privado por adultos, sendo que a questão foi analisada com enfoque nas relações homossexuais, apesar da lei não fazer nenhuma diferenciação clara nesse sentido.

esteve muito ligado a um aspecto negativo de tal direito: a não intromissão alheia. O direito à privacidade é o *right to be alone*. O direito de estar só, sem sofrer intromissão alheia.

Passando diretamente à inviolabilidade do domicílio, quando pensamos em sua tutela, não é a proteção do prédio, do edifício em si, mas é do que o domicílio representa: ou seja, é estar entre as quatro paredes, fora das vistas alheias. Dentro da minha residência eu tenho uma casca que protege a minha privacidade. Tudo que eu fizer lá, desde que obviamente não seja ilícito e não constitua crime, pouco importa a terceiros e não deve estar sujeito aos olhares e a crítica de quem quer que seja. Se é moralmente aceitável ou criticável, se a maioria da população gosta ou não gosta, isso pouco importa. Faz parte do meu direito à privacidade assim poder agir, sem estar passível ao conhecimento e crítica alheia, como elemento essencial para o desenvolvimento da personalidade. Isso é essencial para cada um de nós. Nosso comportamento é diferente quando ninguém sabe o que estamos fazendo. De outro lado, não ter esse espaço muda nosso comportamento. Se entramos em um elevador e nele houver uma advertência: "sorria, você está sendo filmado", nós agimos de uma determinada maneira; já num elevador sem câmera de segurança, nos comportamos de modo diferente. Se você não está sendo filmado, irá olhar no espelho, arrumar o cabelo, fazer qualquer coisa. E se você está sendo filmado, você se comporta de uma maneira diferente, deixando de fazer o que faria se ninguém pudesse lhe ver.

Porém, essa proteção que nós tínhamos, assegurada por aquela "casca" que o domicílio representa, mas que é uma proteção ao direito da privacidade e dos comportamentos que se desenvolviam lá dentro, hoje é insuficiente. Com o avanço da tecnologia, a proteção da privacidade exige novos contornos, distintos daqueles que eram assegurados pela simples inviolabilidade do domicílio. Não é preciso retroceder muito

no tempo. Se utilizamos a noção das progressões de gerações das mudanças legislativas na proteção de dados pessoais, quando se promulgou a Constituição de 1988, estávamos na segunda geração, talvez migrando para a terceira geração.[3] Mas a ideia da proteção de dados pessoais evoluiu muito desde então.

3. Refiro-me à classificação elaborada por Viktor Mayer-Schönberge, Generational development of data protection in Europe, In.: Agre, Philip E.; Rotemberg, Marc, Technology and privacy: the new landscape. Cambridge: The Mit Press, 2001.

Analisando o artigo 5º da Constituição, facilmente se constata três níveis de proteção distintos, nos incisos X, XI e XII. Farei a comparação a partir deste último. O inciso XII, como sabido, protege a liberdade de comunicação à distância, pelo emprego de quatro meios de comunicação distintos: comunicações postais, comunicações telegráficas, comunicações de dados e comunicações telefônicas. Não importa tanto distingui-las, mas sim constatar que, em relação à liberdade de comunicações, para sua restrição legítima a Constituição explicitamente exigiu dois níveis de proteção: reserva de lei e reserva de Constituição. O inciso XII prevê: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal e instrução processual".[4] A parte que nos interessa nesse debate é a que disciplina as exceções ao direito, prevista no final do dispositivo. Naquela época, o principal meio de comunicação à distância era a transmissão de voz por telefone – e o telefone de então era só um aparelho para comunicação de voz, muito diferente dos nossos aparelhos de telefone celulares de hoje –, e restrição à liberdade de comunicação à distância era sujeita à reserva de jurisdição e reserva de lei.

4. Não é preciso, para os fins dessa exposição, entrar na polêmica sobre o sentido da expressão "no último caso", sobre quais liberdades de comunicação do pensamento estariam envolvidos.

Já para proteger um mecanismo que assegura a privacidade, que é a inviolabilidade do domicílio, o inciso XI do art. 5º da Constituição estabelece: "a casa é o asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial". A exigência de que o ingresso se dê, "por determinação judicial", indica a necessidade de reserva de jurisdição. Não se estabeleceu, contudo, em relação ao ingresso no domicílio, a exigência de reserva de lei. Enquanto para interceptação das comunicações telefônicas e de dados, a Constituição exige que haja "ordem judicial", nas "hipóteses e nas formas previstas em lei", para a busca e apreensão domiciliar basta a "determinação judicial".

Por fim, assegurando o direito à privacidade, de uma forma ampla, o inciso X do artigo 5º da Constituição prevê: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação". Fácil constatar que, comparando os três incisos sequenciais do artigo 5º da Constituição, do mais amplo nível de proteção, para o mais restrito, exige-se: reserva de jurisdição e reserva de lei, para as interceptações telefônicas e telemáticas; apenas reserva de jurisdição, para as buscas e apreensões domiciliares; e para a restrição da privacidade, genericamente considerada, não há nenhuma exigência prévia do legislador constituinte quanto sua restrição.

O Supremo Tribunal Federal, há muito tempo, se posiciona no sentido da

5. STF, MS nº 21.729-4/DF, Pleno, Rel. Min. Marco Aurélio, rel. p/ ac. Néri da Silveira, j. 05.10.1995, m.v. No referido voto são citados, ainda, no mesmo sentido, os seguintes precedentes: "RHC 31.611, rel. designado Min. Afrânio Costa, j. 25.07.1951, DJU 28.09.1953, p. 2.880 (apenso ao n. 222); MS 2.172, rel. Min. Nélson Hungria, j. 10.07.1953, DJU 05.01.1954; [...] HC 67.913-SP, rel. p/o ac. Min. Carlos Velloso, j. 16.10.1990, RTJ 134/309; Pet 577 (Questão de Ordem)-SP, rel. Min. Carlos Velloso, j. 25.03.1992, RTJ 148/366; AgInq 897, rel. Min. Francisco Rezek, j. 23.11.1994, DJU 24.10.1995".

necessidade de reserva de jurisdição para restrição de direitos fundamentais, quaisquer que sejam eles. Há reserva de jurisdição, segundo o entendimento do STF, no julgamento do MS 21.729-4/DF, como se verifica do seguinte passo do voto do Min. Maurício Corrêa: "A jurisprudência desta Corte, consolidada e cristalizada a partir do julgamento dos citados Mandados de Segurança 1.047-SP e 1.959-DF, é rica em precedentes que nunca deixaram de entender que sigilo bancário é um direito individual não absoluto, podendo ser rompido somente em casos especiais, onde há prevalência do interesse público e, mesmo assim, por determinação judicial"[5]. Portanto, restrições legítimas do direito à privacidade, diante das necessidades de casos concretos, exigem prévia análise de um juiz. Porém, ainda assim, não me parece que seja equivocado considerar que o constituinte faz uma escala de intensidade para restrição desses direitos. E por que isso é preocupante, notadamente se o direito à proteção de dados pessoais for assimilado ao direito à privacidade? Porque se analisarmos as regras legais que disciplinam mecanismos concretos de restrição da privacidade, mesmo havendo a exigência de uma reserva de jurisdição, o que o legislador exige como requisito é muito pouco, sendo frágil a proteção da intimidade e da privacidade. É o que ocorre, por exemplo, tanto no sigilo fiscal quanto no sigilo financeiro, que são matérias que a dou-

6. Embora a expressão "sigilo bancário" seja bastante usual, não há porque restringir esse sigilo somente às instituições bancárias. É inegável que as instituições financeiras, em suas atividades rotineiras, têm acesso a vários dados de usuários do sistema financeiro, que envolvem aspectos de sua vida privada – ou mesmo de terceiros – que merecem proteção. Justamente por isso, melhor a denominação "sigilo financeiro" do que "sigilo bancário". Estão vinculados, pois, ao chamado "sigilo bancário", não só as instituições bancárias em sentido estrito, mas as instituições financeiras, públicas e privadas, em geral, bem como outras entidades que se subordinam à regulamentação legal do Sistema Financeiro Nacional. Corretamente, a LC n.º 105/2001, que dispôs sobre o sigilo das operações de instituições financeiras, prevê, em seu art. 1º, caput, que: "As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados" Por sua vez, o parágrafo único do referido artigo traz um rol exemplificativo das entidades obrigadas à preservar o sigilo financeiro.

trina e a jurisprudência consideram que estão sob proteção constitucional, como manifestação do direito à privacidade. O requisito legal para a chamada "quebra do sigilo bancário" ou a "quebra do sigilo fiscal", mediante decreto judicial do afastamento da privacidade são, quase que nenhum, tamanha sua amplitude.

Em relação ao sigilo bancário,[6] a Lei Complementar nº 105, no art. 1º, § 4º, prevê que, mediante ordem judicial,[7] é cabível a quebra de sigilo "quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial", seguindo-se um rol exemplificativo de crimes.[8] Admitir um meio de obtenção de prova, quando sua realização for necessária para apuração de crime, é possibilitar o afastamento do sigilo para praticamente toda e qualquer persecução penal.

Já quanto ao sigilo fiscal, o Código Tributário Nacional, no art. 198, *caput*, alterado pela Lei Complementar nº 104/2001, veda a divulgação, por parte da Fazenda Pública, de informações fiscais dos contribuintes. Por outro lado, o afastamento do sigilo fiscal é previsto, entre outras hipóteses, por "requisição de autoridade judiciária no interesse da justiça". Ou seja, basicamente, tem-se apenas a reserva de jurisdição, sem uma maior preocupação com a reserva de lei.

Nos dois exemplos acima, embora se exija prévia autorização judicial, como a reserva de jurisdição não é complementada pela necessária reserva de lei, há possibilidade pratica-

7. Na doutrina, pela necessidade de ordem judicial: Técio Lins e Silva; Marcela Lima Rocha, Apontamentos sobre o sigilo bancário, Revista Brasileira de Ciências Criminais, ano 12, n. 48, São Paulo: RT, maio-jun. 2004, p. 227; Mantovanni Colares Cavalcante, O sigilo bancário e a tutela preventiva. Revista Dialética de Direito Tributário, n. 68, São Paulo: Dialética, maio 2001, p. 94; Eduardo Cambi, Sigilo bancário e fiscal: a inconstitucionalidade da quebra sem autorização judicial, Revista Síntese de Direito Civil e Processual Civil, v. 2, n. 11, p. 28, Porto Alegre: Síntese, maio-jun. 2001; Milton Terra Machado, Sigilo bancário: a inconstitucional quebra do sigilo bancário. Revista de estudos Tributários, v. 3, n. 18, Porto Alegre, mar-abr. 2001, p. 16; Paulo Roberto Lyrio Pimenta, Possibilidade de quebra de sigilo bancário pelo Fisco à luz da CF. In: Pizolio, Reinaldo; Galvadão Jr., Jayr Viégas (Coord.). Sigilo Fiscal e bancário. São Paulo: Quartier Latin, 2005, p. 107.

mente ilimitada de restrição do direito fundamental. Isso porque, o juiz terá que verificar previamente, e conforme as condições do caso concreto, se aquela é uma situação que permite uma constrição legítima do direito fundamental. Mas se não há determinação constitucional que haja lei que estabeleça, de modo claro, preciso e objetivo, em que hipóteses poderá haver a restrição ao direito fundamental, cabe ao juiz decidir em que caso é ou não necessário, sem parâmetros previamente definidos. Também não haverá definição legal de limites temporais para duração da restrição. Em suma, reserva de jurisdição, sem reserva de lei, evita a discricionariedade do agente administrativo que atua na investigação penal, mas não impede a discricionariedade praticamente absoluta do julgador! Não havendo o limite da lei, o juiz pode, quando e por aquilo que bem entender, decretar essas medidas.

Então, sobre esse plano, avulta-se a importância de se compreender a proteção dos dados pessoais como uma projeção da tutela da inviolabilidade do domicílio. Mas isso não resolve adequadamente o problema. Ainda assim, trata-se de proteção insuficiente.[9] Basta lembrarmos que, para busca domiciliar, sequer é necessário que o local a ser varejado seja habitado por investigado ou

8. O § 4º do art. 1º da Lei Complementar nº 105/2001, estabelece: "§ 4º A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes: I – de terrorismo; II – de tráfico ilícito de substâncias entorpecentes ou drogas afins; III – de contrabando ou tráfico de armas, munições ou material destinado a sua produção; IV – de extorsão mediante sequestro; V – contra o sistema financeiro nacional; VI – contra a Administração Pública; VII – contra a ordem tributária e a previdência social; VIII – lavagem de dinheiro ou ocultação de bens, direitos e valores; IX – praticado por organização criminosa".

9. Sob uma ótica comparativa, a disciplina infraconstitucional da proteção da liberdade de comunicação telefônica e da comunicação telemática, segundo os critérios do art. 2º da Lei nº 9.296/1996 é mais robusta do que a proteção do domicílio. Isso porque, aquela medida somente é cabível para investigações ou processo penais de crimes punidos com detenção (inc. III). E somente pode ser decretada contra investigados em relação aos quais haja "indícios razoáveis da autoria ou participação" em tal infração (inc. I). E, por fim, não basta que haja fundadas razões de que na conversa se possa obter elemento de prova relevante, exigindo-se que a prova não possa "ser feita por outros meios disponíveis" (inc. II).

/ COM O AVANÇO DA TECNOLOGIA, A PROTEÇÃO DA PRIVACIDADE EXIGE NOVOS CONTORNOS, DISTINTOS DAQUELES QUE ERAM ASSEGURADOS PELA SIMPLES INVIOLABILIDADE DO DOMICÍLIO /

/ SEM A PROTEÇÃO DA LEGALIDADE, NOSSOS DADOS PESSOAIS ESTARÃO FACILMENTE DISPONÍVEIS AOS AGENTES DE PERSECUÇÃO PENAL /

imputado de uma persecução penal. O art. 240, § 1º, do Código de Processo Penal, admite a busca e a apreensão domiciliar desde que haja "fundadas razões" de que lá haverá "objetos necessários à prova de infração ou à defesa do réu". Ou seja, qualquer domicílio – mesmo que de pessoas que não são investigadas – no qual haja probabilidade de existir elemento de prova relevante para a investigação ou instrução criminal, pode ser local de busca.

Para complicar esse quadro de proteção insuficiente, a LGPD expressamente exclui do seu âmbito de incidência o tratamento de dados pessoais realizados para fins exclusivos de atividade de investigação e repressão de infrações penais.[10] É inquestionável que há uma proteção constitucional para os dados pessoais, a partir do direito à privacidade que, atualmente, vai muito além do direito de ficar só. A necessidade de proteção dos dados pessoais também é mais ampla – e distinta – que o direito de estar protegido pelas paredes do domicílio, do edifício em que a pessoa habita. Há muito mais coisas em jogo quando se pensa na proteção de dados pessoais. E para esse novo plexo de situações merecedora de proteção, no plano infraconstitucional, e em relação à atividade de investigação penal, há um déficit legislativo enorme.

10. A Lei nº 13.709/2018, na alínea "d" do inciso III do *caput* do art. 4º prevê a seguinte ressalva: "Art. 4º. Esta Lei não se aplica ao tratamento de dados pessoais: ... III - realizado para fins exclusivos de: ... d) atividades de investigação e repressão de infrações penais"

Pensem na seguinte indagação: "Você prefere sofrer uma busca domiciliar ou você prefere que alguém vasculhe o seu aparelho de telefone celular?" Creio não me equivocar que a grande maioria das pessoas considera mais invasiva a segunda situação. Diante da diversidade de funcionalidades e da enorme capacidade de armazenamento de dados, a invasão do aparelho de telefone celular - não vou nem falar notebook ou computador pessoal - é muito mais gravosa. Um aparelho

de telefone celular hoje tem muito mais informações e dados pessoais armazenados do que se constava antigamente, nós diários íntimos, escritos em papel, no qual cada pessoa anotava lá os acontecimentos especiais de sua vida. Um *smartphone*, se apreendido e examinado o seu conteúdo, permitirá que se faça uma reconstrução detalhadíssima de quase tudo que aconteceu no dia a dia de seu usuário. A todo momento, nós acessamos sites, enviamos e-mails, recebemos e transmitimos mensagens, por texto ou de voz, escrita de WhatsApp, Telegram ou outro aplicativo semelhante. Esse conteúdo massivo de dados pessoais gera uma necessidade intensa de sua proteção. E, no caso da investigação criminal ou instrução processual penal, é necessário que haja lei prevendo hipóteses estritas e restritas de possibilidade de seu acesso, sempre mediante prévia ordem judicial, para fins de persecução penal.

Some-se a essa fragilidade da legislação para investigação e para persecução penal uma característica da persecução penal dos últimos tempos. Hassemer, diz - ao meu ver, com muito acerto - que a persecução penal, recentemente, vem se concentrando na fase de investigação.[11] Percebe-se que em todas essas grandes operações há um crescente uso de meios invasivos de investigação, geralmente meios de obtenção de provas, que para serem eficazes atuam tendo como condição um fator surpresa: o investigado não saber que ele está sob objeto de investigação. E depois da coleta desses elementos, que são elementos que muitas vezes permitem uma profunda reconstrução histórica dos fatos, o que sobra para a fase processual propriamente dita, ou para uma instrução em contraditório,

11. Wilfried Hassemer (Perspectivas para uma moderna política criminal, *Revista Brasileira de Ciências* Criminais, v. 8, out-dez/1994, p. 46) já alertava, há décadas, que "a situação se torna mais dramática no novo Direito Penal, na área formal, no direito processual penal. A reforma do Direito Penal no campo formal consiste no aguçamento do sistema de investigação, do processo investigatório e mais nada. A reforma fez com que o processo investigatório tradicional passasse por uma revolução".

judicial, etc. é praticamente nada. O destino daquela sentença foi selado na investigação e no que se conseguiu obter através desses meios invasivos e secretos.

Basta constatarmos, por exemplo, na Lei de Organização Criminosa - além do Artigo 1º que define o que é organização criminosa e do Artigo 2º que tipifica o delito de pertencimento à organização criminosa - praticamente todos os demais dispositivos não são de uma lei penal de tipificação da organização criminosa, são de uma lei processual penal, e mais do que isso, da fase da investigação processual penal. E ela se destina a disciplinar os chamados meios de obtenção de prova, a começar pela colaboração premiada, passando pelo agente infiltrado, pela ação controlada, se reportando em relação a certas matérias regidas por leis especiais como interceptação telefônica e telemática nas leis especiais. Mais recentemente, o chamado "Pacote Anticrime", aprovado pela Lei nº 13.964/2019, disciplinou o que antes estava só nominado na Lei nº 12.850/2013, que é a captação de sinais ópticos, acústicos e eletromagnéticos, que também é um meio de obtenção de prova, acrescentando o art. 8-A à Lei nº 9.296/1996. Por tanto, nós estamos cada vez mais expostos a estes meios de obtenção de prova.

E aqui o Supremo Tribunal Federal, ao analisar a possibilidade do compartilhamento de dados pelo COAF diretamente ao Ministério Público, não fez uma distinção que é fundamental em termos de fluxo informacional: é preciso separar, de um lado, quem detém a informação, e

12. Foi fixada a seguinte tese: "1 - É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal, para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional. 2 - O compartilhamento pela UIF e pela Receita Federal do Brasil, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios".

de outro, quem detém o poder de persecução penal. O Plenário do STF, analisando a tese de repercussão geral no Recurso Extraordinário (RE) 1055941, considerou válido o compartilhamento com o Ministério Público e com as autoridades policiais dos dados bancários e fiscais do contribuinte obtidos pela Receita Federal e pela Unidade de Inteligência Financeira (UIF) sem a necessidade de autorização prévia do Poder Judiciário[12].

Toda vez que se concentra poderes, se facilita autoritarismo e aumenta a probabilidade de abusos. Por outro lado, ao se dividir o poder, é possível que haja alguma perda de eficiência, mas há ganhos nos controles daquele exercício do poder. Eis o meu momento Julia Roberts: o Supremo Tribunal Federal está errado! Isso porque, embora o COAF não trabalhe necessariamente com a persecução penal, ao Ministério Público cabe o exercício da ação penal e, como reconheceu próprio STF, tal instituição também tem poderes de realizar investigação criminal. Assim sendo, por meio da transmissão direta de informações pelo COAF, os órgãos de investigação terão acesso independentemente de controle jurisdicional – i.e., sem reserva de jurisdição – a dados pessoais sensíveis, abrangidos pela proteção da privacidade, que são as informações bancárias a fiscais dos cidadãos. O COAF trabalha com o recebimento, análise e disseminação de informações. Portanto, ainda que indiretamente, a polícia e o Ministério Público terão o poder informacional. Mas, quando se permite que o Ministério Público receba do COAF, sem uma barreira prévia de controle jurisdicional no caso concreto os dados bancários e fiscais, há concentração, em um mesmo órgão, do poder informacional e do poder de persecução penal. Isso é extremamente perigoso!

Uma coisa é assegurar o acesso à informação a agentes estatais, para a realização de atividade pré-delitiva, de natureza preventiva, visando evitar o cometimento do delito e

aprimorar a segurança pública. Outra coisa, é dar o acesso a tais informações aos agentes estatais que realizam atividade pós-delitiva, de persecução penal de um crime já praticado.

Por exemplo, é possível a análise de geolocalização de pessoas, mediante dados anonimizados, para saber locais de maior concentração de indivíduos e, com isso, planejar e executar uma atividade preventiva mais adequada de policiamento ostensivo em uma determinada região, num certo período do dia. Trata-se, contudo, de atividade que não é investigativa, até porque, não se está a dirigida a um delito específico, mas prevenir a prática geral de crimes. Situação muito diversa é, após o cometimento de um crime, acessar e utilizar dados pessoais para fins de investigação criminal ou instrução processual penal. No processo penal é muito clara a distinção entre uma polícia que realiza atividade com finalidade de prevenção, de um lado, e uma polícia que age no início da persecução penal, com o escopo de investigar crimes. A primeira age antes do delito, a segunda, após o crime ser cometido. Não se desconhece que, para muitos, essa concentração de atividade é tida como algo positivo. Há muitos defensores do chamado ciclo único das atividades policiais. Todavia, há um perigo em não distinguir tais atividades e conferir cada uma delas a um órgão diverso. Reconhecida a dignidade constitucional do direito à proteção dos dados pessoais, é necessário que a restrição de tal direito, para fins de investigação, seja regulamentada por lei, com critérios claros e objetivos das hipóteses de cabimento, dos sujeitos passíveis de serem afetados e do período de duração da medida. E tudo isso só poderá ocorrer mediante prévia análise judicial, verificando sua necessidade caso a caso. A proteção dos dados pessoais não pode ficar sem uma baliza legal.

Por fim, concluo com uma observação sobre em que hipóteses, de *lege ferenda*, devem se admitir essa restrição. No meu sentir, os casos legais de cabimento da restrição legal do sigilo

dos dados pessoais devem ser ainda mais restritos que os que autorizam a interceptação telefônica, admissível para todos os crimes punidos com reclusão. Justifico. Ao se analisar o potencial invasivo da interceptação telefônica – ou mesmo os casos em que se pode afastar judicialmente a inviolabilidade do domicílio –, dois aspectos devem ser considerados: um objetivo, referente ao potencial invasivo em termos de atingimento da privacidade do investigado; outro subjetivo, referente a quais sujeitos podem ser atingidos por uma decisão judicial que autorize o acesso ao conteúdo das conversas telefônicas aos órgãos de persecução penal.

Por exemplo, quando se realiza a interceptação telefônica, não se obtêm conversas apenas daquele investigado – i.e., do alvo da medida –, mas também, de outras pessoas que com ele dialogam. Também poderá se obter o conteúdo de conversas de outros indivíduos que usem a mesma linha telefônica, notadamente no caso linhas de telefones fixos. E não há como filtrar previamente o que será obtido. Logo, do ponto de vista subjetivo, é uma restrição que atinge direitos de pessoas que não estão sendo investigadas.

O mesmo raciocínio pode ser feito em relação à restrição da inviolabilidade do domicílio, para fins penais. Nesse ponto, é importante distinguir duas atividades sucessiva que não se confundem. Embora seja comum usar a expressão "busca e apreensão", com se fossem duas coisas que inseparáveis, tal impressão é equivocada. É possível que haja busca, sem apreensão (p. ex.: no caso em que a coisa procurada não é encontrada) como também pode haver apreensão sem busca (p. ex.: de algo cujo local em que se encontra já é conhecido). Por que na atividade domiciliar essa distinção é importante? A busca ou varejamento é realizado para verificar se já no local coisas, armas, instrumentos delitivos ou outras coisas que interessem à prova do crime. É preciso distinguir, de um lado, quais são

os elementos encontrados que são importantes para a investigação, e de outro, quais não lhe dizem respeito. Os elementos relevantes encontrados na busca, serão num momento sucessivo, apreendidos. Os que não lhe dizem respeito, ficarão onde foram encontrados. Evidente que atividade de procura das coisas, durante as buscas domiciliares de locais habitados por mais de um indivíduo, inexoravelmente dará aos investigadores acessos a coisas de terceiras pessoas que não estão sendo investigadas. Durante a busca, serão examinadas, e se não estiverem no seu objetivo, não serão apreendidas. Mas o simples exame já é uma forma de restrição da privacidade de quem não está sendo investigado.

Se esses conceitos forem empregados com relação aos dados pessoais, e para a utilização desses dados pessoais para fins de investigação criminal, me parece que o potencial de invasão da privacidade é maior, consideravelmente maior, do que o potencial de invasão das interceptações telefônicas. Esta somente captara o conteúdo de diálogos telefônicos realizados no período da interceptação. Aquela, poderá obter – a depender da capacidade de armazenamento de informações no meio em questão (um provedor de e-mail, um notebook, ou um pen-drive) – uma infinidade de fotografias e arquivos de textos, ou registros de atividades diárias em agendas, referentes a vários anos, além de conversas de vozes gravadas e enviadas por aplicativos de mensagens, planilhas com dados financeiros, geolocalizações do usuário etc.

Por exemplo, o parâmetro da busca e da apreensão domiciliar, cabível para qualquer delito ou qualquer contravenção penal, se for aplicado para obtenção judicial de dados pessoais para fins de investigação, será excessivamente amplo e desproporcional, diante da necessidade de proteção constitucional. Já na interceptação telefônica e telemática, o critério adotado pelo legislador foi mais restrito: crimes punidos com reclusão.

A justificativa é que, para contravenções penais ou para crimes punidos com detenção, é preferível abdicar de tal meio de obtenção de prova na busca de uma melhor reconstrução histórica dos fatos, mas com isso preservar a confiança dos indivíduos em que, ao utilizarem os aparelhos telefônicos, sua manifestação do pensamento será reservada e seu conteúdo não será conhecido por terceiras pessoas, salvo se estiver sendo investigado por um crime grave. Por isso é insuficiente e frágil aplicar à proteção de dados pessoais o mesmo regime legal da busca e apreensão que, em percepção penal por qualquer infração penal. Logo, para fins de investigação criminal, um juiz poderia autorizar a obtenção de dados pessoais de investigado por uma simples contravenção penal, ou um crime de menor ofensivo, que admite uma transação penal com a desnecessidade de processo. Se assim o for, em toda e qualquer investigação criminal será cabível o afastamento judicial do sigilo dos dados pessoais.

Não sendo suficiente e adequado aplicar, por analogia, o regime dos meios de obtenção de provas já existentes, é de se reconhecer a necessidade urgente de elaboração de disciplina legal específica, e bastante restritiva das hipóteses em que, mediante ordem judicial, o sigilo dos dados pessoais pode ser afastado para fins de investigação penal. Por isso, ao realizar um juízo de proporcionalidade em sentido estrito, o legislador deve permitir a medida mais invasiva – no caso, o acesso a dados pessoais –, em casos mais restritos que os que admite a interceptação telefônica – no caso, todos crimes punidos com reclusão.

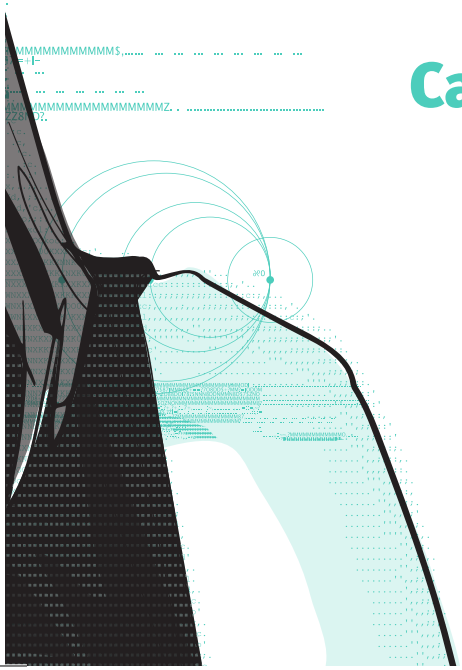
Ainda que esteja em vigor a LGPD, tal regime exclui expressamente sua aplicação ao processo penal. Logo, continuarão as discussões sobre ser ou não possível o emprego da analogia; em caso positivo, a analogia com qual regime; uns vão fazer analogia com a interceptação eletrônica, outros vão

procurar suprir a lacuna, com o regime legal das buscas e apreensões... Esse é um cenário extremamente perigoso. Nós temos visto que os tribunais, inclusive o Supremo Tribunal Federal, mesmo nos casos em que há lei, têm avançado sobre a legalidade, com a eufemística 'interpretação" criativa. A insegurança será absurda, nas situações em que não há lei, deixando os tribunais absolutamente livres para julgarem, e restringirem direitos fundamentais com bem entenderem. O princípio da legalidade ainda é o mais potente instrumento de proteção contra os abusos estatais, inclusive do próprio Poder Judiciário. Sem a proteção da legalidade, nossos dados pessoais estarão facilmente disponíveis aos agentes de persecução penal, e nós estaremos sujeitos a abusos das mais variadas ordens.

04.

SISTEMAS DE VIGILÂNCIA EM MASSA E PROTEÇÃO DE DADOS: CENÁRIO NA SEGURANÇA PÚBLICA

Carolina Ricardo[1]



1. O presente texto se baseia em apresentação oral feita no painel "Sistemas de vigilância em massa e proteção de dados" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

O texto aqui apresentado é a sistematização da minha apresentação sobre "Sistemas de vigilância em massa e proteção de dados: cenários da segurança pública", feita no Congresso do InternetLab em 2020. Quando fui convidada para o evento, expliquei que meu olhar seria muito mais sobre como a segurança pública tem incorporado ferramentas de vigilância e de tecnologia para enfrentar os desafios de criminalidade e violência; e menos uma discussão aprofundada sobre os riscos à privacidade.

A apresentação se baseou em análises realizadas pelo Instituto Igarapé[2] e de alguns outros pesquisadores cujas referências seguem no texto e teve o seguinte percurso: 1) breve panorama do uso dos diferentes sistemas de vigilância na segurança pública no Brasil, o que mais tem sido usado; 2) apontar os efeitos e os resultados desses sistemas. Importante não jogar o bebê com a água do banho – há também resultados importantes também do ponto de vista da segurança pública que valem a pena ser olhados e pensados quando refletimos sobre direito à privacidade?; e depois 3) entrar na discussão específica das limitações desses sistemas, quando será possível fazer uma discussão mais aprofundada sobre os riscos e dilemas.

2. https://igarape.org.br/videomonitoramento-webreport/

PANORAMA DOS SISTEMAS DE VIGILÂNCIA NA SEGURANÇA PÚBLICA NO BRASIL

Para começar, é importante conhecer as diferentes ferramentas pelas quais os governos têm investido no Brasil em termos de segurança pública e tecnologias de vigilância. A primeira delas é o CFTV (circuito fechado de videomonitoramento), que é um sistema de vídeo monitoramento clássico, num ambiente fechado (como num shopping centre ou num grande estacionamento, ou prédios públicos), mas há também os sistemas interligam câmeras, como de agências bancárias, de

vigilância de comércios, entre outras. A versão mais recente desse modelo foi lançada por João Dória, quando prefeito de São Paulo, o programa City Câmeras, com integração maciça de muitas câmeras de pessoas físicas, de residências, de comércios, para ter algo como um "Big Brother", esse grande olhar sobre o que acontece nas ruas da cidade.

Esse é o mecanismo clássico sobre o qual há mais estudos e o que mais é implantado, sobretudo, nas cidades. Em geral, as prefeituras investem muito nesse tipo de ferramenta, que cria uma ideia de uma prevenção situacional - você olha e monitora a cidade, consegue identificar alguns tipos de crime em andamento, algumas situações de desordem. Então esse é um modelo mais clássico.

Há um segundo modelo que é o reconhecimento de placas veiculares (OCR). Que também são câmeras de vigilância, mas já com uma tecnologia mais elaborada para fazer leitura de placas de veículos furtados ou roubados. Essa é uma ferramenta que depende menos do olhar humano; no modelo anterior, em geral, você tem centrais de monitoramento com pessoas observando aquelas imagens. Na tecnologia OCR, há a leitura de placas veiculares e, a partir de um banco de dados de veículos roubados ou suspeitos, há um aviso automatizado quando o sistema reconhece uma placa de carro que está no cadastro como roubado ou furtada, quando passa pela câmera. A partir do aviso, os órgãos de segurança, as polícias, as guardas municipais, vão atrás desse veículo que apareceu como sendo roubado ou furtado. Trata-se de uma tecnologia mais elaborada que cruza dados das placas dos veículos furtados. São os cercamentos eletrônicos, ferramentas muito comuns na entrada e saída de cidades.

O terceiro modelo é o da tecnologia de reconhecimento facial, em que há bancos de dados de imagens de fotografias de pessoas e isso é cruzado com outras informações, muitas vezes informações civis e criminais, para identificação de

"criminosos" ou suspeitos - pessoas que podem estar sendo procuradas. Houve uma implantação mais massiva e recente dessa tecnologia no Brasil, quando há também um aumento de riscos derivados do uso dessa tecnologia.

Uma quarta tecnologia cuja discussão é crescente - sobretudo a partir do caso George Floyd nos Estados Unidos - e no Brasil por conta das discussões de violência policial e racismo estrutural, que tem entrado com mais força no debate sobre a atuação policial, é a câmera corporal, o *Body Camera*. Trata-se da câmera acoplada na farda do policial, e permite o monitoramento da atividade do policial, de sua interação com o público. Temos algumas experiências em caráter piloto no Brasil, a polícia militar de São Paulo está justamente incorporando agora essa tecnologia.

E, por fim, o policiamento preditivo, com experiências muito pontuais no Brasil. Trata-se da possibilidade de organizar e orientar a atuação policial a partir de uma análise preditiva derivada do cruzamento de bancos de dados de local de ocorrência de crime, com dados de pessoas que já tenham sido alvo de algum tipo de registro criminal, locais de ocorrência. Isso gera um algoritmo e é possível, em tese, prever locais e situações em que o crime pode ocorrer. É uma ideia de se antecipar um pouco as situações criminais e orientar o aparato de segurança em função dessa antecipação. São essas as cinco principais ferramentas no estado da arte de tecnologia e segurança pública no país que eu gostaria de debater.

EFEITOS E RESULTADOS DOS SISTEMAS DE VIGILÂNCIA PARA A SEGURANÇA PÚBLICA NO BRASIL

Quais são os efeitos e resultados do uso dessas tecnologias? Em relação ao CFTV, já há mais estudos e análise sobre seus

/ OUTRO PROBLEMA RELEVANTE É A CONFORMAÇÃO DO BANCO DE DADOS, QUAIS AS FOTOS QUE COMPÕEM O BANCO FOTOGRÁFICO, QUAIS OS CRITÉRIOS, E A GERAÇÃO DE FALSOS POSITIVOS /

efeitos. Em geral se identifica algum tipo de redução do crime contra o patrimônio. Não há dados estruturados, o que é um ponto de atenção. Há pouca avaliação sólida ainda sobre isso, sobretudo no Brasil, em relação ao uso das imagens de CFTV em investigações criminais. Mas é comum que as imagens sejam solicitadas em casos de crimes investigados pela polícia civil, e aí há o desafio do tempo de armazenamento das imagens, para o qual não um critério sólido, variando muito, impedindo a alguns casos que a imagem seja usada por falta de armazenamento.

O Instituto Sou da Paz realizou uma pesquisa há alguns anos em Ribeirão Preto e em Campinas sobre o uso da CFTV e o funcionamento das centrais de vídeo monitoramento, para os quais não encontramos dados quantitativos sobre resultados e impactos sistematizados e nem passíveis de sistematização, na análise qualitativa, no entanto, quando foram entrevistados gestores, policiais e outros funcionários, foi possível identificar o uso dessas imagens para investigação criminal. E, em geral, eram imagens de vias públicas. Há os casos dos sistemas de vídeo monitoramento em áreas privadas, como dentro dos edifícios e elevadores. Foi o caso bárbaro do menino que morreu em Recife, o menino negro que foi abandonado e entrou no elevador em 2020. Aquela é uma imagem interna em um espaço privado que foi usado para apuração de uma situação bastante grave. Esse tipo de uso acaba sendo, portanto, o mais clássico. Há limites claros para esse uso, como o local e posicionamento da câmera, o tipo de equipamento, mas esse é um efeito importante para segurança pública desse tipo de tecnologia.

Já em relação à tecnologia OCR, para monitoramento de placas veiculares, o acompanhamento de seus efeitos é feito com base na quantidade de veículos aprendidos a partir da identificação pelo sistema. Não há monitoramento que

permita aferir se esse tipo de tecnologia reduz ou não reduz crime. O monitoramento da quantidade de veículos que foram apreendidos ou outras ocorrências criminais identificadas a partir daquela tecnologia, é muito importante, mas não suficiente. Quer dizer, se queremos ter mecanismos de prevenção de crime que impactam também nas tendências, apenas aferir esse quantitativo operacional não é suficiente. Mas é um tipo de monitoramento que se faz.

Em relação à tecnologia de reconhecimento facial, do que foi possível apurar, se monitora também o número de prisões feitas a partir do reconhecimento facial. Não há avaliações consistentes sobre outros resultados.

Em relação ao uso de câmera corporal pelas polícias, existem muitas avaliações que ainda são inconclusivas[3]. Não há garantia que o uso da câmera melhora a relação da polícia com a sociedade, porque depende muito do que é feito com esse monitoramento. Se, no caso dos policiais, não há uma responsabilização clara após o uso da câmera corporal para identificar algum tipo de abuso, o efeito não é tão significativo. Outro efeito interessante diz respeito ao uso dessas imagens pelos próprios policiais para fornecer provas de que aquela situação de abuso não aconteceu. Isso ainda é novo, o que gera uma importante oportunidade para olhar

3. https://www.bloomberg.com/opinion/articles/2020-07-29/police-body-cameras-why-don-t-they-improve-accountability

4. Ainda que não tenhamos encontrado dados mais aprofundados sobre o tema, consideramos relevante compartilhar algumas reflexões sobre o policiamento preditivo nos EUA: *"Numa busca cada vez maior por não somente prever os crimes, como também por antecipá-los e evitar que aconteçam, a polícia de Chicago passou a desenvolver uma lista de possíveis agentes de ações criminosas e, em alguns casos, vai pessoalmente avisar que eles estão sendo acompanhados de perto, e que caso cometam algum crime ou infração, serão punidos"* (Citação de https://bigdatacorp.com.br/big-data-e-policiamento-preditivo/, acessoem26/08/2020) –estigmatização, antecipação, livre arbítrio *"Além disso, também nos Estados Unidos, algoritmos estão sendo utilizados para avaliar a concessão ou não da liberdade condicional a alguns presos. Seria esse caso a substituição do papel de um juiz? E mais uma vez, seria justo que alguém fosse julgado e condenado por uma possibilidade que é tomada como verdade absoluta?"* (Citação de https://bigdatacorp.com.br/big-data-e-policiamento-preditivo/, acessoem26/08/2020)

essa lógica de apuração investigativa, não só jurídica, mas no âmbito da própria polícia, da corregedoria, o uso dessas imagens na apuração administrativa das infrações e relatos de abusos envolvendo policiais.

Quanto ao policiamento preditivo, não encontramos informações sobre seus impactos[4].

LIMITAÇÕES DOS SISTEMAS DE VIGILÂNCIA[5]

As tecnologias de CFTV são mais eficientes para coibir crimes contra a propriedade, têm efeitos limitados na redução de crimes e muitos problemas de instalação. Então, se não há monitoramento ativo, se não há manutenção periódica, há problemas que inviabilizam os efeitos positivos. Por exemplo, se a câmera é instalada de forma equivocada e começa a filmar o nada ao invés do local inicialmente previsto. Identificamos muitos casos em que a câmera na verdade monitora muito pouco. E quando depende do monitoramento humano, o desafio é muito maior. Sem um bom planejamento, rotina, rodízios, estímulo e formação para quem monitora, há riscos de uma baixa eficiência no monitoramento. É comum que policiais ou profissionais afastados das atividades rotineiras sejam alocados em centrais de video monitoramento, o que gera um trabalho pouco estimulante, inviabilizando a eficiência dessas centrais.

5. https://igarape.org.br/videomonitoramento-webreport/

As tecnologias de reconhecimento de placas tem o mesmo problema de posicionamento da câmera, mas também gera erro de leitura nos caracteres. Às vezes a leitura da placa entende uma letra errada e gera falso positivo.

E, no caso do reconhecimento facial, há o problema com o ambiente das câmeras, mas há maior propensão à erro quan-

do a tecnologia é comparada a sistemas de reconhecimento de íris ou de impressão digital. Outro problema relevante é a conformação do banco de dados, quais as fotos que compõem o banco fotográfico, quais os critérios, e a geração de falsos positivos, por vezes baseados em vieses discriminatórios, que gera erros e injustiças.

RECONHECIMENTO FACIAL NO BRASIL

O Instituto Igarapé produziu um infográfico[6] que fez o mapeamento do status do reconhecimento facial no Brasil, no qual é possível conhecer como vem sendo utilizado. Desde 2011 vem sendo utilizado o reconhecimento facial no Brasil, tornando-se especialmente popular a partir de 2019. Vemos que está bastante distribuído no Brasil, com alguns estados que não contam com reconhecimento facial, mas em São Paulo, por exemplo, muitas cidades contam com a tecnologia, Campinas, Santos, Limeira; no Espírito Santo; alguns estados do Nordeste; Paraná, Santa Catarina... De fato, o Brasil tem incorporado essa tecnologia.

6. https://bityli.com/FxNhB

Alguns setores têm utilizado o reconhecimento facial. Ele é prioritariamente utilizado no setor de transporte, para evitar fraude no uso de transporte público, por exemplo, depois para segurança pública, em seguida para o controle de fronteiras e educação.

No setor de educação, por exemplo, são utilizadas tecnologias de reconhecimento facial para autorizar ou proibir matrícula em uma escola. É um meio necessário para que uma criança possa ser matriculada em uma escola, por exemplo. É um tipo de uso em que a tecnologia pode ser importante, mas também pode ser restritiva.

PRINCIPAIS DILEMAS DO RECONHECIMENTO FACIAL

Existem alguns dilemas que identificamos em relação ao reconhecimento facial. A primeira questão é em relação à privacidade. No diálogo entre privacidade e segurança: como essas imagens são armazenadas e com que garantia de segurança? De onde elas são obtidas? Há consentimento das pessoas quando elas são fotografadas por algum aparelho, para que essa foto vá fazer parte de um banco de reconhecimento facial, ou não há consentimento? Há cruzamento de outras bases de informação sobre a vida civil e criminal das pessoas? Há clareza disso? Quais são os critérios? Essas perguntas precisam ser claramente respondidas, para que o uso garanta privacidade e segurança sobre os dados e imagens.

Outra questão se relaciona às bases de dados com vieses. Existe a possibilidade de falsos positivos e a dificuldade de reconhecimento em relação à questão racial, por exemplo, com banco de dados com fotos de pessoas brancas, de pessoas negras e sem um mecanismo de compliance muito claro para organizar esse monitoramento, há riscos de injustiças e ineficiência. Por exemplo, um falso positivo gera uma ação por parte do órgão que está fazendo monitoramento. A tomada de decisão para essa ação tem que ser muito cuidadosa, porque um falso positivo pode gerar um impacto muito sério para a vida de uma pessoa que pode ter sido identificada como um possível criminoso e que não tem nenhuma relação com o caso.

Outro aspecto é a a falta de transparência, de critérios e de adequação à Lei Geral de Proteção de Dados Pessoais. Isso gera desconfiança sobre a tecnologia - que pode ser usada de forma positiva, mas se começamos sem cuidados com esses problemas, gera-se descrença, inclusive sobre as instituições que agem a partir de um estímulo equivocado de um falso positivo, por exemplo. Por fim, é preciso muito cuidado com

a ampliação desmedida do uso como forma de controle de acesso a serviços, por exemplo, acesso a escolas e serviços de saúde, já que há o risco de se limitar o acesso a direitos fundamentais a partir dessa ampliação desmedida do uso.

FORMAS MAIS SEGURAS PARA O RECONHECIMENTO FACIAL

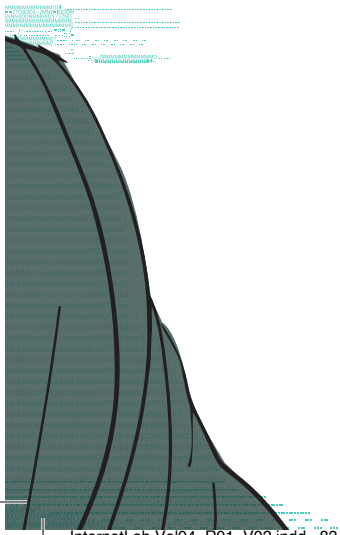
Por fim, apresentamos caminhos para o melhor uso do reconhecimento facial no Brasil. O pesquisador Rodrigo Dias de Pinho Gomes[7], do Rio de Janeiro, elaborou propostas que os mecanismos de reconhecimento facial sejam utilizados de maneira mais segura. Algumas delas são: i. transparência e clareza por parte das autoridades de quais são os critérios usados para compor os sistemas, com processos públicos e participativos, e a criação de comitês multisetoriais que permitam a construção e a fiscalização dos sistemas; ii) a existência de revisão permanente dos algoritmos para que se consiga diminuir os erros e sobretudo as decisões provenientes desses falsos positivos e problemas do sistema; iii) a realização de testes periódicos para termos um percentual mínimo de acertos como critério para o uso da tecnologia, para não ficar na mão desses erros e dos falsos positivos; iv) clareza sobre a finalidade para o uso da tecnologia; v) que o arcabouço de garantias de direitos da pessoa humana, dos direitos individuais, seja sempre o plano de fundo para implantação da tecnologia.

7. https://bityli.com/cvhNT

05.

BIG DATA E DEVIDO PROCESSO: PODER PENAL PREDITIVO

Maurício Dieter[1]



1. O presente texto se baseia em apresentação oral feita no painel "*Big data* e devido processo: poder penal preditivo" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

Agradeço ao convite do InternetLab, é a primeira vez que eu estabeleço um diálogo com vocês, então obrigado pelo convite, que foi mediado também pela Nathalie, minha ex aluna na pós-graduação.

Eu tenho um desafio temporal que é tratar da minha tese de doutorado defendida há oito anos, agora em 15 minutos. Demorei 4 anos para fazer esse doutorado, razão pela qual é um pouco difícil tentar colocar em 15 minutos a síntese do que eu consegui elaborar.

Eu vou contextualizar essa pesquisa. Eu comecei a investigar a política criminal atuarial a partir de uma certa perplexidade com o fundamento material do juízo de censura na culpabilidade no conceito analítico de fato punível, a estrutura do conceito de culpabilidade, que fundamenta o juízo de censura penal - ele depende ainda de uma base metafísica. O máximo que a dogmática penal alemã, por exemplo, conseguiu desenvolver em termos de fundamento material da censurabilidade é a dirigibilidade normativa, mas isso ainda reserva um campo de *agency*, de agência, muito grande diante das possibilidades e escolhas concretas sem explicar o que determina a censura de uma escolha concreta em uma circunstância específica.

Então, na busca de um fundamento material da culpabilidade, Eugenio Raúl Zaffaroni havia indicado o fundamento material da culpabilidade estruturada a partir da vulnerabilidade, aos processos de criminalização primária e secundária. Depois havia a sugestão do Sr. Juarez Cirino dos Santos que indicava alteridade como fundamento da censura, eu comecei a pesquisar qual poderia ser um fundamento alternativo e me deparei com a prognose de reincidência como esse fundamento. Fiquei bastante incomodado com aquilo e fui investigar o tema a fundo e isso se tornou no meu doutorado - passei quatro anos investigando isso a fundo.

Mas seja como for, não achei no Brasil interlocutores sobre esse tema, especialmente do ponto de vista crítico - havia muita apologia nos Estados Unidos, muita condescendência com esse método de determinação de responsabilidade penal e de disciplina do indivíduo dentro do sistema de Justiça Criminal, mas havia pouca crítica. Tinha críticas do Malcolm Feeley e Bernard Harcourt, mas não achei que aquilo tinha, digamos, a densidade suficiente para sustentar uma tese. E foi na parceria com o professor Sebastian Scheerer na Universidade de Hamburgo, onde eu realmente consegui o acúmulo teórico necessário para desenvolver uma perspectiva original que fundamentasse a crítica, então, da política criminal atuarial.

O que é o atuarialismo? O atuarialismo é, basicamente, quando você aplica critérios de prognose para determinar uma tomada de decisão. Para introduzir isso para as pessoas que não são familiarizadas com o tema, dá para dizer que o atuarialismo, a política criminal atuarial, se desenvolve dentro de uma das três tendências prementes da política criminal contemporânea - no trânsito do século XX para o XXI nós tínhamos três tendências predominantes: o populismo, o chamado internacionalismo e o gerencialismo. Dessas três perspectivas não há exatamente um conflito, mas uma convergência na medida em que elas reestruturam o discurso punitivo, que atende evidentemente a uma demanda por ordem, de maneira em que eles suprem as suas lacunas, as suas elipses respectivamente.

Então, às vezes quando você tem déficits gerencialistas, as alternativas populistas fundamentam programas punitivos. Da mesma forma os tratados internacionais que implicam criminalização, às vezes em favor dos direitos humanos, às vezes contra eles - por exemplo a Lei da Lavagem de Dinheiro, que é uma infiltração horrorosa classicamente, digamos, colonizadora que disciplina o mercado financeiro no país que foi imposta de cima para baixo - ou você tem tratados

internacionais de direitos humanos que tentam controles de conformidade em relação a proteção. Então entre populismo, internacionalismo e gerencialismo existe, na verdade, uma confluência, eles acabam se abastecendo mutuamente para definir um programa de política criminal que mantenha o controle social sobre direção pragmática e discursiva.

A política criminal atuarial é, na verdade, uma distribuição de justiça conforme o grupo de risco ao qual a pessoa pertence. Em termos gerais, vocês conseguiriam enxergar um exemplo básico de justiça atuarial, tanto quanto for justiça isso, na indústria dos seguros em relação ao veículo automotor. Um homem jovem, ainda que seja um bom motorista, vai pagar o seguro do seu veículo um valor muito maior do que uma velha senhora. Por quê? Porque homens jovens estão vinculados ao maior grupo de risco para acidentes fatais ou com perda total. Portanto não importa tanto o que você faz mas o grupo de risco ao qual você pertence, o custo da *policy* é tanto maior quanto mais vinculado ao grupo de risco o qual você pertence, aqui no caso, por exemplo, definido por critérios etários e sexuais. E a ideia de você ter uma justiça atuarial no sistema de Justiça Criminal implica você começar a utilizar prognósticos acumulados e o longo acúmulo desses dados vai constituir um repertório de *big data*, a partir do prognóstico de reincidência que uma pessoa tem no sistema criminal - essa é a ideia geral.

O desenvolvimento histórico disso é bastante interessante. Isso acontece ainda na alvorada do século XX, então em 1923 temos as primeiras experiências nas comissões para livramento condicional, chamada *parole boards* no estado de Illinois. Aqui tem a importância de um criminólogo estadunidenses bastante famoso chamado Ernest Burgess que era uma das proeminências da Escola de Chicago, e ele estabelece o primeiro mecanismo prognóstico que ajuda as comissões para

livramento decidirem se vão ou não conceder livramento condicional para as pessoas que submetem a essa entrevista. O prognóstico se estabelece com 22 variáveis que definem uma certa tendência de mecanismos prognósticos de reincidência.

Depois, comparativamente, nos Estados Unidos, a pesquisa mais próxima disso é a do casal Sheldon e Eleanor Glueck que estabelecem 13 fatores que estariam conectados à reincidência - depois a gente vai mencionar alguns dos fatores que se repetem - e essa pesquisa segue: Clark Tibbitts, George B. Vold, Elio D. Monachesi, Courtlandt Churchill Van Vechten Jr., Ferris F. Laune, Albert J. Reiss Jr., Louis Guttman, John L. Gillin, Lloyd Ohlin e Daniel Glaser nos anos 1950. Então você tem dos anos 1920 até os anos 1950, um monte de pesquisadores que tentam desenvolver mecanismos que digam para uma comissão de livramento se o sujeito deve ou não sair da prisão, de acordo com critérios que indicam vínculo estatístico com o risco de reincidência de acordo com experiências frustradas de pessoas que tiveram livramento concedido, mas violaram as condições de livramento e retornaram à prisão.

A característica geral desses mecanismos prognósticos é a definição do risco pelo comportamento e situação de vida marginal. Lembremos que em 1920 a criminologia etiológica individual, essa criminologia que pressupõe a existência de sujeitos desviantes, é bastante associada a um preconceito do comportamento antiestadunidense e um exagero no peso da reincidência é a característica geral desses primeiros instrumentos prognósticos. Eu poderia citar aqui pessoas que desenvolveram mecanismos aplicáveis na época: Peter Hoffman e James Beck com o importante *Salient Factor Score* (SFS), que depois ficou conhecido como 4x6 porque ele cruzava uma tabela com 4 fatores no eixo horizontal, no eixo vertical 6, e você cruzava o tipo crime que o sujeito praticava com a perigosidade que ele representava de acordo com esse

prognóstico - cruzava os dois elementos e você tinha um risco de reincidência definido.

Os elementos mais comuns desses mecanismos prognósticos da primeira metade do século XX eram: quantidade de condenações que o sujeito já teve; prisões anteriores, quer dizer, penas aplicadas e executadas; idade a época do primeiro delito, prisão ou condenação; o histórico de uso de drogas; condenação por furto ou fraude; alcoolismo, que se diferenciava do uso de outras drogas da época, especialmente na época de *prohibition;* trabalho; vida escolar; violação de *probation* ou *parole* em episódio anterior; e, finalmente, natureza do relacionamento social mantido durante a vida carcerária, ou seja, a existência de família, prole, etc.

Esse sistema de prognóstico entra em decadência no final dos anos 1950 porque o sistema de Justiça Criminal dos Estados Unidos em geral vai abandonando o sistema de sentenças indeterminadas que trabalham com livramento condicional, e você tem emergência de um modelo chamado *true sentencing*, que em uma tradução difícil para o português eu diria que é um sentenciamento "para valer". Então aquela ideia de que o sujeito recebia uma pena que vai ficar preso não menos que três anos, ou no máximo dez anos, podendo sair antes etc. isso vai para um sistema em que a sentenças são rigorosamente determinadas. E se as sentenças são determinadas pelo juiz de maneira rigorosa, não existe mais tanta necessidade de comissões de livramento que decidam a partir de critérios atuariais a soltura ou não de alguém.

E o que acontece em seguida, nos anos 1970: o caso relativo dos prognósticos é recuperado, mas sob um outro signo, que é da rejeição da prevenção especial positiva. A prevenção especial positiva, como se sabe, define o ideal de ressocialização, ou reeducação do sujeito, como objetivo da aplicação e execução de uma pena privativa de liberdade. Na medida em que - e

/ A POLÍTICA CRIMINAL ATUARIAL É, NA VERDADE, UMA DISTRIBUIÇÃO DE JUSTIÇA CONFORME O GRUPO DE RISCO AO QUAL A PESSOA PERTENCE /

podemos, por exemplo, citar o ensaio conhecido do Robert Martinson de 1964 que fala "nothing works", nada funciona - a política estadunidense em matéria jurídica criminal se divide em duas posições. A primeira que é a abolição da pena, a abolição da prisão, porque ela não consegue reeducar ninguém apesar de todos os esforços e dinheiro, e a outra posição que diz: bom, se a prisão não prende, pelo menos ela é capaz de incapacitar os criminosos, capaz de neutralizar criminosos perigosos. E aí se estabelece, como a direita sai vencedora desse debate, uma luta para separar o joio do trigo, que se traduz na busca de alvos prioritários. É aquela conversa furada que já ouvimos tantas vezes de que a coisa não é prender muito, é prender bem - a experiência mais fracassada de tentar prender bem se articulou precisamente com esses mecanismos prognósticos.

Esse foco na prevenção naturalmente começa na busca dos chamados delinquentes juvenis e os criminosos de carreira. E aí eu posso citar o texto de Figlio, Sellin e Wolfgang de 1972 que apresenta a ideia de um *fator k* de três variáveis que tenta definir quem é o adolescente criminoso potencial do futuro que vai se converter em um reincidente crônico. As três variáveis são, basicamente, a idade em que ele teve o primeiro contato com a polícia; a natureza da infração praticada; e a raça do indivíduo. Como dá para ver desde logo, esse é um mecanismo que reforça a seletividade racial da justiça criminal por definição.

Depois eu posso mencionar, por exemplo, o texto e o mecanismo atuarial de prognóstico de Donald West e David Farrington, que demonstram a ideia do reincidente crônico. Eles dizem que se vinga a ideia do reincidente crônico e no Canadá isso vai produzir dois mecanismos de prognóstico para meninos e meninas, respectivamente conhecidos pelos seus anagramas Earl B e Earl G, que é o *early risk assessment list*. Todos esses mecanismos prognósticos, eles têm esse nome comercial, esses anagramas que reduzem as letras dos

mecanismos para se tornarem mais comerciais. No fundo é isso que está em jogo também, tentar vender esses mecanismos prognósticos para definir a segurança pública onde eles podem ser comercializados.

Em relação aos adultos, há um foco na repressão em busca dos chamados reincidentes crônicos e tem o estudo, por exemplo, do Mark Peterson, do Harriet Braiker em 1981 e o pior deles, o que produziu o maior dano, que é o ensaio do Peter Greenwood. Eu chamo ensaio embora seja praticamente um relatório, até o nível teórico dele é muito baixo, mas é um relatório do Peter Greenwood, de 1982. Peter Green é conhecido: ele é um conservador dos Estados Unidos que justifica uma repressão bastante violenta e em 1982 ele publica esse texto que é dirigido às autoridades públicas, quase como um manual de como fazer, e ele apresenta os *seven factors scale*, que vai trabalhar com sete critérios que são critérios dominantes na maior parte dos prognósticos para definir quem são os reincidentes crônicos. O primeiro elemento é a existência de reincidência específica; permanência na prisão por mais de 50% de tempo nos últimos dois anos; existência de condenação antes dos 16 anos; passagem por instituição destinada a menores infratores; uso recente de drogas ou na adolescência; e desemprego por mais de 50% do tempo nos últimos dois anos.

Esses estudos são seguidos por propostas do Mark Moore, Terence Thornberry, Terrie Moffitt e Avshalom Caspi, que vão projetar isso novamente, de volta para o controle de possíveis reincidentes crônicos já identificados nos primeiros anos de vida. Tem, nesse período dos anos 1980, muito poucas vozes críticas contra o uso disso, mas vale mencionar o texto de Lyle Shannon, Rudy Haapanen, John Laub e Robert Sampson, embora com menos ênfase já nos anos 1990. Como vocês podem ver, é muita coisa - só para dizer que isso tem uma história, tem uma bibliografia grande nisso.

Nos anos 1990 em diante, a coisa vai basicamente se destinar contra os chamados predadores sexuais. O texto de Stuart Miller, Simon Dinitz e John Conrad, o chamado *Dangerous Offender Project*, vai coincidir com profundas alterações no sistema de Justiça Criminal dos Estados Unidos a partir de modificações em leis que vão autorizar ampla vigilância sobre os chamados predadores sexuais, mas não apenas - inclusive vai autorizar a incapacitação civil, não pelo direito penal, das pessoas definidas como perigosas nesse contexto. E de certa maneira, a colonização do sistema da Justiça Criminal por essa maneira operacional vai levar a uma diminuição da discricionariedade da magistratura ou mesmo da polícia, ou mesmo do Ministério Público, sobre quem prender, quem acusar, quem condenar e por quanto tempo. Então a primeira coisa que esse sistema faz é tornar mais ou menos inúteis os juristas e, embora eles tenham boas razões para fazer isso, ao custo certamente da violação sistemática de direitos humanos.

Então, para encerrar, qual é uma avaliação crítica desse processo? Bom, a primeira avaliação, bastante superficial, que não é criminológica, é normativa, quer dizer: aquilo que diz respeito propriamente aos juristas, não tem muito peso científico, é realmente um suporte mais normativo. Claro, estou aqui constando a diferença entre criminologia e direito como ciência e técnica, porque o direito só vai ser uma ciência se você mudar muitos pressupostos do que se entende epistemologicamente por ciência sem dizer que, com isso, ele é menos importante, simplesmente são formas epistêmicas distintas.

Mas vamos lá: primeiro você vai ter uma perda da legitimidade dos direitos humanos porque a medida que você operacionaliza isso, você vai ter contradições radicais com o princípio da legalidade, da lesividade, da proporcionalidade e da humanidade das penas. Mas o problema mais óbvio, claro, é a negação do princípio da culpabilidade, porque você vai

ter uma criminalização que não é pelo o que o sujeito fez e nem mesmo pelo que ele é, como já seria horrível ao direito penal do autor, você vai criminalizar o sujeito pelo grupo social de risco ao qual ele pertence. Quer dizer, isso é uma forma de você regredir, em matéria de direitos fundamentais, a um contexto obscurantista, embora elevado a uma certa racionalidade tecnocrática. Então é uma pura expressão de um direito penal do autor pós-moderno, o que é um erro em todas as suas dimensões.

E, no entretanto, essa crítica normativa diante dos atuariais, as pessoas que defendem esse sistema, vai ter uma resposta cínica que vai dizer: olha, pode ser que erremos também com o atuarialismo, mas não é como os juristas estivessem fazendo um bom trabalho. O maior crime contra a humanidade em curso no país é o sistema carcerário e ele é produzido por gente como nós, de gravata no ar-condicionado trabalhando dentro do sistema de Justiça Criminal. Então, a crítica dos engenheiros atuariais é um pouco assim: tudo bem, pode ser que o nosso sistema tenha problemas e violam alguns princípios, mas digam a vocês que estão preocupados com esses princípios pelos quais vocês juraram atuar. E eles tem razão nessa crítica, é uma contradição performática do Direito.

A segunda crítica que eu desenvolvi é de dizer: olhe, se o conflito com o Direito não é assim tão importante, vamos ver os atos de legitimidade desse próprio sistema, que a ideia é que ele é um sistema eficiente. Bom, mas isso é claramente mentira, esse sistema que usa prognósticos de risco não é eficiente, ele é extremamente caro, ele coincide com o giro punitivo cuja maior expressão é o encarceramento em massa. Ele traz questões sociais muito graves em termos de prevenção, é o chamado efeito cremalheira, como anuncia Bernard Harcourt na sua crítica, que vai dizer que: olha, isso aqui não consegue instalar uma criminalização lotérica distribuída de

maneira igualitária porque qualquer prognóstico atuarial só funciona se o acúmulo de data que ele tem é em relação ao sistema neutro. Mas como todo sistema de Justiça Criminal é seletivo, e o do Brasil é especialmente seletivo, porque 87% da população penitenciária masculina, dos 1684 crimes que existem, só respondem por 5 crimes, sendo que 3 deles não envolve violência ou grave ameaça, não dá para você usar o acúmulo de uma resposta seletiva para tentar definir uma criminalização lotérica. É um erro de pressuposto.

E aí, no último instante, a pergunta é: se o sistema é claramente ineficiente - ele é ineficiente - mas ele é ineficaz? Aqui você tem um problema porque as pesquisas que tentam validar o uso de prognóstico de risco na Justiça Criminal indicam que eles podem até funcionar, mas que o custo dele, em termos humanos e operacionais, é alto demais. Ou seja, mesmo que ele funcione, ele não é recomendável como estratégia de política criminal.

A última fase crítica do meu trabalho foi mostrar convergência estrutural dessa lógica de você usar o acúmulo do sistema de Justiça Criminal para fazer prognóstico de risco, para definir todos os critérios de criminalização, que eles têm uma profunda convergência com o modo de produção da vida social reorganizado a partir da reestruturação produtiva do capitalismo contemporâneo. A financeirização, sua adequação à ideologia neoliberal, a ideia de gestão social da miséria pelo critério de governamentalidade sacralizando a divisão de classes, o que vai tentar apostar no fim das contradições mediante a assimilação natural da desigualdade por meio dos sistema de justiça criminal. Por isso que o subtítulo da minha tese, "Política Criminal Atuarial", é "a criminologia do fim da História".

Em síntese, o que eu posso dizer é isso, dizer que essa é uma tecnologia que só funciona em um estágio pré-científico da criminologia que confunde criminalidade e criminalização. Então não é, digamos, uma resposta animadora para as pes-

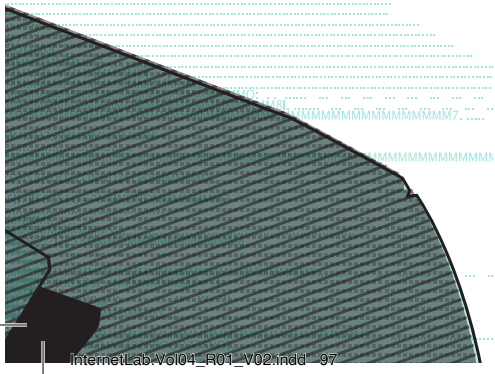
soas que pretendem embarcar na onda do uso de *big data* para definir critérios de punição. O último comentário, antes de chegar nos 20 minutos, eu só queria dizer o seguinte: há um único lugar em que eu consegui pensar no uso democrático da orientação prognóstica, no Brasil, é na definição da pena de multa, que hoje é quase que absolutamente arbitrária, sendo definida em valor de um salário-mínimo, sem qualquer relação com a realidade do acusado... nisso daria para pensar talvez um uso democrático no sistema de Justiça Criminal esse tipo de prognóstico atuarial.

E para quem pede indicação de leitura, sem fazer propaganda, eu posso recomendar o meu livro. Até hoje no Brasil é a única tese que foi publicada sobre a política criminal atuarial. E com razão: é um tema que não interessa a ninguém - eu escrevi esse livro, dediquei à minha esposa e nem ela leu. Então se você se interessou por esse tema, o que já me causa um grande espanto, eu posso recomendar a leitura da minha tese.

06.

O ALCANCE DA PROTEÇÃO DO SIGILO DAS COMUNICAÇÕES NO BRASIL

Tercio Sampaio Ferraz Junior [1]



1. O presente texto se baseia em apresentação oral feita no painel "O Alcance da proteção do sigilo das comunicações no Brasil" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

Em 1988, a expressão "dados", constante do inciso XII, levava a uma certa perplexidade. Nesse sentido, em 1990, a observação de Manoel Gonçalves Ferreira Filho (Comentários à Constituição Brasileira de 1988, São Paulo, 1990, vol. I, p. 38): *"Sigilo de dados. O direito anterior não fazia referência a essa hipótese. Ela veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática. Os dados aqui são os dados informáticos (v. incs. XII e LXXII)"*.

Para a doutrina, à época, a expressão *dados*, constante do inciso XII do art. 5º da CF, provocou alguma estranheza, percebida até como uma certa *impropriedade* (Celso Bastos & Ives Gandra, Comentários à Constituição do Brasil, São Paulo, 1990, art. 5º-XII). Esses autores reconheciam que por "dados" não se entende o *objeto* de comunicação, mas uma *modalidade tecnológica* de comunicação. A *inviolabilidade* seria dessa *modalidade* e não propriamente dos *dados*.

Essa relativa incerteza quanto ao sentido da expressão tornou-se um problema prático, por volta de 1992. Na época, o Governo Collor debatia medidas de combate a fraudes tributárias. Nesse contexto, foi editada a Lei Complementar nº 70/91, que permitia à Receita Federal demandar de instituições financeiras no geral, incluindo empresas administradoras de cartão de crédito, informações cadastrais sobre os usuários (nome, filiação endereço e número do CPF). A operacionalização dessas demandas precisava ser delineada em regulamento específico, que permitiria à Receita Federal utilizar cruzamentos para identificar números falsos de CPF e CGC, movimentação de caixa 2 e sinais de sonegação de impostos.

O Ministério da Economia, Fazenda e Planejamento objetivava emitir duas portarias regulamentares: uma destinada às instituições financeiras e outra às administradoras de cartão de crédito. Conforme se entendia pacificamente à época (1992), as instituições financeiras não seriam obrigadas a fornecer

dados de movimentação das contas dos clientes, pois elas estariam protegidas pelo sigilo bancário; mas tal restrição não valeria para empresas de cartão de crédito, por não serem "instituições financeiras" no sentido estrito do termo. As administradoras de cartão de crédito, por sua vez, contestavam tal interpretação e defendiam a inconstitucionalidade da medida.

Em maio de 1992, como Procurador Geral da Fazenda Nacional, elaborei um parecer, depois transformado em artigo, publicado em 1993 sob o título: "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado"[2].

Da leitura do inciso XII do art. 5º (inviolabilidade do sigilo), entendia que o sigilo ali referido diz respeito estritamente à *comunicação*. A partir das simetrias identificadas no texto constitucional (correspondência e telegrafia, telefonia e dados),e recorrendo a Pontes de Miranda, entendia a inviolabilidade do sigilo como uma liberdade de "negação". Ela seria, portanto, uma imunidade contra o pretendido poder de devassa ou interceptação/intromissão investigativa em certas esferas das vidas privadas de cidadãos. O sigilo, e sua manutenção, efetivariam esse direito, mas sem se confundir com o conteúdo daquilo que protegem. Assim, quanto aos dados, especificamente, concluía que o objeto da inviolabilidade do sigilo não seriam os dados em si, e sim a liberdade de negar acesso ao fluxo comunicacional. Mas não ao conteúdo por ele abarcado.

A interceptação de uma mensagem – isto é, a invasão do fluxo entre emissor e receptor, visando a acessar o conteúdo comunicacional que é transmitido – seria uma violação da proteção conferida pelo sigilo, nas hipóteses em que o teor da comunicação não puder ser obtido de outra forma. Como a inviolabilidade era prevista para o fluxo, não para o conteúdo

2. Ferraz Júnior, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.Revista da Faculdade de Direito, Universidade de São Paulo, 88, pp. 439-459.

comunicado, a interceptação de comunicações seria aceita por ordem judicial somente nas comunicações telefônicas, nas quais não restam vestígios físicos do conteúdo comunicado, por sua característica de "instantaneidade".

Neste horizonte estreito, a tese do texto foi levada ao STF, a partir de casos relativos à higidez do sigilo financeiro de cidadãos em face da atividade fiscalizadora do Estado.

Em 1994, em um mandado de segurança impetrado pelo Banco do Brasil contra ato do Procurador-Geral da República, que demandava, por ofício, lista de nomes dos beneficiários de liberação de recursos públicos ao setor sucroalcooleiro, além de dados específicos sobre existência de débitos e naturezas das operações que os originaram, a tese encampada pela PGR, da inviolabilidade do sigilo de comunicações, mas não dos dados armazenados, elaborada com apoio no texto de meu artigo, sagrou-se vencedora. Em dois votos vencedores, dos Ministros Sepúlveda Pertence e Francisco Rezek, o texto foi expressamente citado. Por maioria de 6 a 5, o STF indeferiu o mandado de segurança.

A tese acabou prevalecendo, tornando-se pacífico na jurisprudência constitucional e de tribunais inferiores que a inviolabilidade do sigilo (*da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas*) refere-se ao *fluxo* da comunicação.

Ainda em agosto de 2020, a Terceira Seção do STJ negou provimento a três recursos em mandados de segurança em face de ordens judiciais com perfil genérico: dispensam a indicação de um alvo individualizado e suspeito em uma investigação, para requerer o conjunto inespecífico e coletivo de informações sobre usuários que (i) tenham feito buscas por certas palavras-chave, e (ii) tenham transitado em certas áreas geográficas. Fundamento: o inc. XII do art. 5º da CF não se referia a informações comunicadas em correspondências,

/ A COMUNICAÇÃO DE DADOS – FLUXO-ARMAZENAMENTO – É EM RELAÇÃO COMUNICATIVA. DAÍ A SUA COMPREENSÃO COMO UM "BEM" NECESSARIAMENTE SOCIAL /

mensagens telegráficas, dados e telefonemas em si, mas ao *fluxo* da comunicação enquanto ocorre.

Porém, também no mesmo ano, em um caso, no qual o réu foi denunciado por infração ao art. 33 da Lei de Drogas e art. 12 do Estatuto do Desarmamento, após policiais apreenderem seu aparelho celular e, ali, procederem à investigação no aplicativo WhatsApp, em que se verificaram trocas de conversas, cujo teor indicaria a traficância, o Ministro Gilmar Mendes pronunciou "*a nulidade das provas obtidas mediante o acesso indevido ao aplicativo WhatsApp e à residência do paciente e, constatada a derivação de todas as demais provas*", declarando "*nulo o processo, determinando o trancamento da ação e a absolvição do paciente*".

Importante, nesse passo, ressaltar os fundamentos dessa decisão. O voto reconhece que, tradicionalmente, a doutrina e a jurisprudência do STF entendiam que que a inviolabilidade das comunicações *não se aplicava aos dados registrados*. Porém, a modificação das circunstâncias fáticas e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos smartphones levariam, na atualidade, a solução distinta, "*operando-se caso de mutação constitucional*".

Note-se, então, que a *comunicação de dados* – fluxo-armazenamento - *é em relação comunicativa*. Daí a sua compreensão como um "bem" necessariamente *social*. Não *social* em termos de mera interação individual (indivíduos nucleares, como numa correspondência, num telegrama), mas de comunicação *em sistema de acesso* que só tem uma qualidade: como *bem social*, *constitui-se* apenas na dimensão do *acesso*.

Nesses termos, *"o direito à autodeterminação informacional é, em consequência, não um direito de defesa privatístico do indivíduo que se põe à parte da sociedade, mas objetiva possibilitar a cada um uma participação em processos de co-*

municação"[3] O sujeito de direito é pensado como um agente que se comunica não *por meio,* mas *em meio* a esses bens. Aqui se fala de "meios", mas não como "*instrumento*", antes como "*ambiente*".

3. Wolfgang Hoffmann-Riem. Rechtliche Rahmenbedingungen, em *Der neue Datenschutz*, Helmut Bäumler (org.) Neuwied/Kriftel, Luchterhand, 1998, p. 13.

Importante perceber, nessa esteira, que a confluência tecnológica – caso ostensivo do celular – acabou, então, por alterar a percepção tradicional no que se refere à relação entre fluxo e dados armazenados. Basta ver, hoje, a facilidade com que se copia e cola no fluxo mesmo da comunicação. Por isso, para sua compreensão, entra inevitavelmente uma ponderação entre o direito individual à livre comunicação (liberdade de e direito à informação) e o valor atribuível à promoção da segurança pública (inviolabilidade do sigilo).

Particularmente isso afeta a hipótese de uma autorização judicial para qualquer *acesso privilegiado* de parte de um agente estatal (investigação criminal), que deve, então, levar em conta a possibilidade de uma vulnerabilidade ao sistema comunicacional no contexto da inviolabilidade à comunicação em termos de um conteúdo *privado/social*, indivíduos nucleares *em sistema de acesso.*

Nesse sentido, a garantia de um *direito fundamental à confidencialidade e integridade dos sistemas* significa para os usuários que a ruptura da esfera de intimidade de qualquer pessoa, quando ausente a hipótese configuradora de causa provável revela-se incompatível com o modelo consagrado na Constituição da República, pois a quebra de sigilo não pode ser manipulada, de modo arbitrário pelo Poder Público. Não fosse assim, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada, que daria, ao Estado – não obstante a ordem judicial – o poder de vasculhar registros sigilosos de pessoas indeterminadas, sem quaisquer indícios concretos, de modo a viabilizar, mediante uma ilícita utilização

do procedimento de devassa indiscriminada (que nem mesmo o Judiciário pode ordenar), o acesso a dados supostamente impregnados de relevo jurídico-probatório, em função dos elementos informativos que viessem a ser eventualmente descobertos.

Na verdade, no âmbito da comunicação de dados mesclam-se as fronteiras jurídicas entre as esferas da comunicação individual e em massa que eram até então separadas. No mundo das redes e da internet enquanto a rede das redes, as fronteiras entre público e privado tornaram-se porosas. Donde a questão de saber se seria juridicamente possível sustentar que o usuário de redes, ao optar por utilizar um perfil público, assume o risco de disponibilizar os seus dados de forma irrestrita e, por esse motivo, não teria legitimidade para se insurgir contra a possibilidade de utilização desses dados por qualquer interessado. Ou seja, de um lado, o tema da liberdade de expressão, de outro, a disponibilidade sem peias a que se expõe o destinatário.

Trata-se de um problema difícil de resolver-se quando se percebe no horizonte a conformação da sociedade como imensos sistemas virtuais dos quais a liberdade parece ter sido despersonalizada e que se regularão apenas por modelos sempre mais uniformizadores do *arbítrio* dos indivíduos, já então reduzidos a uma *tecla de acesso* e despojados de sua razão de ser como portadores do *ethos*.

Trata-se do problema da *transsubjetividade* em lugar da comunicação como *intersubjetividade*.

A digitalização elimina a realidade. A realidade é experimentada graças à resistência que oferece, que também pode ser dolorosa. A digitalização, toda a cultura "like", suprime a negatividade da resistência. Ou seja, a revolução cultural trazida pelo mundo digital faz-nos perceber que, aos poucos, antigas e sedimentadas noções, como a de *direito subjetivo*, não são mais capazes de lidar com essa desintegração em pedaços (*bits*) da estrutura íntegra das coisas. Pois a revolução cultural

e, nessa extensão, *jurídica*, que nos torna aptos a construir universos alternativos e paralelos ao mundo supostamente *dado*, nos converte de *sub-jectus* – indivíduos únicos – em *pro-jectus* de vários mundos.

A comunicação nas "redes sociais" é liquefeita; ela pode ser alterada pelo crescimento e pela mudança dos círculos de relação respectivos, seja de maneira intencional ou por agregação gradual espontânea: sempre e sempre mais *post*.

Ora, a regulamentação dos meios clássicos de formação da opinião pressupunha, no passado, sempre a formação de convenções estáveis ou móveis, que ditavam o que poderia ser apresentado como um tema válido. Isso era também um requisito para o controle das fronteiras da esfera pública em face da esfera privada.

No presente, porém, a erosão das fronteiras do dizível na fragmentada rede das redes que é a internet é tão clara e evidente que salta aos olhos. E controles externos da proteção judicial funcionam apenas de forma consideravelmente limitada contra comunicações ilícitas na internet.

Veja-se, por exemplo, o problema de como tratar juridicamente o uso de dados e metadados "produzidos" mediante *fake news*. Lida-se, na verdade, com questões ontológicas sobre a essência de uma tecnologia ou de uma aplicação na internet. Por exemplo: o *site* seria uma *"plataforma"* onde potenciais violadores de direitos autorais apenas se comunicam (sem responsabilidade pelo *site*) ou um *"quadro de avisos"* que estimula a prática de violações jurídicas?

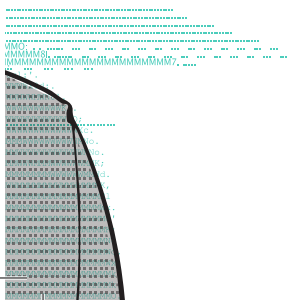
Parece claro que a proteção do sigilo da comunicação, em termos de direitos fundamentais individuais, ganha uma dimensão que mal se vislumbrava há 30 anos atrás. E a dúvida é saber se os instrumentos jurídicos elaborados no correr dos anos seriam ainda inteiramente adequados. Esse é um problema por resolver.

07.

MÉTODOS OCULTOS, DEVIDO PROCESSO E O ENFRENTAMENTO À CRIMINALIDADE ORGANIZADA

Diogo Malan[1]

1. O presente texto se baseia em apresentação oral feita no painel "Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.



Meu cordial boa noite a todos. Queria começar agradecendo imensamente ao InternetLab pelo honroso convite para participar desse 4º Congresso Internacional, agradeço na pessoa da Dra. Nathalie Fragoso, nossa mediadora, queria cumprimentar também os colegas do Painel, Dra. Fabiana Schneider, Dr. Orlandino Gleizer.

O tempo é curto, então vou ser bem objetivo: vou fazer um recorte de natureza mais político-criminal, algumas breves considerações introdutórias sobre o modelo de investigação preliminar na criminalidade econômico-financeira e, depois, algumas características dos *métodos ocultos de investigação*, conceitualmente e também peculiaridades aqui no Brasil.

Eu vou falar no conceito de um professor italiano - que eu acredito que seja quem melhor trabalha a questão da investigação dos crimes econômico-financeiros - o professor Ennio Amodio. Ele vai trabalhar com a ideia de que a investigação preliminar nessa esfera de criminalidade do colarinho branco adquire uma camada adicional de complexidade, em razão do uso de uma estrutura corporativa para fins de prática do delito.

A própria característica estrutural do ente corporativo, uma série de organismos a cargo de diferentes funcionários e gestores, fornece à atividade de investigação do Estado um campo mais amplo de investigação e, portanto, há uma natureza mais aflitiva, invasiva da investigação preliminar do crime, porque a própria natureza jurídica do ente corporativo oferece um campo mais amplo para o Estado desenvolver a sua investigação preliminar, que por vezes se espraia para além do alvo ou foco original da investigação, se estendendo a outras pessoas jurídicas ou naturais, como empresas coligadas, empresas subsidiárias, escritórios de advocacia ou de contabilidade. Portanto, o escopo do que ele chama de *investigação preliminar de banda larga* basicamente consiste na apuração de como

é que se formou a vontade de cometer o delito, quem foram as pessoas que efetivamente concorrem para a ideação do plano criminoso e, também, a medida em que o grau de coautoria ou participação de cada um de fato corresponde à divisão formal de tarefas e às atribuições constantes do organograma da empresa. Então existe uma certa rotatividade, um certo *turnover* na investigação preliminar de banda larga, porque há uma série de pessoas que entram e saem do raio de investigação preliminar durante essa atividade.

Quais são as consequências práticas dessa investigação preliminar de banda larga na criminalidade econômico-financeira, segundo esse professor italiano? Em primeiro lugar, existe uma verdadeira invasão estatal no negócio, que fica submetido a uma espécie de estado de assédio, que pode inclusive ser capaz de paralisar as suas atividades-fim. Por exemplo, na hipótese de haver uma apreensão do parque informático, haver uma apreensão dos livros contábeis daquela empresa. Existe também o risco de uma divulgação voluntária ou involuntária dos chamados *segredos de empresa*, que são aqueles conhecimentos técnicos altamente especializados, e que dão à empresa um diferencial competitivo no segmento em que ela atua. O que vemos muito na prática é a existência de um dano considerável à imagem empresarial, o que pode repercutir no faturamento da corporação de negócios, pode ensejar a rescisão de contratos com clientes e fornecedores. Caso se trate de uma companhia de capital aberto, pode ter uma queda no valor de mercado das suas ações, e eventualmente uma demissão massificada de funcionários da empresa. Portanto, o contexto das investigações preliminares de banda larga sobre a criminalidade natureza econômico-financeira é o campo, o terreno fértil e propício, para o emprego bastante comum, talvez até massificado, do que chamamos de *métodos ocultos de investigação*.

Vou trabalhar com a conceituação do meu mestre, Professor Titular Antonio Magalhães Gomes Filho, que sustenta que métodos ocultos de investigação têm características que os diferenciam dos chamados *meios de prova* (documental pericial e testemunhal). Os métodos ocultos de investigação têm a característica de serem extraprocessuais, normalmente se desenvolvem na fase de investigação preliminar do crime, de maneira não contraditória, são geridos por quem normalmente não ostenta qualidade ou condição jurídica de *parte* no processo criminal, agente de polícia judiciária, dependendo do país também pode ser agente de inteligência do Estado. Esses métodos servem para que o Estado possa se apoderar de provas materiais do crime, ou, se preferirem, de *fontes reais de prova*, e, como consequência, por serem extraprocessuais e não contraditórios, eles não servem diretamente à formação do convencimento do juiz sobre a culpa ou inocência do acusado, e se houver uma violação ao regramento procedimental previsto em lei, a consequência prática não é a *nulidade* do ato processual respectivo, e sim *inadmissibilidade probatória* do objeto arrecadado através do método oculto de investigação - daí a diferença para o chamado *meio de prova*, que tem características opostas. Ele é processual, ele é contraditório, ele é gerido pelas partes e, portanto, serve diretamente ao convencimento do juiz sobre o mérito da causa, se houver o descumprimento do procedimento probatório regulado por lei, a consequência prática é a nulidade do ato processual respectivo, e não a inadmissibilidade.

Tem um texto que eu gosto muito do Professor Manuel da Costa Andrade. Ele tenta estabelecer uma teoria geral dos métodos ocultos de investigação em um livro chamado “Que futuro para o direito processual penal?”. Nesse livro, nesse texto, o Professor Manuel da Costa Andrade vai tentar estabelecer as características do contexto político-criminal no qual

/ ELE PASSA A DESEMPENHAR UM PAPEL PREVENTIVO, O PROCESSO PENAL COMO UM INSTRUMENTO DE PREVENÇÃO À FUTURA PRÁTICA DE INFRAÇÕES PENAIS /

surgem os métodos ocultos, então ele sustenta que há uma nítida ruptura de um paradigma conceitual e filosófico do processo penal que vem desde a época do Iluminismo de 1789: a ideia calcada no estatuto jurídico do acusado enquanto sujeito processual titular de direito, situado em pé de igualdade com a parte acusadora, uma concepção do processo penal como sendo essencialmente um instrumento de *contenção* do poder punitivo, um conjunto de práticas e procedimentos racionais de *controle* do poder punitivo do Estado. Ele também aponta que, no contexto da massificação dos métodos ocultos de investigação, há uma certa erosão, uma restrição excessiva ou até uma aniquilação de algumas garantias liberais clássicas do processo penal, como a privacidade individual, a inviolabilidade de comunicações etc. E, também, a multiplicação tanto em termos de quantidade, quanto em termos de potencial restritivo a direitos fundamentais individuais.

Se o processo penal tradicionalmente é sempre permeado por uma tensão entre duas finalidades de certa maneira antitéticas ou antagônicas, nas lições do Professor Jorge Figueiredo Dias - por um lado o processo penal objetiva a máxima eficácia na realização da justiça e, por outro lado, a proteção dos direitos fundamentais individuais do investigado ou acusado -, nesse contexto político criminal de massificação, nitidamente o pêndulo se inclina na direção de interesses securitários, na tutela do poder punitivo do Estado em detrimento de direitos fundamentais e individuais.

Outra característica é uma certa tendência de *policialização* da investigação preliminar, no sentido em que há uma hipertrofia dos poderes da polícia judiciária, e uma certa ausência de uma supervisão e controle judicial efetivo nessa fase. Também se constata um certo grau de privatização da investigação preliminar, que permite, por vezes, que um particular seja usado como uma espécie de *longa manus* da autoridade policial, no exercício da atividade fim dela.

E a última característica, também muito interessante: o processo penal tem tradicionalmente natureza *retrospectiva*, ele visa ao acertamento, à reconstrução histórica de um fato pretérito, para se determinar se o acusado é culpado ou inocente. Com a massificação dos métodos ocultos de investigação, ele passa a desempenhar um papel *preventivo*, o processo penal como um instrumento de prevenção à futura prática de infrações penais.

Então, assim, segundo ele, esses métodos ocultos têm algumas características. Alguns métodos ocultos não tinham tradicionalmente uma certa institucionalização. Por exemplo, o emprego de agentes encobertos sempre foi utilizado por regimes de natureza autoritária para o controle e repressão a inimigos, dissidentes políticos. Mas nesse contexto de massificação, os métodos ocultos passam a ter uma institucionalização, tanto na perspectiva do Direito Penal material, quanto na perspectiva do Direito Processual Penal, sendo cada vez mais incorporados aos textos normativos, ou aplicados com base numa integração analógica.

Também há uma certa generalização. Eles têm essa característica de atingirem os direitos fundamentais de uma gama muito ampla de pessoas. Posso citar o exemplo de uma decisão judicial que autoriza a interceptação de dez linhas telefônicas - isso na prática vai implicar o monitoramento de milhares de ligações telefônicas, e vai implicar necessariamente a devassa da privacidade de centenas de pessoas. Não só dos alvos da medida, mas também outras pessoas com as quais o alvo guarda relações profissionais, sociais, familiares etc.

Então, quais seriam as características desses métodos no Brasil, ao meu ver? Em primeiro lugar, existe um certo déficit legislativo, um *buraco negro* em termos de regulamentação. Hoje são usados métodos que não têm previsão normativa expressa. Por exemplo a chamada *busca e apreensão virtual*: quando a Polícia Federal acessa um servidor de e-mail e copia

o conteúdo daquele servidor, mensagens enviadas, recebidas, catálogo de endereços, rascunhos, e também o pagamento de *verba sigilosa de informante* pela Polícia Federal a um particular no curso de uma investigação. Não há regulamentação de um procedimento probatório específico para esses métodos, e também, ao meu ver, não existe um método típico que possa ser usado por analogia nessas hipóteses.

Outra característica que vemos hoje no Brasil, com certa frequência: existe um *procedimento técnico-operacional oculto*, no sentido em que nem sequer o magistrado que autoriza, ou as partes no processo criminal, sabem exatamente qual foi a tecnologia usada para implementar a medida. Por exemplo, quando se faz a chamada captação ambiental de sinais acústicos, não se sabe exatamente como é que foi inserida uma aparelhagem para captar esses sinais no local de trabalho, no domicílio do suspeito, e depois essa informação não é devidamente documentada e incorporada aos autos do processo criminal.

O que vemos com alguma frequência também é a chamada *quebra da cadeia de custódia da prova*. Há uma certa deficiência no Brasil de uma cultura policial, uma cultura ministerial, uma cultura de observância de protocolos técnicos na coleta de fontes de prova e também um certo déficit na documentação cuidadosa da cadeia de custódia das provas incorporadas ao processo. Isso pode ter duas consequências: a primeira delas é a inviabilidade do exame direto do objeto da perícia por assistentes técnicos nomeados pelas partes e, também, essa quebra da cadeia de custódia da prova que pode gerar a eventual perda, adulteração ou contaminação da prova, pode ensejar a inadmissibilidade em juízo da prova, conforme foi reconhecido pelo Superior Tribunal de Justiça nesse *leading case* que é o HC 160.662. Então me parece uma discussão extremamente importante e que deve ser feita no Brasil, e que eu trago aqui para debate e reflexão coletiva, é: como é

que devemos sistematizar os limites ao emprego casuístico dos métodos ocultos de investigação? Essa me parece que é a discussão mais importante.

Aqui eu estou trabalhando muito com base no texto do professor Henrique Bacigalupo e também, em certa medida, com a jurisprudência do Tribunal Europeu de Direitos Humanos. A ideia é de que há limites importantes, como, por exemplo, a cláusula da legalidade estrita que vem manifestada por esse brocardo *nulla coatio sine lege:* não pode haver coação sem lei e, portanto, nesse terreno dos métodos ocultos há um regime de *legalidade estrita*. Não se pode se utilizar de interpretação extensiva, integração analógica, poderes gerais de cautela, métodos ocultos atípicos não previstos em lei etc. Também é importante se observar casuisticamente a *proporcionalidade* entre o grau de restrição a direitos fundamentais individuais causado pelo método oculto e a gravidade do crime, as circunstâncias do fato, as características pessoais do acusado, nos termos do art. 282, inciso II do CPP. *Reserva jurisdicional*, importantíssima garantia, hoje expressa no artigo 282, § 2º do CPP, excluindo a possibilidade de quaisquer órgãos que não sejam o juiz natural da causa autorizarem essas medidas. *Subsidiariedade* também me parece um limite extremamente importante, no sentido de que os métodos ocultos só devem ser empregados casuisticamente quando se lograr demonstrar que é impossível se utilizar um meio de investigação menos restritivo ou, pelo menos, é desproporcionalmente difícil se entregar um outro meio de investigação menos restritivo.

O professor Bacigalupo também trabalha com a ideia de um *roteiro normativo* para decisão judicial que autoriza o emprego dos métodos ocultos de investigação, em que haja uma delimitação clara, por exemplo, do fato naturalístico que está sendo apurado, o aspecto *objetivo*; do nome e da qualificação das pessoas que suportarão os efeitos jurídicos do método

oculto, delimitação *subjetiva*; o local de execução da medida; o meio técnico operacional que será utilizado para implementação da medida etc.

Preservação da cadeia de custódia da prova, também um limite importante, é preciso que seja devidamente registrado e documentado, através da preservação da integridade da prova, para que ela não sofra nenhum tipo de alteração, contaminação ou perda, que as partes possam ter acesso à prova idêntica àquela que foi colhida no local da diligência, cena do crime etc. E, por fim, o Tribunal Europeu de Direitos Humanos exige que haja um mecanismo processual de controle *a posteriori*. Como esses métodos são implementados *inaudita altera parte*, sem contraditório prévio, é importante que o indivíduo que sente que sofreu um método oculto de natureza abusiva, excessiva ou ilegal, tenha um meio efetivo para recorrer à tutela jurisdicional, e se defender e buscar uma restituição dos seus direitos.

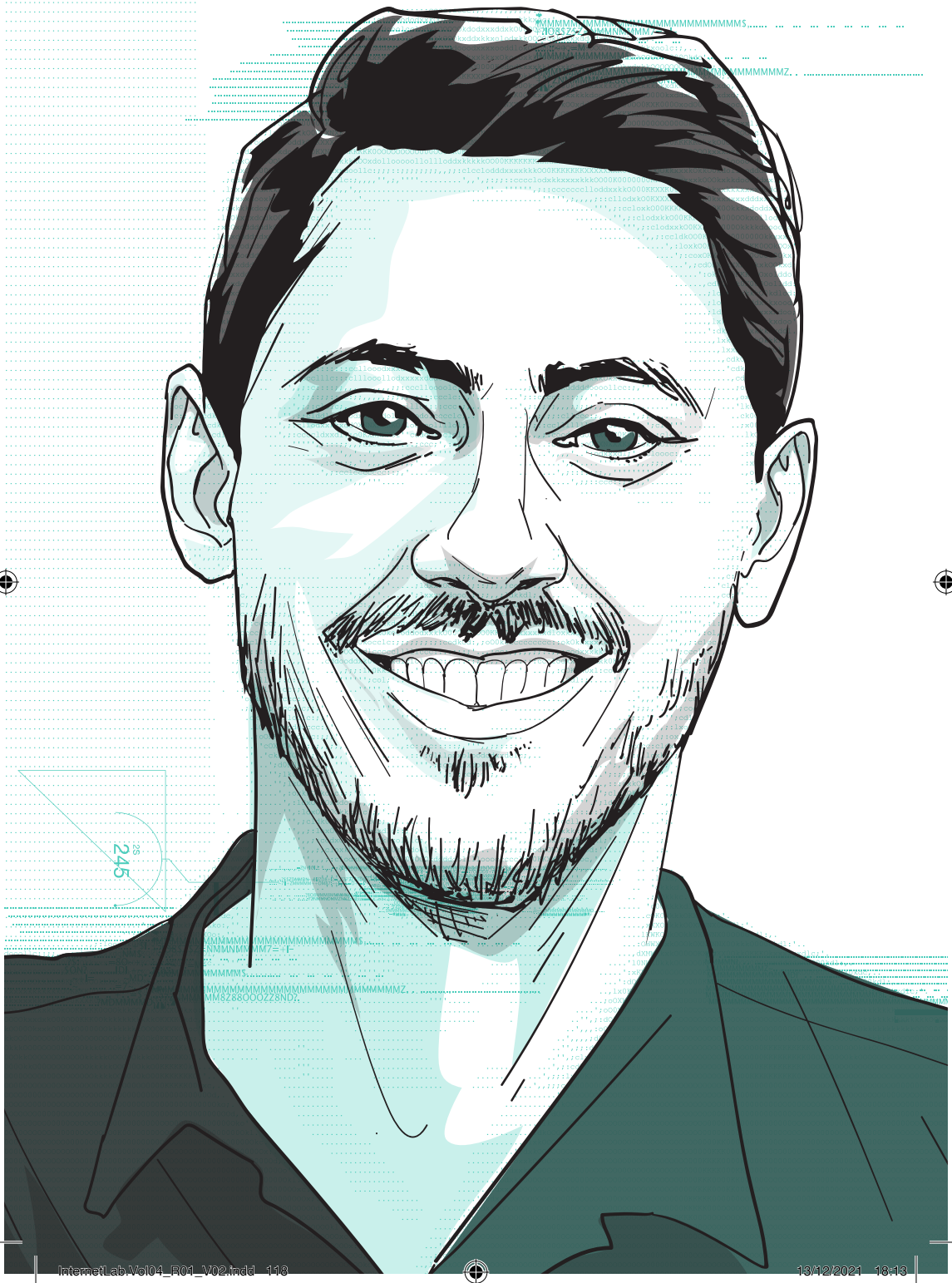
Então, eu gostaria de trazer alguns temas para discussão e debate. O primeiro deles é o seguinte: os métodos ocultos surgem num contexto político-criminal que podemos chamar de *securitário*, em que há uma nítida primazia de interesses relacionados à tutela do poder punitivo, da segurança pública, muitas vezes implicando um certo grau de sacrifício de direitos fundamentais individuais nesse altar da defesa social contra a criminalidade organizada.

Me parece também que esses métodos vieram para ficar, que é romântica a luta contra os métodos ocultos de investigação, é meio que nem lutar contra o processo eletrônico, o e-mail ou o *smartphone*, que são um caminho sem volta. Então, me parece que a discussão mais relevante hoje é discutir como sistematizar, da melhor maneira possível, os *limites* a esses métodos ocultos, e fazer uma adequada regulação procedimental desses métodos. Me parece, sem sombra de dúvida, que a revolução tecnológica caminha no sentido de cada vez

mais haver uma maior quantidade de métodos ocultos de investigação, com um potencial restritivo ao direito à privacidade individual. Hoje já há, por exemplo, medidas que buscam utilizar o *smartphone* do suspeito para fins de determinação da sua localização geográfica, através de sistemas de georreferenciamento, então hoje o *smartphone*, por exemplo, não serve só para monitoramento de mensagens e eventuais conversas telefônicas, mas para a própria localização do suspeito, no curso de uma investigação preliminar.

Me parece que o principal desafio hoje é justamente essa sistematização de limites aos métodos ocultos, limites de quatro naturezas: *constitucionais*, *convencionais* (que são aqueles previstos no sistema internacional de Direitos Humanos), *legais* e *racionais*. Basicamente eram esses os quatro pontos, há conclusões não definitivas, provisórias, para trazer ao debate dos senhores.

Muito obrigado, mais uma vez agradeço ao InternetLab pela honrosa oportunidade de poder participar desse congresso tão instigante, tão bem concebido e executado.



08.

A DOGMÁTICA DOS MÉTODOS OCULTOS DE INVESTIGAÇÃO NO PROCESSO PENAL

Orlandino Gleizer[1]

1. Este texto é uma transcrição revisada da fala do palestrante. Algumas poucas partes foram acrescidas ou eliminadas, a fim de garantir maior compreensão textual. Ainda assim, permanecem no texto imprecisões e incompletudes próprias da apresentação oral. O texto reproduz parte do conteúdo do livro Gleizer/Montenegro/Viana, O direito de proteção de dados no processo penal e na segurança pública, São Paulo: Marcial Pons, 2021. Além disso, explicações adicionais também podem ser encontradas em Greco, Introdução, in: Wolter, O inviolável e o intocável no direito processual penal, São Paulo: Marcial Pons, 2018. Portanto, para maior compreensão das ideias aqui expostas, aconselha-se consulta às referidas obras.

Boa noite! Eu começo pelos agradecimentos. Eu gostaria de agradecer ao InternetLab pelo convite, também queria cumprimentar o professor Diogo Malan e a professora Fabiana Schneider, que hoje dividem esta mesa virtual comigo. Eu terei que ser breve na primeira parte da exposição, para que eu consiga abordar questões mais importantes na sua última parte.

Ao longo da minha fala, eu começarei definindo o que chamarei de métodos ocultos de investigação. Depois, eu apresentarei alguns aspectos comuns a qualquer intervenção em direitos fundamentais; e, posteriormente, eu tratarei dos aspectos específicos das medidas ocultas de investigação.

1. DA DEFINIÇÃO DE MÉTODOS OCULTOS DE INVESTIGAÇÃO

Métodos ocultos de investigação são definidos como métodos processuais penais de colheita de elementos informacionais, colheita essa cuja eficácia pressupõe o desconhecimento da medida pelo afetado. Portanto, oculto aqui é sinônimo de secreto. Assim como todo processo conduzido pelo Estado, as investigações policiais ou judiciais são medidas de direito público, e as ações dos agentes estatais, que de modo geral afetam os âmbitos da vida privada protegidos pelos direitos fundamentais, ostentam a qualidade de intervenções. Portanto, intervenção é toda ação estatal de afetação do âmbito de proteção dos direitos fundamentais. E essas ações só são legítimas caso estejam justificadas.

2. DA JUSTIFICAÇÃO DE INTERVENÇÕES EM DIREITOS FUNDAMENTAIS

Como cada direito fundamental é uma proteção a um âmbito específico da vida dos indivíduos, cada um deles estabelece

diferentes pressupostos para a legitimidade das intervenções. A primeira tarefa, portanto, é delimitar com precisão o *âmbito de proteção* de cada um dos direitos fundamentais. Um exemplo que eu gosto de mencionar é o da interceptação de telecomunicação na fonte, necessária caso o investigado use algum programa computacional de telecomunicação como o Skype. A instalação de um malware, para a captura desses diálogos no próprio dispositivo informático, antes que passem pela criptografia do programa computacional, não representa uma intervenção no direito fundamental ao sigilo das comunicações – o que ficará claro adiante –, mas no direito à confidencialidade e à integridade dos dispositivos informáticos; por isso, é importante saber qual é o direito fundamental que está sendo afetado em cada ação estatal específica.

O segundo passo dessa análise de justificação das intervenções em direitos fundamentais é o plano da *intervenção*. A intervenção é toda ação estatal que afeta o âmbito de proteção de um direito fundamental. De novo, vou usar o exemplo da interceptação telefônica. A interceptação telefônica é uma intervenção no direito fundamental ao sigilo das comunicações. A ideia é garantir que um indivíduo possa desenvolver livremente um aspecto da sua personalidade, qual seja, a comunicação com outros indivíduos. Como isso só pode ocorrer caso ele se sinta tão seguro à distância, como se sentiria em um diálogo presencial, esse direito fundamental protege a confiabilidade no uso de meios de telecomunicação. Como ele não protege a confiança do indivíduo em seu interlocutor, a escuta telefônica – ou seja, quando o interlocutor, por exemplo, coloca a chamada em viva-voz, para que agentes estatais possam ouvi-la – não é uma intervenção nesse direito fundamental. Porque em razão da escuta telefônica, o investigado não perde a confiança no uso do meio de telecomunicação empregado, senão no seu próprio interlocutor.

E essa confiança interpessoal não é protegida por direitos fundamentais. Um outro exemplo são os dados oriundos de telecomunicação já encerrada, como os e-mails salvos em um dispositivo informático. Nesse caso, o direito ao sigilo da telecomunicação também não é afetado pela captura desses dados. Porque, com o fim do processo de telecomunicação, esses dados estão sob domínio do indivíduo, que pode, por exemplo, eliminá-los. Por isso, esses documentos em nada diferem de outros documentos quaisquer. A captura desses dados afeta um outro direito fundamental, que protege também a personalidade do indivíduo: a autodeterminação informacional.

Por fim, o âmbito mais exigente dessa verificação é o da *justificação*. Aqui, são enfrentadas questões de várias ordens. Simplificando, a justificação de qualquer ação de intervenção carece de fundamentos de ordem formal e material. Em geral, o âmbito de análise dos fundamentos materiais é o mais complexo. Mas a exigência de um fundamento formal para a intervenção, ou seja, a exigência de lei, parece não ter sido bem compreendida pelos tribunais brasileiros. Mesmo a literatura jurídica brasileira tratou, durante alguns anos, as medidas interventivas como algo em si lícito, carente apenas de mera regulação; e não o contrário.[2] Além disso, como cada ação interventiva corresponde a um dever de tolerância pelo ofendido, que não pode se opor à realização dessa medida, essas normas autorizativas precisam ser claras, determinadas e específicas, porque elas servem não apenas para fundamentar, mas também para limitar as ações estatais. É uma garantia do próprio indivíduo, o Estado não pode intervir além dos estritos limites das autorizações expressas do legislador. É o que estabelece o art. 5º II CF.

2. Nesse sentido, *Greco*, Introdução, in: Wolter, O inviolável e o intocável no direito processual penal, São Paulo: Marcial Pons, 2018, p. 40.

/ MÉTODOS OCULTOS DE INVESTIGAÇÃO SÃO DEFINIDOS COMO MÉTODOS PROCESSUAIS PENAIS DE COLHEITA DE ELEMENTOS INFORMACIONAIS [...] CUJA EFICÁCIA PRESSUPÕE O DESCONHECIMENTO DA MEDIDA PELO AFETADO /

/ A CAPTURA DESSES DADOS AFETA UM OUTRO DIREITO FUNDAMENTAL, QUE TAMBÉM PROTEGE A PERSONALIDADE DO INDIVÍDUO: A AUTODETERMINAÇÃO INFORMACIONAL /

Nesse sentido, a ciência e a jurisprudência desenvolveram critérios rigorosos para essas normas no debate internacional. Nessa ocasião, há tempo de destacar apenas alguns desses aspectos. Em primeiro lugar, normas de competência jamais autorizam intervenções. Normas de competência distribuem tarefas públicas internamente à estrutura do Estado, ou seja, a quem incumbe o quê. Por isso, são voltadas para dentro. Já as normas de autorização dirigem-se para fora. Elas autorizam ações dos entes incumbidos da realização de tarefas estatais que afetem direitos fundamentais dos cidadãos. Isso significa, por exemplo, que àquele a quem incumbe julgar não é permitido qualquer coisa para que possa julgar, somente o que está autorizado para o cumprimento dessa tarefa.

Em segundo lugar, as normas devem individualizar as ações com termos naturalísticos. Aqui também são usados verbos precisos, como acessar, produzir, compartilhar etc. Apenas a ação expressamente autorizada pode ser legitimada. De uma autorização de acesso a determinados dados individuais não pode decorrer uma automática autorização de compartilhamento desses mesmos dados, ou algo similar. Caso contrário, qualquer autorização estaria vinculada a um conjunto imprevisível de autorizações implícitas e a lei perderia toda a sua capacidade protetiva.

Em terceiro lugar, as normas precisam estabelecer expressamente parâmetros de legitimidade e proporcionalidade, como a subsidiariedade, o rol de delitos autorizadores da medida (conhecido como catálogo de fatos), os correlatos deveres de proteção, dos quais eu falarei adiante, etc. Essas questões centrais da intervenção não podem ser deixadas a cargo do aplicador do direito, ele próprio precisa estar submetido a essas exigências.

Em relação aos fundamentos materiais, analisam-se, nesse âmbito, sobretudo as considerações de proporcionalidade. Os agentes interventores precisam fundamentar o porquê

de intervir no âmbito constitucionalmente protegido da vida do afetado. Mesmo o legislador, que, ao editar medidas interventivas, afeta de forma geral esses direitos do indivíduo, precisa superar esses obstáculos. E quanto mais precisa e restrita, ou seja, menos interventiva for a ação autorizada ou praticada, menores podem ser esses obstáculos (interventivos). O raciocínio também pode ser apresentado pela sua face inversa: quanto mais severa for a intervenção, maiores devem ser os obstáculos interventivos, como a qualidade dos crimes autorizadores da medida, as circunstâncias concretas nas quais a medida pode ser executada, a suspeita concreta contra o acusado, níveis de proteção contra riscos decorrentes da medida, deveres de notificação etc. E aqui, aproveitando a oportunidade para estabelecer um ponto de encontro entre os aspectos que até agora chamei de comuns ou gerais e aqueles que chamei de aspectos específicos das medidas ocultas, começarei a tratar desses últimos.

3. DA JUSTIFICAÇÃO DE INTERVENÇÕES OCULTAS EM DIREITOS FUNDAMENTAIS

Quanto aos aspectos específicos de justificação das medidas ocultas de intervenção no processo penal, eu gostaria de destacar, em primeiro lugar, a redução das possibilidades de defesa jurídica da esfera individual pelo titular do direito fundamental. Os métodos ocultos corporificam uma afetação secreta de uma posição individual juridicamente protegida. Nesse sentido, são medidas muito mais graves previstas pelo ordenamento jurídico. É verdade que a prisão preventiva também é especialmente grave, mas o afetado, necessariamente, toma conhecimento dessa medida e a ela pode opor-se juridicamente. A escuta ambiental e a interceptação telefônica, por exemplo, aproveitando-se do desconhecimento do afetado,

não podem ser contestadas contemporaneamente e, durante o tempo em que perduram, representam uma grave afetação do âmbito da vida privada do indivíduo, que tem legítima expectativa de não ser afetado quando ausentes os pressupostos autorizadores da medida.

A questão é que esses pressupostos, diferentemente do que ocorre com as medidas ostensivas, como a busca e apreensão, só podem ser verificados pelo interessado após terem esgotado sua eficácia, ou seja, após a intervenção ter sido encerrada. Isso que significa que o conhecimento do afetado chega tarde demais. Com isso, eu não quero dizer que as medidas ocultas não possam ser justificadas, parece ser evidente que podem. O que eu quero dizer é que esse aspecto precisa estar compensado de outras maneiras. Eu quero ressaltar três maneiras de compensar a natureza oculta das medidas, de modo a aumentar a proteção da esfera individual.

A primeira delas: a submissão da medida a pressupostos autorizativos mais rigorosos. Se uma medida pública pode ser praticada para proteção de bens jurídicos de alguma importância, medidas ocultas devem ser autorizadas apenas para a proteção de bens jurídicos de maior valor/importância. Enquanto a exigência desses critérios fica a cargo da lei, eu penso ser importante que o seu controle esteja a cargo da ciência e dos tribunais. Aqui, a figura do ensejo ganha ainda mais relevância. Apenas alguém que dá ensejo, isto é, que cria um perigo ou pratica um crime, deve poder ser objeto de medidas tão drásticas. O ensejo funcionaria aqui como uma forma de manter nas mãos do indivíduo a possibilidade de não sofrer essa intervenção. Aquele que não dá ensejo pode ter maior expectativa de ser deixado em paz.

Uma segunda forma de compensar essa natureza oculta dessas medidas seria a imposição de rígidos deveres de proteção. Diante da impossibilidade do afetado de defender

pessoalmente sua esfera protegida, é importante designar alguém para substituí-lo nessa função. E, para tanto, duas opções parecem convincentes, necessárias e ao mesmo tempo complementares: em primeiro lugar, aquele que pratica a intervenção oculta precisa assumir o ônus de proteger o acusado contra qualquer consequência extra advinda dessa intervenção. Deve ser obrigação daquele que manuseia e mantém a guarda de dados pessoais que também os proteja contra o acesso não autorizado de terceiros. Em segundo lugar, a figura de um proto-defensor, que foi sugerida pelo Prof. *Bernd Schünemann*[3] e que vem sendo discutida no âmbito das investigações preliminares transnacionais da União Europeia – onde é chamada de euro-defensor – parece ser a proteção possivelmente mais eficiente dos direitos fundamentais dos afetados nesses casos. Esse proto-defensor teria a tarefa de verificar a legitimidade das medidas secretas e seria obrigado a manter o sigilo também em relação ao afetado. Na minha opinião, a Defensoria Pública, no Brasil, poderia perfeitamente assumir essa função.

3. *Schünemann*, ZIS 2009, 484, 493, acessível em: http://www.zis-online.com/dat/artikel/2009_10_358.pdf.

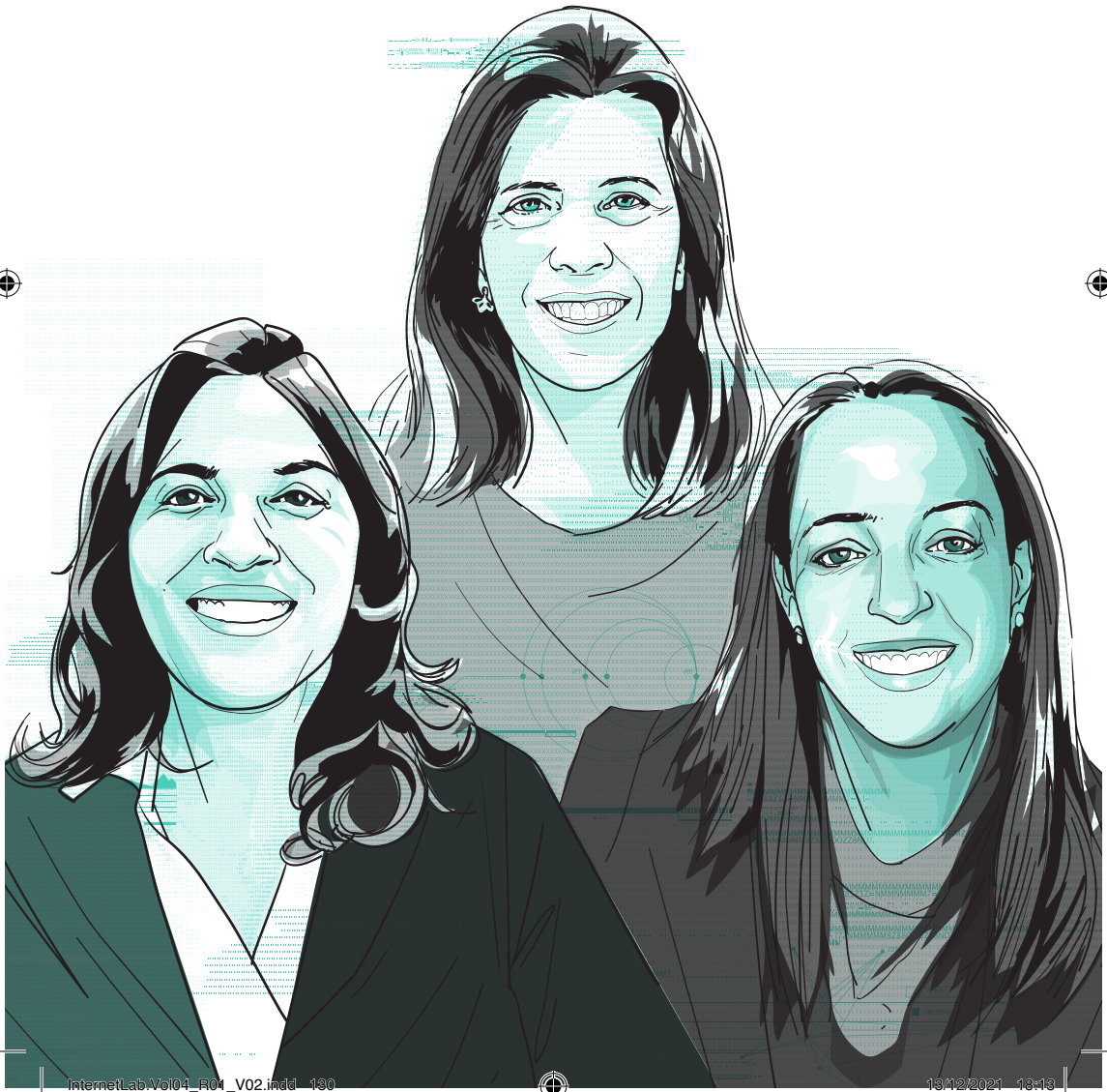
O outro dever de proteção consiste na obrigatória notificação dos afetados. Nem todo afetado pela medida oculta será acusado ao fim da investigação. Isso significa que nem todos tomarão conhecimento de que foram alvos de uma intervenção oculta, de forma que possam tomar providências jurídicas, ainda que *a posteriori*. Portanto, haveria um dever do Estado de notificar, tão logo inexista motivo que fundamente a manutenção do segredo, todos aqueles que foram afetados pelas medidas ocultas. Por fim, deveres de proteção também fundamentam deveres de eliminação dos dados obtidos.

A terceira forma de compensar a natureza oculta das medidas seria a criação de ainda maiores obstáculos para interven-

ção da esfera daqueles que convencionalmente são chamados de não-implicados ou, no processo penal, de insuspeitos. Esse foi um aspecto completamente negligenciado pela recente decisão do STJ, que determinou ao Google a entrega de dados pessoais de usuários para investigação penal que apura os mandantes do homicídio de Marielle Franco e Anderson Silva (STJ RMS 60.698, RMS 61.302, RMS 62.143, j. em 26.8.2020).[4] A consequência dessa negligência soa absurda em um Estado de Direito: milhões de pessoas terão seus dados disponibilizados a autoridades estatais, sem que tenham dado qualquer ensejo à medida e sem que, sobre elas, recaia qualquer suspeita de cometimento de fatos ilícitos. É uma decisão que ainda pode ser revertida pelo Supremo Tribunal Federal, a quem cumpre, penso eu, urgentemente implementar as ideias aqui expostas.

Agradeço muito pela atenção.

4. Para uma crítica mais detalhada, cf. *Estellita/Gleizer, A investigação penal de insuspeitos*, jornal Folha de São Paulo, 12.9.2020, acessível em: https://www1.folha.uol.com.br/opiniao/2020/09/a-investigacao-penal-de-insuspeitos.shtml.



09.

TRANSFERÊNCIA INTERNACIONAL DE DADOS PARA FINS DE INVESTIGAÇÕES CRIMINAIS À LUZ DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Fernanda Teixeira
Melissa Garcia
Neide Mara

INTRODUÇÃO

Para discorrer sobre proteção aos dados de investigação e cooperação jurídica internacional criminal é essencial contextualizar a Lei Geral de Proteção de Dados brasileira e seus desdobramentos, no âmbito da cooperação jurídica internacional. Nesse contexto, relativamente à matéria penal, é necessário informar que o Brasil se encontra em processo de adesão à Convenção do Conselho da Europa contra a Cibercriminalidade, também conhecida como Convenção de Budapeste.

A Convenção sobre Cibercriminalidade do Conselho da Europa – ETS nº 185 (CONSELHO DA EUROPA, 2001) é atualmente o principal instrumento internacional para a persecução de crimes cibernéticos e obtenção de provas eletrônicas. As principais economias do mundo já a ratificaram ou estão em processo de adesão, excetuando-se China e Rússia. São membros da Convenção, além dos países do Conselho da Europa, Estados Unidos, Austrália, Japão, Canadá, Argentina e Chile dentre outros. O Brasil foi convidado a aderir em dezembro de 2019 e, atualmente, enquanto em processo de ratificação[1], possui *status* de observador.

Além de conter a tipificação de condutas penais referentes a crimes cibernéticos próprios e de outros facilitados pelo meio eletrônico (artigos 2º a 10º), a Convenção traz ainda em seus artigos 14º a 35º instrumentos de investigação e compartilhamento de dados e provas eletrônicas entre os Estados-membros.

O pedido de adesão do Brasil, encaminhado por meio do Ministério das Relações Exteriores (MRE), foi resultado de anos de trabalho do Ministério Público Federal junto a esse órgão, analisando-os os benefícios a serem proporcionados ao Brasil pela Convenção e sobre sua compatibilidade com a legislação brasi-

1. O pedido de ratificação foi encaminhado à Câmara dos Deputados, no dia 22 de julho de 2020, após o convite do Conselho da Europa para a adesão pelo Brasil à referida Convenção.

leira[2]. A principal vantagem será o estabelecimento de uma cooperação jurídica internacional, mais eficiente e confiável, com os países membros da Convenção.

2. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas. Acesso em 14 out.2020.

Além disso, espera-se conseguir mais agilidade na transferência de provas relacionadas a crimes cibernéticos, bem como de provas eletrônicas, o que inclui, na maioria das vezes, a transferência de dados pessoais de investigados. Necessário, assim, analisar os dois regimes de proteção de dados pessoais, o brasileiro e o europeu, a fim de se determinar o arcabouço atual de transferência de dados para fins penais.

O REGIME BRASILEIRO DE PROTEÇÃO DE DADOS

A LGPD, Lei nº 13.709, foi aprovada em 14 de agosto de 2018, com um período de *vacatio legis* de dois anos. Após a indefinição sobre a sua entrada em vigor, inicialmente prevista para 14 de agosto de 2020, se não fosse o artigo 4º da Medida Provisória (MP) nº 959, para maio de 2021, a norma passou a ter vigência em 18 de setembro, quando sancionada em lei a MP, que restou aprovada sem aquele dispsoitivo. No entanto, as sanções administrativas (artigos 52 a 54) nela previstas foram postergadas para 1º de agosto de 2021, devido à aprovação da Lei nº 14.010/2020, que trata do Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado.

Seguindo o regulamento geral de proteção de dados europeu – *General Data Protection Regulation* (GDPR) – Regulamento (UE) n. 2016/679 do Parlamento Europeu e do Conselho da União Europeia, a LGPD prevê várias regras com o fim de garantir a máxima proteção e segurança na transferência internacional de dados. E da mesma forma que a legislação europeia, a

lei brasileira disciplina três regimes diferentes de salvaguardas para transferências internacionais de dados, que seriam:

(I) a declaração de existência de grau de proteção de dados pessoais, adequado ao previsto na LGPD;

(II) a existência de garantias de cumprimento dos preceitos da LGPD;

(III) derrogações específicas do regime da LGPD, casuisticamente listados com vistas a promover algum objetivo de interesse público. (...) a manutenção de três regimes diferentes está – ao menos em tese – em consonância com o ponto de vista de que a proteção de dados pessoais está intimamente relacionada à proteção de direitos fundamentais. (CARVALHO, 2019, p. 624).

Para melhor compreensão do assunto aqui tratado, faz-se necessária uma breve análise de cada um deles.

2.1. DA TRANSFERÊNCIA DE DADOS PARA PAÍSES COM REGIME ADEQUADO DE PROTEÇÃO

No inciso I do art. 33 da LGPD está prevista a permissão de transferência internacional de dados para países, ou organismos internacionais, que proporcionem nível adequado de proteção. Esse dispositivo, entretanto, não esclarece os detalhes para a qualificação de determinado sistema legal como "adequado" aos preceitos da lei brasileira. Tal função é reservada à autoridade nacional, no art. 34, que em seus incisos prevê as bases que devem ser levadas em consideração.

Assim, a lei brasileira não exige que ordenamentos estrangeiros contem com uma legislação específica sobre proteção de dados, mas que, "*em última análise, o núcleo fundamental da LGPD possa ser encontrado, ainda que difusamente, no ordenamento destinatário dos dados a serem transferidos*". (CARVALHO, 2019, p. 626).

Essa análise caberá à Autoridade Nacional de Proteção de Dados e sua decisão, com efeitos amplos e gerais, significará sua postura diante daquele ordenamento, e deverá ser considerada como declaração de idoneidade daquele ordenamento, por determinado período de tempo, sobre o qual esse posicionamento pode ser alterado (CARVALHO, 2019, p. 626).

2.2. DA TRANSFERÊNCIA DE DADOS QUANDO HÁ GARANTIAS DE CUMPRIMENTO DOS PRECEITOS DA LGPD

O segundo regime de transferência internacional de dados, trazido no art. 33, inc II, do diploa, prevê essa possibilidade mediante *"a existência de garantias de cumprimento dos preceitos da LGPD"*. Isso permite, mesmo em um quadro normativo com um nível de proteção menor que a legislação brasileira, a transferência de dados com base em salvaguardas apresentadas pela parte requerente dos dados, aprovadas pela autoridade nacional, conforme previsto na LGPD, em observância aos padrões fixados por autoridades de controle independentes e desvinculadas de governos. (CARVALHO, 2019, p. 627).

Nesse caso, mesmo que o país estrangeiro para onde os dados se destinem não dê todas as salvaguardas necessárias ao atendimento dos padrões protetivos previstos pela LGPD, é possível que o controlador específico ofereça e comprove garantias de cumprimento dos preceitos da lei brasileira, seja por meio de cláusulas contratuais (padrão ou específicas),

normas corporativas globais, ou selos, certificados e códigos de conduta regularmente emitidos.

2.3. TRANSFERÊNCIA DE DADOS EM RAZÃO DO INTERESSE PÚBLICO

Por fim, a LGPD prevê um terceiro regime para a transferência internacional de dados, disposto nos seus incisos III a VIII do art. 33, que são situações específicas, não abrangidas pelos incisos anteriores, que visam outros objetivos de interesse público, *in verbis*:

< III > quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

< IV > quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

< V > quando a autoridade autorizar a transferência;

< VI > quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

< VI > quando for necessária para a execução de política pública ou atribuição legal do serviço público;

< VIII > quando o titular tiver fornecido o seu consentimento específico para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente essa de outras finalidades;

< IX > quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

2.4 TRANSFERÊNCIA DE DADOS EM RAZÃO DA SEGURANÇA PÚBLICA, ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO DE INFRAÇÕES PENAIS

Nos termos do art. 4º, III da LGPD, os dados pessoais destinados à segurança pública e às atividades de investigação e repressão de infrações penais, bem como à segurança pública e à defesa nacional estão excepcionados das regras de proteção previstas na LGPD, à semelhança da redação do GDPR, que também os excepciona. Em ambos os regimes, há a previsão da edição de normas específicas para regulamentar a proteção e transferência de dados pessoais para fins de persecução penal.

A União Europeia já tem um regulamento próprio trazido pela Diretiva (UE) n. 2016/680 (UNIÃO EUROPEIA, 2016) do Parlamento Europeu e do Conselho da União Europeia, que trata da proteção dos dados referentes à prevenção, investigação e persecução penal, bem como repressão de infrações penais e execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Mas o Brasil, não. Embora o artigo 33 faça expressa menção à possibilidade de transferência internacional de dados "quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional", dentre outras situações, o artigo 4º, §1º da LGPD dispõe que deve haver legislação específica para a matéria.

Assim, em notícia publicada pela Câmara dos Deputados (JÚNIOR,2019), em novembro de 2019, foi criada, pelo seu presidente, uma Comissão Parlamentar na Câmara dos Deputados

formada por juristas renomados no tema, para propor projeto de lei sobre o uso de dados pessoais em investigações penais e segurança pública.

Com a entrada em vigor da LGPD e a esperada breve ratificação pelo Brasil da Convenção de Budapeste, almeja-se que essa Comissão possa acelerar a retomada dos trabalhos, interrompida com a pandemia da Covid-19. Pretende-se que o projeto de lei sobre a proteção de dados pessoais referentes a segurança pública, defesa nacional e investigações criminais seja finalizado e aprovado o mais breve possível.

As previsões das exceções devem observar os princípios previstos no art. 6º da Lei, principalmente os da finalidade e da segurança. Alguns princípios presentes na LGPD, também constam em outras leis de primeira e segunda geração, segundo Doneda (2011), uma vez que são universais e facilitam a transferência internacional de dados.

3. O REGIME EUROPEU DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

Conforme exposto, a LGPD se inspira em diversos dispositivos do GDPR para regular a proteção de dados. Em linhas gerais, em seu artigo 45, o regulamento europeu também permite a transferência de dados quando há o reconhecimento de que o ordenamento jurídico do país recipiente possui nível de proteção adequado, ou quando o controlador apresenta salvaguardas apropriadas – art. 46.

Entretanto, conforme descrito acima, a transmissão de dados para fins de persecução penal entre países regidos pelo GDPR e outros deverá obedecer ao regramento próprio trazido pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho da União Europeia.

/ A COOPERAÇÃO PREVISTA NA CONVENÇÃO SEGUE OS MESMOS PRECEITOS DA COOPERAÇÃO JURÍDICA EM MATÉRIA PENAL, COM ANÁLISE DE CABIMENTO CASO A CASO E ATENDIMENTO INDIVIDUALIZADO /

/ OS MECANISMOS DE ACESSO DIRETO TRAZIDOS PELA CONVENÇÃO CONTÉM AVANÇOS CONSIDERADOS SIGNIFICATIVOS NA ÉPOCA DE SUA ELABORAÇÃO, EM 2001, EMBORA HOJE NECESSITEM DE REVISÃO /

3.1. O REGIME DA DIRETIVA "POLICIAL" (UE) 2016/680

Com a regulação da proteção dos dados pessoais no âmbito da União Europeia, surge a questão relativa ao tratamento a ser dispensado aos dados pessoais coletados com os fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais - salvaguardas e prevenção de ameaças à segurança pública.

Evidente que tais dados não poderiam seguir o mesmo regime dos dados comuns, delineado no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho – o GDPR, uma vez que, para estes dados, com finalidade específica voltada à segurança pública, há uma imposição na coleta e tratamento que não se coaduna com o consentimento, um dos pilares da nova regulação. Logo, o consentimento do titular dos dados não pode ser o fundamento jurídico do tratamento desses dados pelas autoridades competentes. Isso não significa que tais dados estarão isentos de proteção na sua coleta, tratamento e compartilhamento.

Dessa maneira, os dados coletados pelas autoridades competentes com os fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais - salvaguardas e prevenção de ameaças à segurança pública devem circular livremente entre as autoridades competentes congêneres justamente para permitir a eficiência na manutenção da ordem e segurança públicas. É isso o que a Diretiva (UE) n. 2016/680 aponta no item (4) da sua explanação de motivos ao dizer que a transferência desses dados para países terceiros e organizações internacionais deve ser facilitada, assegurando-se simultaneamente um elevado nível de proteção dos dados pessoais.

Assim, a proteção de dados pessoais no domínio da cooperação jurídica em matéria penal e da cooperação policial assenta-se em garantir que as autoridades estrangeiras e/ou organismos internacionais dispensarão aos dados comparti-

lhados o mesmo nível de proteção e tratamento que lhes é dispensado pelas autoridades que os detêm. Isso diz respeito, por exemplo, à finalidade específica de uso desses dados pessoais, que deve ser permitida pela autoridade que os compartilha, não podendo ser reutilizados para outros fins sem sua prévia autorização; à confidencialidade e segurança que devem ser garantidos a tais dados, de forma que o acesso, a utilização desses dados e do equipamento empregada para o seu tratamento somente estejam franqueados a pessoas autorizadas.

O item 31 da explanação de motivos da Diretiva esclarece ainda que, ao se levar em conta a circulação desses dados em cooperação jurídica em matéria penal e em cooperação policial, é esperada, quando aplicável, a distinção entre dados pessoais de diferentes categorias de titulares de dados como: suspeitos, pessoas condenadas, vítimas, terceiros, assim entendidos testemunhas e informantes e outras pessoas consideradas relevantes para as investigações. Podem, ainda, ser previstas condições reputadas necessárias pelas autoridades transmissoras dos dados, como proibição de notificação do titular dos dados ou garantias adicionais quando os dados transmitidos forem considerados dados sensíveis que toquem direitos e liberdades fundamentais.

A autoridade competente para remessa e recebimento dos dados pessoais regulados pela Diretiva, nos termos do seu art. 3º, número 7, são precisamente as autoridades públicas competentes para exercer as atividades de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Assim, o diploma apresenta como formas de validar a transferência internacional dos dados a ela pertinentes:

- a decisão de adequação, que reconhece no país terceiro, no organismo internacional ou em um ou

mais setores específicos desse país terceiro um nível de proteção de dados pessoais adequado;

- o fornecimento de garantias adequadas para essa proteção via instrumento juridicamente vinculativo;

- a derrogação das regras da diretiva no caso de situações específicas: se a transferência for necessária para proteger interesses vitais do titular dos dados e/ou seus legítimos interesses, para prevenir ameaça iminente e grave contra a segurança pública de um Estado-membro ou país terceiro, e em outros em que haja justificativa, inclusive exercício ou defesa de um direito num processo judicial.

De notar-se que a decisão de adequação pode ser dada em relação a um país terceiro ou a um ou mais setores específicos desse país.

Esse dispositivo se encontra descrito no art. 36 da Diretiva e nos itens 66 a 70 da Explanação de Motivos. Ele traz os critérios adotados para decidir pela adequação, abrindo a possibilidade para a transferência de dados pessoais para um setor específico do país que já atenda o nível esperado de proteção, mesmo que o país não tenha completamente se adequado a todas as regras de proteção. Ele possibilita, portanto, que as transferências de dados pessoais para esse setor específico do país terceiro ocorram sem necessidade de autorização específica, facilitando sobremaneira a circulação dos dados pessoais e permitindo a fluidez tão desejada e necessária no âmbito da prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Embora as disposições mais estritas concernentes à transferência internacional de dados pessoais para fins de investigações criminais ainda não estejam sendo aplicadas na prática, à medida que em alguns Estados se movimentaram para aumentar o grau de proteção desses dados, os demais Estados passaram a reformular suas legislações para acompanhar a evolução na sofisticação das medidas.

4. OS MECANISMOS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS PREVISTOS NA CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste indica, basicamente, duas formas de transferência internacional de dados para fins de investigações criminais, por meio de cooperação internacional e por meio de acesso direto.

4.1. COOPERAÇÃO INTERNACIONAL

A cooperação internacional prevista na Convenção é regida pelos arts. 23 e seguintes, podendo caracterizar-se pela transmissão espontânea de dados, art. 26[3], quando um Estado-parte identifica elementos que possam justificar o início de investigação criminal por outro Estado-parte, e pelo cumprimento de pedidos de cooperação. Nesse contexto, regulado pelos arts. 27 e seguintes, a própria Convenção pode servir como tratado disciplinador da cooperação, caso os dois envolvidos optem por utilizá-la ou caso não possuam entre si instrumento próprio de cooperação internacional.

3. Art. 26 - Uma Parte pode, dentro dos limites de sua legislação interna e sem pedido anterior, transmitir, para outra Parte, informações obtidas por seu próprio sistema investigativo, quando considerar que o encaminhamento de tais informações pode auxiliar a Parte destinatária a iniciar ou a levar adiante investigações ou procedimentos relativos a crimes tipificados de acordo com esta Convenção ou possa levar a um pedido de cooperação por aquela Parte, em conformidade com este capítulo (...). (Tradução nossa).

A cooperação jurídica em matéria penal regida pela Convenção possui mecanismos próprios para assegurar a rapidez na execução dos pedidos, como a possibilidade de transmissão das solicitações entre autoridades judiciais diretamente responsáveis pelo pedido e pelo cumprimento[4], com simples aviso para a autoridade central em caso de urgência, e a preservação rápida de provas[5], tudo em razão da natureza volátil das provas eletrônicas. Entretanto, de maneira geral, a cooperação prevista na Convenção segue os mesmos preceitos da cooperação jurídica em matéria penal, com análise de cabimento caso a caso, e atendimento individualizado, com ou sem a imposição de condições para uso da prova.

4. Art. 27, 9 a.
5. Art. 29.

4.2. O ACESSO DIRETO TRANSFRONTEIRIÇO

Já os mecanismos de acesso direto trazidos pela Convenção contém avanços considerados significativos na época de sua elaboração, em 2001, embora hoje necessitem de revisão. Os arts. 18 e 32 permitem o acesso direto a dados:

> Artigo 18 - Requisição
>
> < 01 > Cada Estado-Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para ordenar:
>
> < A > a qualquer pessoa em seu território a entrega de dados de computador especificados sob seu controle ou posse, que estejam armazenados em um sistema de computador ou em qualquer meio de armazenamento de dados de computador;
>
> < B > a qualquer provedor de serviço que ofereça serviços no território da Parte para entregar as informações

cadastrais de usuários relacionadas a tais serviços, que estejam sob a posse ou controle do provedor.

< 02 > Os poderes e procedimentos referidos neste artigo estão sujeitos aos artigos 14 e 15.

< 03 > Para fins deste artigo, o termo "informações cadastrais do usuário" indica qualquer informação em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a usuários de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:

< A > o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para o período de serviço;

< B > a identidade do usuário, endereço postal ou geográfico, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com os termos de prestação de serviço;

< C > qualquer outra informação sobre o local de instalação do equipamento de comunicação, disponível em razão dos termos de prestação de serviço,

Artigo 32 - Acesso transfronteiriço a dados de computador armazenados mediante consentimento ou quando acessíveis publicamente

Uma Parte pode, sem autorização de outra Parte:

< A > acessar dados de computador armazenados disponíveis ao público, independentemente de onde os dados estejam geograficamente localizados; ou

< B > acessar ou receber, por meio de um sistema de computador em seu território, dados de computador armazenados localizados no território de outra Parte, se a Parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autorida-

> de legal para entregar os dados à Parte por meio daquele sistema de computador. (PARLAMENTO EUROPEU E DO CONSELHO DA EUROPA, 2016).

O segundo dispositivo lida com situações aparentemente corriqueiras, mas que eram de grande valia quando da entrada em vigor da Convenção.

A alínea *a* reconhece que as autoridades dos Estados-parte podem acessar, de seu território, dados disponíveis ao público, mas que sejam guardados em outro território. A alínea *b* permite que esse acesso se estenda a dados privados desde que haja expresso consentimento do titular dos dados.

Em outras palavras, o dispositivo permite que autoridades de um país acessem e coletem como prova válida dados publicados em sítios mantidos em outro país. Condição para isso é que esses dados sejam públicos ou que seu uso seja consentido, de modo "*legítimo e voluntário*", pelo titular.

Ao condicionar o acesso à natureza pública dos dados ou ao consentimento do titular, o dispositivo não distingue quanto ao tipo de dado, permitindo o acesso direto transfronteiriço a qualquer dado eletrônico, inclusive conteúdo de comunicações, desde que observadas as duas condições mencionadas.

Por outro lado, o art. 18 determina que os Estados-parte, em suas legislações locais, estabeleçam mecanismo que permita às autoridades judiciais a requisição de quaisquer dados armazenados sob a posse ou controle de provedores localizados em seu território (1. a) e de dados cadastrais de usuários que estejam sob a posse ou controle de provedores que prestam serviço em seu território, ainda que estrangeiros (1. b).

Há aqui, portanto, duas situações: uma que permite o acesso, mediante o cumprimento da legislação local, a todos os dados armazenados por provedores locais, incluindo conteúdo; e outra, que permite acesso a dados cadastrais de usuários con-

trolados por provedores estrangeiros, desde que estes prestem serviço no território do Estado requisitante. Admite-se, assim, o acesso direto a dados localizados em outro território e controlados por provedor estrangeiro desde que: a) as informações buscadas se restrinjam a dados cadastrais; e b) e o provedor estrangeiro preste serviço no território da autoridade requisitante.

A legislação brasileira, mesmo antes da adesão formal à Convenção, já permite o acesso direto a dados eletrônicos localizados fora do território brasileiro em termos semelhantes, mas mais amplos. O artigo 11 do Marco Civil da Internet, Lei nº 12.965,de 23 de abril de 2014 determina que, mediante prévia ordem judicial, as autoridades brasileiras tenham acesso a dados armazenados, inclusive conteúdo de comunicações, por empresas brasileiras, ou por empresas estrangeiras desde que: a) ofereçam serviços ao público brasileiro ou b) tenham ao menos um integrante do grupo econômico com estabelecimento no Brasil.

O citado dispositivo 11 é, portanto, mais amplo que a previsão do art. 18. Enquanto este permite o acesso apenas a dados cadastrais de usuários controlados por empresas estrangeiras que prestam serviço no território do Estado-parte, aquele permite o acesso a todos os dados, inclusive conteúdo armazenado por empresa estrangeira, desde que ela oferte serviços a brasileiros ou aqui mantenha estabelecimento de um dos componentes de seu grupo econômico.

5. AS CONSEQUÊNCIAS DO REGIME DE PROTEÇÃO DE DADOS PARA A TRANSFERÊNCIA DE DADOS EM INVESTIGAÇÕES CRIMINAIS – NOVA PROPOSTA

O atual sistema de proteção de dados, mesmo com regras específicas para a persecução penal, afeta diferentemente o regime

de transferência de dados, dependendo do tipo de transferência utilizada.

Para as transferências por meio de cooperação internacional, os acordos de cooperação continuam servindo como base, pois a Diretiva (UE) n. 2016/680, no art. 61 expressamente ressalvou a manutenção dos tratados internacionais em vigor até que sejam alterados, substituídos ou revogados[6].

6. Art. 61. Os acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou para organizações internacionais, celebrados pelos Estados-Membros antes de 6 de maio de 2016, e que sejam conformes com o direito da União tal como aplicável antes dessa data, continuam a vigorar até serem alterados, substituídos ou revogados.

Essa disposição permite a continuidade da troca de informações no âmbito da cooperação policial e da cooperação judiciária internacional. Se tal não fosse, toda a circulação de dados para fins de persecução penal a prevenção às infrações penais estaria paralisada em razão das exigências desta normativa, uma vez que o nível de proteção dos dados exigido dos países terceiros não é passível de ser alcançado no curto prazo devido às inúmeras adequações que precisam ser feitas.

Tal solução, porém, é provisória, sendo indispensável buscar solução definitiva que passa pela decisão de adequação.

Quanto ao acesso direto, os efeitos da ausência de decisão de adequação podem começar a ser sentidos imediatamente. Como mencionado, a Convenção de Budapeste prevê dois tipos. O previsto no art. 32 não é afetado pelas disposições da Diretiva porque se refere a dados públicos, não abrangidos pelo regime de proteção de dados, ou a dados privados que são acessados mediante o consentimento do titular. Não há, assim, problema para a transferência.

Entretanto, o assunto adquire outra relevância quando se trata de acesso direto à prova eletrônica, nos termos do art. 18 da Convenção de Budapeste e do art. 11 do Marco Civil. Nesses casos, sem decisões prévias de adequação ou de reco-

nhecimento de salvaguardas, as empresas europeias que aqui prestam serviços a usuários brasileiros podem se considerar impedidas de transferir os dados, com sérias consequências para investigações penais em andamento.

Enquanto a decisão sobre a adequação do regime brasileiro de proteção de dados não vem, e na pendência da ratificação da Convenção de Budapeste, que poderá servir como respaldo jurídico para a transferência de dados pessoais, faz-se necessário o estabelecimento de outro modelo, que permita que o fluxo de dados para fins de persecução penal não seja interrompido[7]. Nesse sentido, propõe-se ao Ministério Público Federal adequação ao quanto exigido pela Diretiva e pelo GDPR, recebendo em nome próprio a decisão de adequação.

7. Tratados internacionais podem servir de base legal para permitir a transferência de dados, incluindo a Convenção de Budapeste (CETS 185 – CONSELHO DA EUROPA, 2001).

Como exposto, nos termos do art. 36 da Diretiva (UE) n. 2016/680, a decisão de adequação pode ser concedida não apenas a países terceiros, mas a territórios ou a um ou mais setores específicos de um determinado país. Exemplo disso, é a decisão de adequação, ainda vigente apesar de baseada na antiga Diretiva (UE) n. 95/46 - substituída pelo GDPR -, que reconhece apenas os setores abrangidos pela lei canadense de dados pessoais e documentos eletrônicos como adequados à regulação europeia[8]. É possível, assim, que determinados setores sejam reconhecidos como adequados, ainda que o país como um todo não o seja.

8. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002D0002&from=en. Acesso em: 14 out.2020.

Neste ponto é que se propõe que o sistema nacional de Justiça, em especial o Ministério Público e o Poder Judiciário, busquem a adequação exigida pelo GDPR e pela Diretiva (UE) n. 2016/680.

Enquanto o Brasil, como Nação, não obtém a decisão de adequação, o que hoje depende, em grande parte, da estrutura da Autoridade Nacional de Proteção de Dados - ANPD, tanto o Ministério Público, quanto o Poder Judiciário, podem buscar essa adequação para fins de acesso direto de dados em investigações criminais, como um setor específico.

Embora ainda não tenha sido editada lei regulamentando a proteção de dados referentes a segurança pública e investigações criminais, é certo que o sistema de Justiça brasileiro tem todas as condições de se adequar ao regime da diretiva. O acesso a dados pessoais somente é feito mediante ordem judicial, por meio de decisão fundamentada, em casos específicos e para a investigação de condutas determinadas. Os dados obtidos são mantidos sob sigilo durante todo o processo penal, com acesso restrito às partes. O uso em outros feitos depende também de autorização judicial, o que estabelece sistema robusto de proteção. Ademais, o titular dos dados é informado da obtenção e do uso, ainda que de forma diferida, possuindo mecanismos legais para excluir os dados a qualquer momento, seja nos próprios autos, ou por meio de ações autônomas, como *habeas corpus* e mandado de segurança.

Importante notar que o sistema legal, em vigor, não precisa ser uma cópia, ou o reconhecimento item por item das previsões do sistema europeu, bastando que as proteções sejam equivalentes. Ademais, a análise da adequação do setor funda-se nos aspectos específicos desse setor. O item 67 da exposição de motivos determina que:

> De acordo com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou de um setor específico num país tercei-

> ro, ter em consideração em que medida um determinado país respeita o primado do Estado de direito, o acesso à justiça, bem como as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. *A adoção de uma decisão de adequação relativa a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro.* Este deverá dar garantias de assegurar um *nível adequado de proteção, essencialmente equivalente ao segurado na União,* em particular quando os dados são tratados num ou em vários setores específicos. Em especial, o país terceiro deverá garantir o controle efetivo e independente da proteção dos dados e estabelecer mecanismos de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial (UNIÃO EUROPEIA, 2016 - Grifos nossos)

Vê-se, portanto, que para fins de investigações e processos criminais, o arcabouço legal, em vigor, no Brasil, já atende ao quanto exigido pela diretiva e pelo GDPR. Embora ainda não haja legislação específica sobre o assunto, como exigido pela LGPD, as limitações impostas pela Constituição Federal, pelo Marco Civil e pela legislação processual penal já são suficientes para assegurar proteção adequada aos dados e demonstrar adequação ao sistema europeu. Assim, o reconhecimento dessa adequação é medida que pode ser buscada pelo Poder Judiciário e Ministério Público, como um setor à parte.

6. CONCLUSÃO

O novo sistema de proteção de dados pessoais introduzido pelo GDPR, pela Diretiva (UE) n. 2016/680, e pela LGPD precisa ser levado em consideração na busca de provas em investigações e processos criminais.

Esse sistema pode gerar consequências para a correta aplicação do art. 11 do Marco Civil da Internet, em especial, quanto à obtenção de dados de empresas europeias, que prestam serviço no Brasil, e que, por estarem submetidas aos diplomas normativos da UE, podem criar empecilhos para o acesso direto aos dados, na forma da lei brasileira.

Solução de longo prazo, e que precisa ser buscada, é o reconhecimento da adequação da legislação brasileira ao quanto exigido pelas normas europeias. Enquanto essa adequação não é obtida, o Poder Judiciário e o Ministério Público podem buscar o reconhecimento da adequação como setor específico, que já cumpre o quanto exigido.

Isso permitirá que os dados sejam transferidos sem interrupção para fins de persecução penal, possibilitando a continuidade de investigações em andamento e assegurando a celeridade exigida pela natureza da prova eletrônica.

REFERÊNCIAS BILIOGRÁFICAS

BRASIL. *Lei no 12.965 de 23 de abril de 2014*. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 14 out. 2020.

BRASIL. *Lei no 13.709 de 14 de agosto de 2018*. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 out. 2020.

BRASIL. *Lei no 14.010 de 10 de junho de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/

lei/L14010.htm#:~:text=Disp%C3%B5e%20sobre%200%20Regime%20Jur%C3%ADdico,coronav%C3%ADrus%20(Covid%2D19).&text=Art.&text=3%C2%BA%20Os%20prazos%20prescricionais%20consideram,30%20de%20outubro%20de%2020. Acesso em: 14 out. 2020.

BRASIL. *Medida Provisória 959 de 29 de abril de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 14 out. 2020.

BRASIL. Ministério Público Federal. *Notas técnicas 4 e 5*. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas. Acesso em: 14 out.2020.

CARVALHO, Angelo Gamba Prata de. Transferência internacional de dados na Lei Geral de Proteção de Dados – Força normativa e efetividade diante do cenário transnacional. *In*: FRAZÃO Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito brasileiro*. São Paulo: Thompson Reuters do Brasil. 2019.

CONSELHO DA EUROPA. Convenção de Budapeste. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 8 out. 2020.

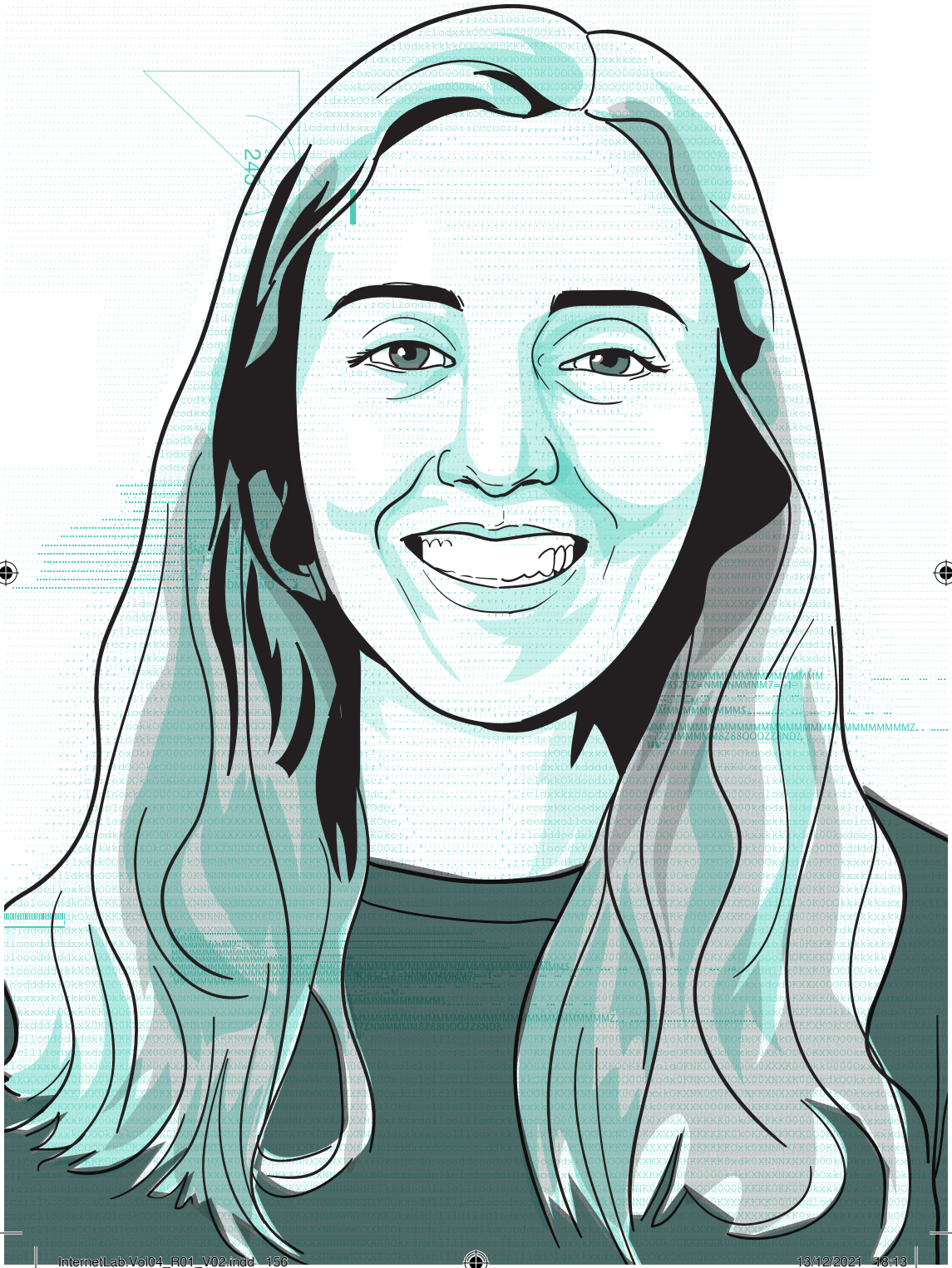
DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul.-dez. 2011.

JÚNIOR, Janary. Maia cria comissão de juristas para propor lei sobre uso de dados pessoais eminvestigações: Colegiado terá 120 dias para elaborar o anteprojeto que, depois, será analisado pelo Congresso. Brasília. Câmara dos Deputados, 27 nov. 2019. Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em: 14 out.2020.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho da Europa. *Diretiva (UE) 2016/680 de 27 de abril de 2016*. Disponível

em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=EN#d1e1048-89-1. Acesso em: 14 out. 2020.

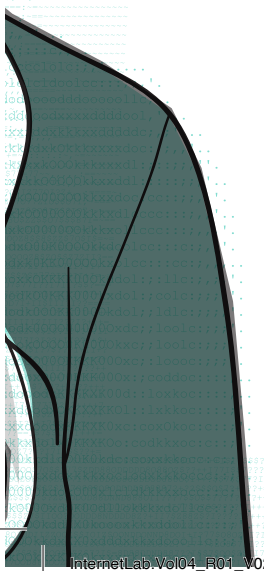
UNIÃO EUROPEIA. Parlamento Europeu e Conselho da Europa. General Data Protection Regulation – GDPR 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 14 out. 2020.



10.

PROTEÇÃO DA PRIVACIDADE E COOPERAÇÃO JURÍDICA INTERNACIONAL

Jacqueline Abreu[1]



1. O presente texto se baseia em apresentação oral feita no painel "Proteção da privacidade e cooperação jurídica internacional" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

I.

Bom dia a todos. É um prazer enorme estar aqui com vocês, Luísa e Neide, que têm sido parceiras no diálogo sobre esse tema já há bastante tempo, e que têm me ensinado tanto. Chico e Nathalie, queria cumprimentar por mais essa edição do Congresso. Me dá muita alegria ver o quanto o Congresso cresceu, quanto os debates estão cada vez mais sofisticados.

Já fiz o meu agradecimento, queria só fazer o *disclaimer*. Hoje, como o Chico disse, eu atuo como advogada, mas esse é um tema que eu comecei a estudar há bastante tempo, pelo menos desde o meu mestrado em 2015, e foi um tema que explorei também bastante como coordenadora de pesquisa no InternetLab, então o que eu falo aqui hoje vem justamente dessas minhas reflexões acadêmicas.

Vou tratar hoje de cooperação jurídica internacional propriamente dita e localizar como a questão sobre a proteção da privacidade se coloca nesse debate. A seguir, vou falar de como isso se localiza dentro de um debate mais abrangente sobre transferências internacionais de dados, e que eu acho que está principalmente em pauta hoje quando estamos pensando no anteprojeto de lei de proteção de dados em matéria de segurança pública e investigações criminais.

II.

O plano de fundo dessa primeira parte, sobre cooperação internacional, como o próprio Chico antecipou, é um caso que está no STF. Então a principal provocação do painel, quando se fala de cooperação jurídica internacional, diz respeito a uma questão que frequentemente se coloca em investigações, em processos penais hoje em dia, que é responder quando um país depende da cooperação com outro país para conseguir a produção de provas ou de elementos de prova relevantes para a investigação. Essa é uma pergunta que está no centro da ADC 51, principalmente nessa for-

mulação: há necessidade de pedido de cooperação internacional para obtenção de conteúdo de comunicações quando o provedor de origem estrangeira, principalmente essas plataformas de internet, controla os dados, mas presta também um serviço direcionado ao Brasil ou tem uma filial no Brasil? Ou nessas circunstâncias o pedido pode ser feito diretamente por autoridades brasileiras, mediante o preenchimento dos requisitos apenas da legislação brasileira para acesso àquela prova, isto é, sem necessitar de pedido diplomático?

Essa é uma questão fundamentalmente de *jurisdição* sobre os limites dos poderes de Estado frente a outros Estados, mas vale analisarmos principalmente que tipo de questão de jurisdição é essa. Podemos pensar em jurisdição em três sentidos: jurisdição no sentido de competência judiciária, ou jurisdição prescritiva legislativa, ou uma jurisdição executiva. A discussão por exemplo da ADC 51 é uma discussão sobre competência judicial? Ao meu ver, não. Para que seja colocada a questão sobre a necessidade da cooperação jurídica internacional no âmbito de uma investigação concreta, já se precisa supor que as autoridades envolvidas nessa investigação, nesse processo penal, possuem competência efetivamente para investigar e apurar determinado crime, e aqui, como estamos falando no Brasil, em um crime ocorrido no Brasil que tenha produzido efeitos no Brasil. Então, focar só nessa questão não resolve o nosso problema. Isso na verdade não faz parte fundamentalmente do debate; existe jurisdição dos órgãos judiciais brasileiros nas investigações em que isso aparece.

Há uma discussão, por outro lado, sobre lei aplicável depois que é fixada essa questão da competência do juiz. A próxima questão natural que se coloca, principalmente quando estamos pensando em lógicas de direito internacional privado, é estabelecer qual lei vai ser aplicável para resolver essa demanda, esse caso. E aqui acho que começamos a nos aproxi-

mar do núcleo desse debate, mas ao mesmo tempo também das confusões que assombram com frequência essa discussão. Qual é a pergunta sobre lei aplicável que nós estamos fazendo em um caso como a ADC 51? Em certo sentido, me parece que, em um sentido bastante abrangente de lei aplicável, é óbvio que há respostas sobre qual é a lei que governa investigações no Brasil, ou serviços que são prestados no Brasil, é a legislação brasileira. Acontece que estamos olhando para um núcleo, isto é, a questão de lei aplicável em um aspecto muito específico dentro de uma investigação, que é como deve ser regrada a produção de provas, ou de meios de informação, dentro desse processo quando existe uma repercussão internacional.

Então, particularmente aqui, é uma questão de como deve ser regrado o acesso a dados, conteúdo de comunicações, que são bens intangíveis - eles estão em toda parte ao mesmo tempo, ou podem ser movidos com muita facilidade - e que são controlados por empresas que também tem uma atuação transnacional, estão presentes a nível de internet praticamente em todos os países, então é uma questão muito mais pontual de lei aplicável. Nessa circunstância, qual é a lei que deve governar o acesso a dados, ou quais leis devem controlar a situação? E aqui me parece então, era esse o ponto que eu queria chegar, que esbarramos em uma questão sobre o encontro de jurisdições prescritivas: a natureza dos dados levam mais de um país a instituir leis que se aplicam ao mesmo conjunto de dados, digamos assim, ou ao mesmo conjunto de empresas simultaneamente, e isso amplia as ocasiões em que há conflitos de lei. Eu vou retomar esse ponto mais a frente, era só essa ideia que eu queria passar agora.

O terceiro ponto: esse é um debate sobre jurisdição executiva? Sobre enforcement? Sobre até onde o Estado pode ir para executar uma decisão válida sobre a sua própria lei? Eu também responderia positivamente a essa pergunta. O debate efetiva-

mente nasceu assim. Mas hoje em dia para resolvermos essa discussão precisamos nos reportar diretamente a essas questões de jurisdição prescritiva e conflitos de lei. Vou explicar porquê.

III.

Como que tradicionalmente se sinalizava, dentro de uma investigação, que é necessária a cooperação jurídica internacional? O que levava a acionar esse mecanismo de fazer um pedido de cooperação judiciária, que é regulado por exemplo por esses MLATs - o tratado de cooperação mútua internacional? Dentro do modelo histórico e tradicional dos MLATs, o critério que aciona essa necessidade, o que faz trazer à tona que será necessária a cooperação, era um elemento de localização física da prova fora do país - eu preciso obter um testemunho de uma pessoa que está em outro país, ou um objeto físico que está em outro país - e continuou sendo assim quando se está falando sobre pessoas e objetos físicos. Mas nós estamos agora em um ponto de inflexão, de exaustão desse modelo, já que ele não funciona mais tão bem em termos normativos e práticos quando nós estamos falando de provas eletrônicas – bens intangíveis que são detidos por provedores de aplicação de internet que têm atuação global. Um modelo que realmente não é eficiente, é bastante burocrático e hoje em dia ele está pensado em cima de um critério de localização de prova que não faz mais tanto sentido quando estamos falando de dados eletrônicos.

Então é isso que nós estamos revendo agora. O debate, ao meu ver, é principalmente sobre como aperfeiçoar esses mecanismos para que esses problemas de burocracia, de lentidão, não mais existam, e também para pensarmos em critérios que hoje façam sentido efetivamente para acionar essa necessidade de cooperação jurídica internacional. A localização física da prova, do elemento, do dado, não faz mais sentido já que

dados podem ser compartimentalizados e transferidos com muita facilidade e também podem estar armazenados em outro país mas alguém dentro de outro país pode ter acesso. Ao mesmo tempo, e esse é um critério às vezes alternativo que se coloca, a localização da empresa que tem controle sobre essas informações também não é um critério que efetivamente parece conseguir resolver o problema. É um critério bastante frouxo porque essas empresas possuem uma atuação global, então não se resolve o problema de saber quando a cooperação judiciária internacional é necessária: você tem mais de uma legislação de um país governando a mesma empresa ou determinados dados.

IV.

Nesse contexto, para avançar nessa discussão, o que temos que fazer? Como deve ser repensado esse modelo? Eu queria retomar o título do painel: "Proteção da Privacidade e Cooperação Jurídica Internacional", que eu achei muito pertinente porque me provocou a pensar nesse tema sob essa perspectiva. E é curioso que eu não falei, até aqui, em privacidade, se vocês observaram. Então qual é a questão da privacidade que está por trás na questão de cooperação jurídica internacional? Existe em certo sentido uma resposta bastante óbvia de que essa não é uma discussão sobre privacidade, não estamos discutindo aqui o sentido de privacidade, até onde vai esse direito. Então, por exemplo, ontem teve esse painel sobre o sigilo das comunicações e qual é o escopo do sigilo das comunicações, o que faz sentido hoje ou que não faz mais sentido manter hoje de concepção mas que fazia sentido 30 anos atrás e coisas assim, se vocês assistiram. Tivemos também um painel que estava discutindo se determinados critérios substantivos de restrição da privacidade quando estamos pensando em mecanismos como esses métodos ocultos de infiltração.

/ É UMA QUESTÃO DE COMO DEVE SER REGRADO O ACESSO A DADOS, CONTEÚDO DE COMUNICAÇÕES, QUE SÃO BENS INTANGÍVEIS /

/ O NOSSO DIREITO DE PRIVACIDADE DEPENDE DE COMO NÓS RESOLVEMOS ESSA PERGUNTA DE JURISDIÇÃO DE QUAL CRITÉRIO ACIONA A COOPERAÇÃO JURÍDICA INTERNACIONAL /

Então era uma discussão material de: isso pode, e se pode, quais devem ser os critérios?

Essa discussão sobre cooperação jurídica não é sobre privacidade nesse sentido. Mas certamente há diversas implicações para privacidade a partir da forma como resolvemos essas questões de jurisdição. O nosso direito de privacidade depende de como nós resolvemos essa pergunta de jurisdição de qual critério aciona a cooperação jurídica internacional. E isso em dois sentidos relacionados: (i) sobre o nível de proteção que indivíduos em países que não são comprometidos com direitos humanos terão acesso e (ii), pensando mais diretamente em nós aqui no Brasil, sobre a extensão e a efetividade da proteção de privacidade que a nossa legislação garante frente a Estados estrangeiros. E inclusive frente a países que não tem um histórico positivo de proteção a direitos humanos.

Para explicar essa ideia eu gosto sempre de retomar um trecho de um *amicus curiae* do relatório de privacidade da ONU, o Joe Cannataci, que apresentou no caso Microsoft Ireland em uma parceria que ele fez com a Harvard Law Clinic:

"The Court cannot decide this case without implicitly endorsing (or rejecting) a theory of what jurisdictional contacts are adequate (or not) for one sovereign to seize certain data unilaterally, when there are other sovereigns with very significant jurisdictional interests in this data. This may pose a danger to the protection of the right to privacy in cyberspace, especially if non-rights respecting states should adopt for their own ends jurisdictional theory that this Court espouses." (p.2)[1]

Esse caso, Microsoft Ireland, discutia uma questão de jurisdição sobre quais deveriam ser os critérios quanto à necessidade de cooperação internacional - uma versão semelhante da ADC 51 - e chegou até a Suprema Corte dos Estados Unidos para então

1. A peça pode ser encontrada em: https://clinic.cyber.harvard.edu/2018/01/03/cyberlaw-clinic-files-brief-for-un-special-rapporteur-in-microsoft-ireland-case/ .

ser considerado prejudicado porque a questão foi resolvida legislativamente. Mas, enfim, esse trecho bastante interessante alerta que a Corte não pode decidir sobre esse caso sem implicitamente endossar ou rejeitar uma teoria sobre quais os contatos jurisdicionais são adequados ou não para que um estado soberano apreenda certos dados unilateralmente, isto é, sem ter de recorrer a esses mecanismos de cooperação internacional. A implicação da decisão da Suprema Corte, nesse caso, seria de que ela teria que se posicionar sobre quando o MLAT precisa ser acionado ou não. E quais são os critérios então que devem controlar? O que vale em último grau para que haja a produção unilateral dessa prova? Se é só termos de jurisdição sobre a empresa, é só passar uma lei que assim disponha; se é a localização dos dados, é só aprovar uma lei que determine a localização obrigatória dos dados em certo local; mas se é um outro critério ou um conjunto de critérios, temos que repensar e pensar nas implicações que isso tem.

A ideia então aparece principalmente nessa última frase dele, de que isso pode colocar um perigo para a proteção de direito à privacidade no ciberespaço, especialmente se países que não respeitam direitos humanos adotem essas mesmas teorias e critérios que estamos defendendo/usando. Temos que pensar então no exemplo que vamos dar na hora de discutir essa questão e como resolvê-la para que não se instaure uma corrida destrutiva que praticamente anule efetivamente as proteções nacionais que nós temos de direito à privacidade. E que não dê um mau exemplo para outros países que não são tão comprometidos com esses direitos, para que tanto quanto possível se garanta a essas pessoas nesses outros países algum nível ainda de proteção.

Para comentar essa ideia, nessa busca ainda para o que colocamos no lugar dos critérios antigos, como pensamos, eu acho que faz sentido pensar por que os países protegem dados.

Eu trouxe essa frase do Cannataci porque esse é um cuidado, um alerta que cabe ao nosso STF na ADC 51. Mas, retomando, porque os países protegem dados? É claro que existe um interesse muito forte na própria proteção dos cidadãos, uma proteção básica de direitos humanos. Há um interesse na proteção da economia e por tanto das empresas que prestam determinados serviços em certo país, para que elas cresçam. Há o impacto internacional, por isso também se estabelecem regras sobre esse assunto. E há também um interesse na proteção da segurança nacional para que não haja espionagem.

O que vemos nesse nível? O Marco Civil da Internet protege essas informações dos brasileiros. O Stored Communications Act lá dos Estados Unidos também protege informações que são guardadas por provedores, e nos Estados Unidos é uma proteção que busca principalmente ser complementar à Quarta Emenda. No regulamento Europeu também existe essa noção no tratamento de dados de agentes situados na EU mas, mesmo quando eles não estejam, dos titulares de dados que são situados na EU. Então nós temos uma noção que é principalmente voltada à proteção de pessoas e isso é algo extremamente e inequivocamente legítimo. Quando você tem uma investigação aqui no Brasil, por tanto, que esbarra em uma legislação americana nesse sentido de produção de prova, faz sentido que ela deva ser levado em conta, tanto quanto pertinente, para que esse interesse legítimo que outros países têm na proteção de suas empresas, e principalmente de seus cidadãos, seja levada em conta.

Por isso que precisamos pensar em um mecanismo que acomode essas noções e esses interesses legítimos que outros países tenham. Por isso que, quando surge uma investigação, é necessário considerar se isso pode violar a legislação de outro país e como isso afeta cidadãos de outros países. É necessário que seja levado em conta a legislação desses outros países que

se aplique simultaneamente, para que não haja uma anulação dessa lei de um país pelo outro. Esse seria um exemplo que não gostaríamos de dar. Se hoje nós desconsiderarmos as leis de um país; amanhã eles desconsideram as nossas. Não há proteção de privacidade garantida por um país que sobreviveria a outro. Ao mesmo tempo, não queremos que essa lógica sirva para que países que não tenham respeito nenhum a direitos humanos consigam driblar mecanismos de cooperação que hoje servem justamente para garantir um nível básico de comprometimento com o devido processo legal e direitos humanos. Por isso é importante que os critérios para a cooperação judiciária internacional sejam bem pensados e respeitados.

Hoje essa é uma discussão que tem aparecido no PL [das Fake News]. Há um dispositivo que planeja reforçar essa ideia de que " dados devem ser mantidos aqui, deve ser possível acesso direto aqui" e assim aparece um debate que é paralelo ao que acontece no STF. A meu ver, e era esse o ponto, essa não é uma discussão que dá para ser resolvida unilateralmente. Essa discussão sobre critérios, sobre como avançar os mecanismos e repensar os critérios internacionais que vão mobilizar a necessidade de cooperação ou não é algo que você precisa combinar com os outros países, como que isso deve ser feito ou não. Então é um debate que precisa ser feito a nível internacional.

V.

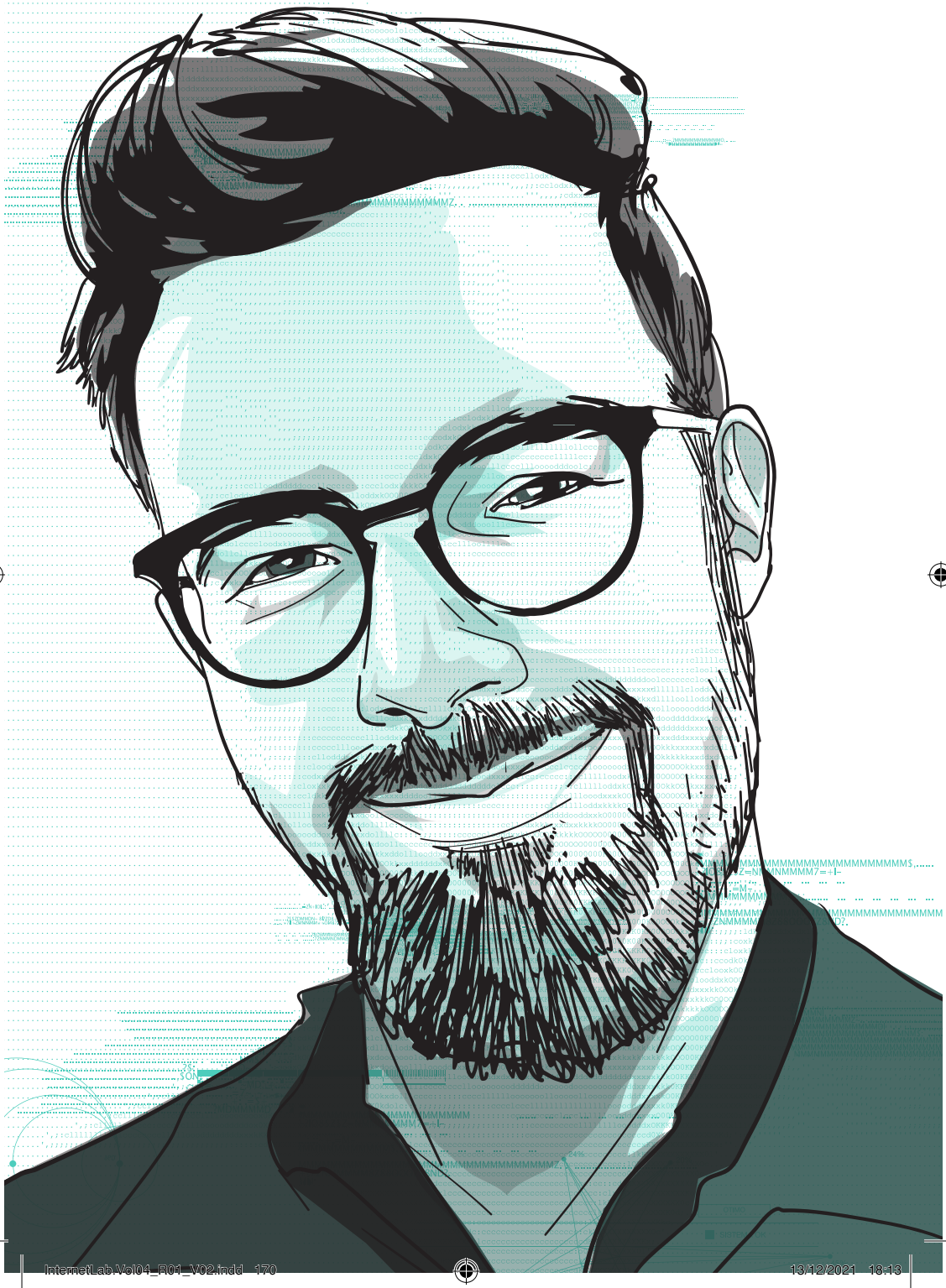
O último comentário que eu gostaria de fazer é sobre o ponto de chegada do anteprojeto. Essa discussão sobre cooperação internacional que eu apresentei até aqui é uma discussão muito pontual dentro do cenário de transferências internacionais de dados. É possível fazer uma tipologia bem simplificada sobre diferentes cenários de transferência internacional de dados.

Vinha falando de uma questão de transferência internacional de dados que podemos chamar de assimétrica, entre uma autoridade e uma empresa, e aqui sobre uma questão dos dados que são controlados por empresas estrangeiras e quando eles podem ser enviados para autoridades no Brasil. Mas você pode pensar em outros sentidos. Você pode pensar nessa mesma transferência internacional assimétrica de dados de autoridades aqui no Brasil para uma empresa no exterior, principalmente quando você encaminha informações de um processo para que haja depois esse retorno de dados a serem produzidos dentro de uma investigação. E mais fundamentalmente também sobre transferências internacionais simétricas, então entre autoridades, nos dois sentidos também, de dados controlados e armazenados por autoridades no exterior para o Brasil e de dados brasileiros, que eu a chamei aqui, para o exterior.

Quando estamos pensando em uma legislação de proteção de dados, me parece que temos que pensar nesse nível mais macro e que também contempla esses exemplos, principalmente nesse tipo dois, que envolvem, por exemplo, acessos a compartilhamentos de banco de dados a nível internacional. Que é como, por exemplo, quando você pensa em instituições de cooperação como a EuroPol, a InterPol, e por isso esses fluxos devem ser governados de forma mais abrangente, que vão envolver obrigações ativas e passivas do governo brasileiro de compartilhamento de dados a nível internacional. Então é algo que não podemos esquecer.

Tentamos resolver parcialmente esse ponto com a LGPD, mas ainda tem sido um entrave - facilitar a participação do Brasil em mecanismos de cooperação - principalmente essas diretas entre autoridades, porque não temos ainda uma lei específica. Então fica a pergunta sobre como deve ser essa legislação específica.

Muito obrigada!



11.

BANCOS DE DADOS PÚBLICOS E O COMPARTILHAMENTO COM AGÊNCIAS PENAIS

Yuri Corrêa da Luz[1]

1. O presente texto se baseia em apresentação oral feita no painel " Bancos de dados públicos e o compartilhamento com agências penais" no IV Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2020.

Primeiramente gostaria de agradecer ao InternetLab pela possibilidade de participar desse painel. Para mim é uma grande alegria poder participar dessa mesa, com gente tão qualificada, a respeito de um tema que está na pauta do dia, e a troca de conversa aqui com certeza ajuda a gente a avançar nesse debate. Eu acho que vou frustrar um pouco as pretensões daqueles que imaginam que, enfim, eu sou do Ministério Público e eu tenho uma visão assim muito pró-compartilhamento de dados. Na verdade, eu tenho muitos pontos de concordância com a fala das painelistas que me antecederam, talvez a única divergência que eu tenha seja em relação a alguns pontos mencionados sobre o COAF. Mas, especificamente na minha fala, vou tentar fazer uma provocação para que pensemos em um outro foco, a respeito do qual eu acredito que precisa haver uma reflexão grande quando estamos preocupados com essa tensão entre privacidade e segurança.

Quem se preocupa com essa tensão e com direitos à privacidade normalmente está monitorando debates legislativos sobre bancos genéticos, a discussão que se coloca em termos de sua constitucionalidade, e também a jurisprudência que se desenvolve a respeito, tanto em torno da legislação aprovada, quanto de casos concretos de investigação, da possibilidade ou não de uso de GPS para monitoramento policial, da possibilidade de acesso a conteúdo de celular obtido a partir de contexto de flagrante etc.. Enfim, esses planos de debate legislativo e de discussão jurisprudencial são de fato muito importantes para avaliação e aprimoramento da nossa compreensão sobre direito à privacidade. Mas não são só nesses planos que decisões muito importantes sobre privacidade são tomadas no nosso país. A fala da Priscila tratou de um plano muito importante em termos *institucionais*: do compartilhamento de dados tanto com base legal quanto com base em convênio de intercâmbio de informação – por exemplo, quando cartórios, Detrans, COAF, Receita, sistema bancário, compartilham dados que são considerados da esfera privada de um cidadão, ou mesmo são

considerados dados relativos a um aspecto específico da vida pública dele. Essas *relações interinstitucionais* são também planos importantes que precisamos monitorar, e a fala tanto da Nathalie quanto a da Priscila colocaram isso muito bem.

Eu gostaria de chamar a atenção para um aspecto que é muito negligenciado no nosso país, que diz respeito às relações, digamos, *intrainstitucionais*, que envolvem disputas entre atores de um mesmo órgão, e que muitas vezes têm consequências gravíssimas para o direito à privacidade das pessoas. Eu vou falar sobre um caso específico que deveria estar no radar, a meu ver, de todo mundo que se preocupa com esses temas, e infelizmente acabou se perdendo na conjuntura da disputa político institucional do país.

Eu não sei se todo mundo sabe, mas em 13 de maio desse ano, a Procuradoria Geral da República expediu ofícios a três forças-tarefas da Operação Lava Jato em Curitiba, no Rio de Janeiro e em São Paulo, requisitando as suas respectivas bases de dados. Ela especificamente pediu que fossem enviados todos os dados, estruturados ou não, com tudo que foi colhido até então e tudo que for colhido a partir daquele momento, alegando que isso se daria com objetivo de subsidiar a atuação de atividades de investigação da PGR, a atuação de coordenação de atividades do Ministério Público em geral, as análises de recursos em trâmite nos tribunais superiores, etc. Essas bases de dados, para termos clareza do que estamos falando, são verdadeiros monumentos de informação de cidadãos investigados no país. Como a Operação Lava Jato é uma operação construída já há muitos anos, só em Curitiba são mais de 60 fases, a verdade é que, ao longo do tempo, as pessoas foram quebrando sigilo de dados, foram realizando buscas e apreensões, reunindo uma enorme quantidade de informações. E como a maioria desses fatos investigados está emaranhada, eles foram se utilizando -na verdade, nós fomos

- nos utilizando de uma série de tecnologias que permitem estruturar essas informações. Então, passou a ser possível fazer buscas por termo, cruzamentos e, em um nível precário ainda em desenvolvimento, até mesmo identificar casos via inteligência artificial. Então, é possível cruzar um dado envolvendo, por exemplo, informações de uma empresa com um dado bancário dela, e verificar, por exemplo, que a movimentação bancária dela é incompatível com quadro de funcionários e, por tanto, ela pode ser uma empresa que está sendo utilizada para lavagem de dinheiro.

Essas bases, portanto, incluem um enorme número de informações que vão desde dados de fontes abertas até dados obtidos por meio de quebras sujeitas à reserva de jurisdição. Algumas inclusive de fora do país, via pedidos de cooperação internacional, informações espontâneas enviadas por autoridades investigadoras estrangeiras etc.

Exatamente porque essas bases abrangem uma série de dados sigilosos, as forças tarefas responderam à PGR dizendo que não poderiam encaminhar todos eles sem autorizações específicas, e negaram o compartilhamento. Só que, em razão disso, a PGR achou relevante ajuizar uma reclamação contra todas as forças-tarefas, aduzindo basicamente dois argumentos.

O primeiro argumento é o de que isso seria importante para eficiência das investigações da PGR. Como já já nessas bases de dados que estão disponíveis, que já foram entregues por bancos, pelo Fisco, por outros países, é muito mais fácil eu pegá-los ali do que eu pedir novamente, então existe aí uma ideia de eficiência, de necessidade e de eficiência às investigações. E um segundo argumento que foi utilizado, foi a ideia de unidade do MPF. O Ministério Público é regido constitucionalmente por alguns princípios - unidade, independência institucional e indivisibilidade -, e segundo a PGR, o princípio da unidade autorizaria que esses dados

/ ESSAS BASES DE DADOS, PARA TERMOS CLAREZA DO QUE ESTAMOS FALANDO, SÃO VERDADEIROS MONUMENTOS DE INFORMAÇÃO DE CIDADÃOS INVESTIGADOS NO PAÍS /

/ É POSSÍVEL PENSAR EM ESTRATÉGIAS DE MAXIMIZAÇÃO DE EFICIÊNCIA QUE NÃO IMPLIQUEM ABSOLUTA DESIDRATAÇÃO DO DIREITO À PRIVACIDADE /

quando são entregues pelo judiciário, ou na verdade com autorização judicial pelos diversos órgãos, não pertencem ao procurador X, mas sim à instituição Ministério Público. E como a Procuradoria Geral da República é o ápice da instituição, ela poderia ter franco acesso, livre acesso, a esse conjunto gigantesco, que foi contabilizado recentemente com mais de 13 terabytes de informações, sem necessidade de autorização específica, de um juízo específico que cuida de determinado caso.

Essa reclamação foi objeto de uma liminar por parte do ministro Dias Toffoli em plantão, concedendo acesso às bases de dados. A PGR começou a extrair esses dados de Curitiba, não chegou a extrair tudo e não chegou, portanto, às bases de dados de São Paulo e do Rio porque logo na sequência, no final do recesso judiciário, a liminar que tinha sido concedida pelo Dias Toffoli foi revogada pelo Fachin. Mas como a PGR agravou dessa decisão, a questão hoje pende de decisão no STF do colegiado. Ou seja, estamos diante -e isso é uma coisa que eu queria chamar atenção - de uma disputa que parece muito coorporativa, de tensão institucional entre órgãos do Ministério Público (a PGR e as forcas-tarefa da Lava Jato), mas, se formos tentar voar acima dessa conjuntura, podemos ver que ela afeta fortemente os direitos fundamentais do cidadão, e precisamos ficar atentos a isso quando temos uma preocupação com os direitos à privacidade.

A primeira coisa que queria chamar a atenção é para o fato de que existem vários problemas no raciocínio da PGR. O primeiro dos problemas é ignorar que essa noção de compartilhamento amplo, fundada nesse princípio da unidade, subverte muito da mecânica de proteção da privacidade no processo penal que conhecemos. Como funciona a proteção à privacidade pelo processo penal? Temos reconhecido na Constituição o direito à privacidade. E esse direito à privacidade, mais do que

só uma conquista civilizatória, enseja uma pretensão de todo cidadão de ter relativizados seus sigilos somente em casos em que são oferecidas boas razões para tanto. Então, quando eu guardo alguma coisa na minha casa, quando eu falo no telefone, eu tenho sempre uma expectativa de aquilo é privado, e não vai ser acessado, salvo se, em hipóteses excepcionais, o Estado me der *boas razões*.

Dar boas razões, na mecânica do processo penal, significa levar ao Judiciário, que vai atuar como um limitador de pretensões das investigações, uma série de elementos para que ele possa avaliar se o acesso pode ser autorizado. Eu vou ter que explicar para o juiz *quais são as suspeitas* que eu tenho contra o investigado, eu vou ter que explicar para o juiz *qual é a base legal* para eu acessar aquele dado, ou seja, não é só porque eu quero e porque parece que alguém está praticando um crime, eu tenho que dizer qual é o fundamento jurídico para que ele possa me entregar um dado ou mandar um ente entregar. E principalmente, eu tenho que dizer para qual *finalidade* que esse acesso é pretendido, ou seja, não é para investigar a vida da pessoa como um todo, é para investigá-la em um dado contexto ilícito e só naquele contexto ilícito. Quando o Judiciário, crivando essas razões, autoriza que órgãos de investigação do Estado em geral acessem determinados dados sensíveis, ele o faz, portanto, vinculando esse acesso a *motivos específicos*, e a *fins específicos*. Então, o sigilo relativizado não é aberto *indiscriminadamente,* ele é aberto, na mecânica do processo penal, de maneira *contextual*.

E se a gente for pensar nisso, é exatamente por esse motivo que, se um órgão investigador de uma localidade X aqui em São Paulo, no contexto de uma investigação específica de lavagem de dinheiro daqui, pede ao juízo competente para ter acesso a um dado bancário, esse dado fica restrito àquele ofício, àquele órgão investigador específico. Isso não significa,

como parece sugerir a tese da PGR na reclamação nº 42050, que estamos falando de um procurador que quer se arrogar a uma posição de superior, ou alguém que não quer se submeter à unidade do Ministério Público. Muito pelo contrário, trata-se de reconhecermos que esses dados privados acessados por um órgão investigador seguem, na linha do que foi dito pela Priscila, sendo *do cidadão*, e não passam a ser do Estado apenas porque em dado momento este o acessa. Dito com um exemplo:, quando eu acesso um diário de um sujeito em uma busca e apreensão, eu não estou transformando esse diário em um diário público, ou mesmo em um diário estatal. Esse é um diário *privado*, que estará acessível ao Estado por motivos específicos e com um crivo de boas razões boas específico. Isso significa que ele não pode ser acessado por outros órgãos investigadores? Não, ele pode. Mas nessa lógica, é preciso que este acesso por outros órgãos seja igualmente vinculado a boas razões, e é por isso que, quando queremos ter acesso a um dado privado obtido em uma investigação de outro órgão, temos que ir ao juízo desse local e pedir *compartilhamento* de provas, apresentando a ele específicas razões, dizendo para ele por que eu quero esse compartilhamento. Essa é uma questão que precisamos ter bastante em mente.

A tese da reclamação que foi ajuizada nesse caso sobre as bases de dados das forças-tarefas, a meu ver, *desidrata* o direito à privacidade, porque, quando um órgão X faz parte de uma estrutura maior, e isso é usado pela chefia dessa estrutura maior para ter acesso a tudo aquilo que for acessado pelo órgão da ponta (digamos, de primeira instância), isso faz com que, no fundo, todo cidadão que for investigado no país terá seus dados expostos *em duas frentes*. Em uma primeira frente, ao investigador específico do caso em que fora investigado, porque apresentou razões, crivadas pelo Judiciário, com motivo específico e finalidade específica de seu uso. Mas

também em uma segunda frente, ao *chefe* da instituição, pura e simplesmente porque ele é... o chefe da instituição. Nesse contexto todo, acho que a gente tem que ter muito cuidado, porque o precedente que pode ser criado nessa tese da reclamação nº 42050 é, no fundo, a de que a chefia da instituição pode ter acesso a tudo que for obtido em qualquer investigação ao redor do Brasil - muito além, inclusive, dos dados obtidos pelas forças-tarefa da Lava Jato. É um poder informacional enorme, sem precedentes no país.

Essa crítica que faço faz com que não possamos pensar em conciliar privacidade e eficiência das investigações da PGR? De modo algum, acho que temos mil formas de conciliar as coisas. Uma coisa que às vezes é muito difícil no Ministério Público, por exemplo, é saber o que que outras pessoas investigaram, ou seja, se já foram obtidos, por exemplo, em algum lugar do país, dados bancários envolvendo a Mariana. E seria bom poder saber isso, porque evitaria que o mesmo dado seja pedido à instituição financeira pertinente mais de uma vez, atrasando seu acesso. Mas se é isso que se quer, você pode construir, digamos, um *data lake* que não me dê acesso ao dado bancário da Mariana, mas pura e simplesmente permita ver, digamos, os metadados sobre seu sigilo. Um data lake, por exemplo, que me permita fazer uma busca e ver que, ali em algum lugar do país, já foi feita uma investigação que abriu acesso a dados bancários da Mariana (sem que se saiba qual o conteúdo desse dado em si); assim, se eu quiser acessar dados bancários dela, eu vou primeiro no *data lake*, checo se existe alguma investigação em que isso foi obtido, em caso positivo descubro em qual processo foi, qual juízo autorizou, e me dirijo a ele, ofereço as minhas razões, e ele criva isso e verifica se é possível que eu obtenha o compartilhamento com o órgão que já detém o dado. Ou seja, é possível - esse é o meu ponto - pensar em estratégias de maximização de eficiência *que não impliquem*

absoluta desidratação do direito à privacidade. Você pode criar mecanismos que sejam eficientes, mas também controlados externa e internamente (por exemplo, mesmo o acesso ao *data lake* tem que ser condicionado a um login de acesso, tem que ser regrado,, tem que saber por que a pessoa está querendo investigar, ela tem que colocar o CPF dela, etc.). Não precisamos expor amplamente e indiscriminadamente o sigilo das pessoas, única exclusivamente com argumentos de eficiência, ou mesmo de unidade de determinada instituição estatal.

Enfim, claro que estou aberto ao debate, mas acho que precisamos olhar para essa afetação da privacidade em uma dimensão *intrainstitucional*. No Brasil, várias das decisões importantes sobre privacidade estão sendo tomadas em âmbitos que nos parecem briga corporativa, disputa política de poder interna a determinado órgão. Mas, às vezes, coisas muito graves para a privacidade de todo mundo e para o próprio desenho institucional sobre compartilhamento de provas, compartilhamento de informações entre órgãos, ficam fora do nosso radar por não percebermos que há coisas maiores em jogo ali. Nós até olhamos as disputas *entre instituições*, mas esquecemos que existem disputas travadas *dentro de instituições*, entre diferentes setores e que podem ser importantes e criarem precedentes muito perigosos para os direitos de todos nós. Então, acho que isso é uma coisa importante de se pensar.

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 GRÁFICA CINELÂNDIA EM 2022.