DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.5 >

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / REBECCA WEXLER / ANDRÉ NICOLITT / MARTA SAAD / MARIA THEREZA ASSIS MOURA / LAURA SCHERTEL MENDES / HELOISA ESTELLITA / LUIZ FERNANDO BUGIGA REBELLATO / RODRIGO MUDROVITSCH / ANAMARA OSÓRIO / LÚCIA HELENA SILVA DE BARROS DE OLIVEIRA / ISABEL SCHPREJER / FELIPE FREITAS / BIANCA KREMER / OWEN LARTER / CARLOS BRUNO FERREIRA / ELOÍSA MACHADO

INTERNETLAB
pesquisa em direito e tecnologia

SÃO PAULO, 2021

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

Citação sugerida
BRITO CRUZ, Francisco; SIMÃO, Bárbara(eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. V. São Paulo. InternetLab, 2022.

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 / Francisco Brito Cruz, Bárbara Simão [editores]. -- São Paulo: InternetLab, 2022. -- (Doutrina e prática em debate; v. 5)

Vários autores.
Bibliografia.
ISBN 978-65-88385-12-8

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

22-117999 **CDU-343.1:004**

Índices para catálogo sistemático:
1. Direito e tecnologia : Direito processual penal **343.1:004**
Cibele Maria Dias - Bibliotecária - CRB-8/9427

AUTORES /

< ANAMARA OSÓRIO >

Procuradora Regional da República em São Paulo. Procuradora-Chefe do Ministério Público Federal no Estado de São Paulo 2011-2015. Doutora e Mestre em Direito Internacional pela USP. MBA em Gestão Pública pela FGV/SP.

< ANDRÉ NICOLITT >

Doutor em Direito pela Universidade Católica Portuguesa – Lisboa. Professor da UFF e do Programa de Pós-Graduação Stricto Sensu em Direito da UniFG – Centro Universitário (UNIFG), Guanambi, Bahia Juiz de Direito do TJRJ. Presidente do Fórum Permanente de Direito e Relações Raciais da Escola da Magistratura do Estado do Rio de Janeiro.

< BIANCA KREMER >

Bianca Kremer é advogada, pesquisadora e consultora em Direito Digital. Doutora em Direito pela PUC Rio. Former Research Fellow na Leiden University (Holanda). Fellow na Coding Rights e Líder de Pesquisa no CJUS FGV Rio. Professora no Instituto Infnet, PUC Rio e Instituto New Law. Autora do livro Algoritmos, Vieses Raciais e o Direito pela Editora Lumen Juris (no prelo).

< CARLOS BRUNO FERREIRA >

Doutor em Direito Constitucional pela Universidad de Sevilla/Espanha (2013). Pesquisador-visitante (inverno/2009- verão/2010) no Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht-Heidelberg (Instituto Max-Planck de Direito Público comparado e Direito Internacional em Heidelberg). Mestre em Direito Constitucional e Teoria do Estado pela PUC/RJ (2005) e em Direito Constitucional pela Universidad de Sevilla (2008). Procurador da República/Secretário de Cooperação Internacional Adjunto da Procuradoria Geral da República (2014-) e Professor da Escola Superior do Ministério Público da União. Foi membro auxiliar da Corregedoria Nacional do CNMP (2013-2015). Tem experiência na área de Direito Internacional, Constitucional, Administrativo e Econômico/Consumidor com ênfase nos seguintes temas: Cooperação Jurídica Internacional, Direitos Fundamentais e Estado Democrático de Direito.

< 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.

< FELIPE FREITAS >

Doutor em Direito pela Universidade de Brasília (2015) com concentração na área de Direito, Estado e Constituição. Foi coordenador nacional do Plano de Prevenção à Violência contra Juventude Negra do Governo Federal (2012 – 2014) e Secretário Executivo do Conselho Nacional de Promoção da Igualdade Racial da Presidência da República (2015 – 2016) Atualmente é pesquisador do Núcleo de Justiça Racial da Fundação Getúlio Vargas de São Paulo e diretor da Plataforma Justa. É professor do corpo permanente do programa de pós graduação (mestrado e doutorado) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e professor colaborador do

Mestrado Profissional em Segurança Pública da Universidade Federal da Bahia (PROGESP UFBA).

< HELOISA ESTELLITA >

Consultora e parecerista na área do Direito Penal Econômico, atuando nas fases preventiva e contenciosa. Agraciada com a Humboldt Research Fellowship para realização de Pós-doutorado na Alemanha, na Ludwig-Maximilians-Universität de Munique e na Universidade de Augsburg (2015-2017), em cooperação com a CAPES. Doutora em Direito Penal pela Universidade de São Paulo (2004). Mestre em Direito (UNESP, 2001). Especialista em Direito Penal Econômico e Europeu (Universidade de Coimbra, 2001). Professora da Escola de Direito da Fundação Getulio Vargas e coordenadora do Grupo de Ensino e Pesquisa em Direito Penal Econômico na mesma instituição.

< ISABEL SCHPREJER >

Defensora Pública do Estado do Rio de Janeiro. Subcoordenadora de Defesa Criminal da Defensoria Pública do Estado do Rio de Janeiro. Membra suplente do Conselho Penitenciário do Estado do Rio de Janeiro. Membra suplente da Comissão Criminal Permanente do Conselho Nacional das Defensoras e Defensores Públicos-Gerais (Condege). Pós-graduada em Processo Penal e Garantias Fundamentais pela Academia Brasileira de Direito Constitucional (ABDConst).

< LAURA SCHERTEL MENDES >

É professora adjunta de Direito Civil da Universidade de Brasília (UnB) e do Instituto Brasiliense de Direito Público (IDP). É doutora summa cum laude em direito privado pela Universidade Humboldt de Berlim, tendo publicado sua tese sobre proteção de dados na Alemanha. É mestre em "Direito, Estado e Constituição" pela UnB e graduada em direito pela UnB. É diretora da Associação Luso-Alemã de Juristas (DLJV-Berlim) e do Instituto Brasileiro de Política e Direito do Consumidor (Brasilcon). Tem experiência nas áreas de direito civil, direito do consumidor e direito constitucional, atuando principalmente nos seguintes temas: direitos da personalidade, privacidade e proteção de dados pessoais, direito e internet, interface entre direito constitucional e direito civil, bem como políticas públicas na Sociedade da Informação. É autora dos livros "Privacidade, Proteção de Dados e Defesa do Consumidor" (Saraiva, 2014) e Schutz gegen Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung: Eine Analyse der Rechtmäßigkeit der Datenverarbeitung im Privatrecht (A proteção de dados pessoais no setor privado: riscos do tratamento de dados e a garantia de um consentimento substancial), De Gruyter, 2015. Co-chair da sessão de Inteligência Artificial e Ética do BRAGFOST (2020), realizado por CAPES e Alexander von Humboldt Stiftung.

< LÚCIA HELENA SILVA DE BARROS DE OLIVEIRA >

Defensora Pública, desde 1997, estando atualmente exercendo o Cargo de Coordenadora de Defesa Criminal da Defensoria Pública do Estado do Rio de Janeiro, sendo também, Coordenadora de Política Criminal da Associação Nacional das Defensoras e Defensores Públicos. Mestre em Direito. Professora de Direito Penal da Fundação Escola da Defensoria Pública. Membro do Fórum Permanente de Penal e Processo Penal da Escola da Magistratura do Rio de Janeiro.

< LUIZ FERNANDO REBELLATO >

Graduado em Direito pela Pontifícia Universidade Católica (PUC-SP). Mestre em Direito Processual Penal pela Universidade de São Paulo (USP). Promotor de Justiça do Ministério Público do Estado de São Paulo. Autor de livros e palestrante.

< MARIA THEREZA ASSIS MOURA >

Ministra do Superior Tribunal de Justiça; Corregedora Nacional de Justiça, Mestre e doutora em Direito Processual Penal pela USP e professora doutora de Direito Processual Penal da Faculdade de Direito da USP.

< MARTA SAAD >

Professora Doutora de Direito Processual Penal da Faculdade de Direito da Universidade de São Paulo. Doutora (2007) e Mestre (2002) em Direito Processual Penal pela Faculdade de Direito da Universidade de São Paulo. Advogada-sócia responsável pela área de penal empresarial de Veirano Advogados. Graduada em Direito pela Faculdade de Direito da Universidade de São Paulo. Ex-Presidente e ex-conselheira do Instituto Brasileiro de Ciências Criminais (IBCCRIM). Advogada.

< OWEN LARTER >

Owen é Diretor de Políticas Públicas no departamento responsável pela I.A. da Microsoft, onde trabalha para ajudar a moldar as estruturas regulatórias que podem garantir que os benefícios da IA possam ser realizados com responsabilidade. Owen trabalhou anteriormente no Reino Unido e nas equipes de Assuntos Governamentais Globais da Microsoft e, antes de ingressar na Microsoft, trabalhou para um MP do Reino Unido. Ele é cofundador da Aspen NextGen Network, membro do Conselho de Relações Exteriores e membro do Conselho da Compass Housing Alliance.

< REBECCA WEXLER >

Professora de direito na University of California, Berkeley, School of Law, onde leciona, pesquisa e escreve sobre questões relativas a dados, tecnologia e justiça criminal. Seu trabalho tem ênfase em direito probatório, processo penal e questões de proteção à privacidade e propriedade intelectual em torno de novas tecnologias de justiça criminal baseadas em dados. também é co-diretora docente do Berkeley Center for Law & Technology.

< RODRIGO MUDROVISTCH >

Sócio-fundador do escritório Mudrovitsch Advogados. Doutor em Direito Constitucional pelo Departamento de Direito do Estado da USP. Mestre em Direito, Estado e Constituição pela UnB. Professor do IDP. Presidente da Comissão Estudos de Direito Penal da OAB Federal. Procurador Nacional da Procuradoria Nacional de Defesa dos Direitos Humanos da OAB - Gestão 2019/2022; Membro Consultor da Comissão Nacional de Direitos Humanos da OAB - Gestão 2019/2022; Secretário- Geral da Comissão de Juristas da Câmara dos Deputados responsável pela elaboração de Anteprojeto sobre o processo constitucional brasileiro; e membro das comissões Estudos Constitucionais e de Defesa da República e da Democracia da OAB.

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 quinta edição do Congresso, que ocorreu online entre os dias 30 de agosto e 03 de setembro de 2021, teve como mote a proteção de dados pessoais no âmbito da justiça criminal, abordando os desafios diante do desenvolvimento e absorção de novas tecnologias na prevenção, repressão e processamento de delitos.

As contribuições aqui compiladas abordam o debate constitucional sobre a privacidade e a proteção de dados, o papel do Conselho Nacional de Justiça no cenário regulatório da proteção de dados para fins de segurança pública, o impacto de sistemas de vigilância em massa e de técnicas de *big data* sobre investigações, aspectos relacionados ao compartilhamento de dados de crimes financeiros e o acesso a dados de pessoas indeterminadas em investigações criminais. Neste ano, também contamos com seção especial com contribuições ao painel de teses sobre reconhecimento pessoal e facial - no qual chamamos especialistas para que colocassem seus respectivos argumentos em debate. O painel de teses contou com a curadoria e moderação de Pablo Nunes, coordenador do Centro de Estudos de Segurança e Cidadania (CESEC).

Todas as contribuições do Congresso 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 2022.

01.

ASSIMETRIAS DE PRIVACIDADE[1]

Rebecca Wexler

1. Texto baseado na transcrição da palestra apresentada por Rebecca Wexler como oradora principal no V Congresso sobre Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab a 09/03/2021. A transcrição foi revista pela autora.

Estou muito feliz por estar aqui. Obrigada ao InternetLab por me convidar, Marta, Francisco e Bárbara. E que agenda emocionante que vocês planejaram. Sinto-me tremendamente honrada por estar aqui.

Quero começar a conversa de hoje com uma história. Esta é uma história sobre uma pessoa real. Um amigo meu de Nova York, que é defensor público na Legal Aid Society.[2] É uma história sobre seu cliente. Com base em provas trazidas por uma testemunha reclamante, a polícia de Nova York prendeu e encarcerou um homem por violar uma medida cautelar do Juízo de Família.

2. N/E: Em tradução livre, Sociedade de Assistência Jurídica.

As provas que a testemunha trouxe eram imagens de mensagens de texto e telefonemas contendo assédio, e um ameaçador correio de voz - o qual ela alegou que este homem havia enviado a ela em violação a uma medida protetiva. Agora, nem a polícia nem o promotor questionaram se essas provas eram autênticas. E, sendo assim, você tem uma pessoa encarcerada em pré-julgamento. Ele poderia muito bem ter se declarado culpado apenas para poder ir para casa, ou poderia ter sido condenado no julgamento. Mas, ao invés disso, este homem protestou, insistiu que ele era inocente. Meu amigo Jerome Greco, seu advogado de defesa, acreditou nele.

Jerome, então, enviou uma intimação por capricho, na verdade, sem nem mesmo saber para que empresa enviá-la, mas por sorte a enviou a uma empresa chamada Spoof Card - que oferece um serviço que permite às pessoas enviar mensagens de texto e mensagens de voz que parecem vir do número de telefone de outra pessoa. Aqui está uma demonstração de como o "Spoofing" funciona.

[vídeo começa]

Vou escolher um número. Portanto, vamos fazer aparecer como (310) 555-2799. Na verdade, quer saber, vamos fazer algo mais louco, ou vamos fazer 555-1000 porque isso é tipo... tipo...você sabe. E depois vamos colocar aqui meu número, que é ***[censurado]****. Acho que vou censurar essa parte. OK, então você tem aqui: o número que vamos fazer aparecer no meu identificador de chamadas e depois você tem o meu número de telefone que está ligando. E aqui está o meu telefone. Vamos ver o que acontece quando você pressiona a chamada. E eu disse aquele número de telefone que escolhi, eu nunca lhe disse aquele número, certo? E meu telefone está tocando com o número exato que eu acabei de escolher. (310) 555-1000. É muito fácil. E é isso aí.* **[vídeo acaba]**

Neste caso, a empresa Spoof Card respondeu assim à intimação. Este é o documento redigido que eles forneceram:

ACCOUNT

FIRST NAME	LAST NAME	EMAIL ADDRESS	DOLLAR BALANCE	IS ACTIVE	MEMBER SINCE
////////	////////	//////////	16.4894894	YES	////////

CREDENTIALS

CREDENTIAL TYPE	IDENTIFIER	IS ACTIVE	DATE CREATED
//////////	////////		////////

ACCESS TOKENS

PROVIDER TYPE	APPLICATION NAME	IP ADDRESS	DATE CREATED

CALLS

ACCESS NO.	REAL CALLER ID	SPOOF NUMBER	RECORDING	START TIME	VOICE CHANGER
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////	YES	//////////	//////////
+148497//	+15///////////	+151689////	YES	//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////	YES	//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////
+148497//	+15///////////	+151689////	YES	//////////	//////////
+148497//	+15///////////	+151689////		//////////	//////////

Acontece que foi, de fato, a informação do assinante da suposta vítima, neste caso, a testemunha reclamante. E mostrou que ela tinha usado o serviço Spoof Card para enviar o correio de voz e mensagens de texto para ela mesma. Você também pode ver que ela usou um sistema de troca de voz - *voice-changer-man* - para disfarçar sua própria voz, para soar como um homem.

Agora, quando o advogado de defesa, Sr. Greco mostrou estes registros ao promotor, o promotor retirou as acusações e o homem foi libertado da prisão. Mas este caso mostra porque, em uma escala muito maior, as investigações da defesa criminal são importantes. As provas aqui só foram expostas porque o advogado de defesa pôde intimar uma empresa de tecnologia para os registros gerados por alguém que não estava na conta de seu próprio cliente.

O governo não tinha esta informação, e eles não iriam obtê-la porque confiaram na vítima - alegada vítima. Intimar diretamente aquele indivíduo - a alegada vítima - seria uma falha quase certa, porque ela estava tentando falsificar os documentos. E assim, aqui você tem a investigação da defesa como o único meio de expor a inocência.

Infelizmente, existe um padrão nas leis de privacidade que bloqueou precisamente este tipo de intimação de defesa. Elas barraram o advogado de defesa de intimar empresas de tecnologia para categorias inteiras de informações sensíveis. E, ao mesmo tempo, elas se inclinam muito a favor da força policial, porque muitas leis relacionadas ao acesso a dados contêm exceções expressas que permitem que o poder de polícia continue acessando informações sensíveis.

Eu chamo este padrão de "Assimetrias de Privacidade", leis de privacidade que permitem aos tribunais ordenar processos legais quando solicitados pelo governo, mas não quando solicitados por advogados de defesa criminal. Em um sistema jurídico adversarial ou em um sistema onde dependemos de um advogado de defesa para investigar a inocência, o que é verdade nos Estados Unidos - e, como eu estava aprendendo ao me preparar para esta palestra, em grande medida, também no Brasil - isto significa que suprimir as investigações de defesa significa suprimir seletivamente as provas de inocência.

Quando pensamos em novas tecnologias e dados em processos criminais, muitas vezes pensamos em investigações de autoridades legais. Pensamos em instrumentos de avaliação de risco, reconhecimento facial, ferramentas preditivas de policiamento, acesso das autoridades policiais a essas amplas faixas de exaustão digital que estão produzindo [dados] o tempo todo sobre tudo o que fazemos, nossos calendários do Google, nossos dados Fitbit, tecnologias vestíveis, nosso conteúdo de e-mail, nossas mensagens de Instagram, tudo. E os defensores da privacidade e os ativistas da sociedade civil estão justamente preocupados com a facilidade de acesso a essas informações por parte das autoridades policiais.

Enquanto isso, as autoridades legais estão preocupados em se manter escondidos; em poder acessar dados antes de serem apagados ou criptografados; em poder acessar dados além fronteiras em investigações criminais transnacionais, agora que temos novas leis de localização de dados, privacidade e proteção de dados em todo o mundo, inclusive no Brasil. Mas, surpreendentemente, nenhuma destas conversas envolve realmente uma consideração significativa das investigações de defesa criminal. Como as novas tecnologias, novas fontes de provas digitais afetam a capacidade do advogado de defesa em investigar e provar a inocência?

Agora, as assimetrias de privacidade na verdade vêm em dois tipos, e eu quero dar um pouco desse pano de fundo para que vocês possam começar a ter uma noção de como elas podem aparecer no Brasil ou em outros dispositivos legais ao redor do mundo. Elas vêm em "assimetrias de acesso" e elas vêm em "assimetrias de notificação". As assimetrias de acesso são leis que barram o

advogado de defesa de acessar uma categoria de informação ou uma fonte de informação, mas permitem que as autoridades de investigação façam exatamente isso. E assimetrias de notificação são leis que impedem que o advogado de defesa acesse a informação confidencialmente, seja retardando a notificação a um alvo ou impondo a não divulgação ou uma ordem judicial de sigilo a um intermediário para impedir que ele informe o alvo da investigação.

Você pode estar pensando: "Oh, estou muito preocupado com isto. Aonde a professora Wexler está nos levando? Aonde Rebecca quer chegar com isto? Nós não gostamos muito disto. Queremos ser avisados". OK, bem, a notificação é muito importante. É verdade. E ainda assim, em alguns momentos, com suficiente supervisão judicial, permitimos que as autoridades policiais atrasem, adiem ou não façam notificações. Permitimos isso porque há circunstâncias em que notificar um alvo [de investigação] poderia arriscar a segurança ou a proteção da vida de alguém, poderia arriscar a adulteração ou intimidação de testemunhas, poderia arriscar a destruição de provas, adulterando as provas. E assim, a qualquer momento que você tenha esse tipo de necessidade para as autoridades policiais, você pode pensar que o advogado de defesa está investigando este mesmo tipo de pessoas. Na verdade, os mesmos tipos de fatos, exatamente os mesmos supostos crimes. Portanto, às vezes eles também podem precisar dessas coisas com suficiente supervisão judicial.

Por que as investigações de defesa criminal são tão importantes? Bem, nos Estados Unidos, os promotores e juízes não têm o dever constitucional ou ético de investigar provas de inocência. Sim, há algumas exceções ao redor dos limites, ou seja, se a equipe de acusação sabe que está no controle de provas absolutórias, eles devem encontrá-las e entregá-las à defesa; se alguém disser a um promotor que ele condenou alguém injustamente após o fato, então há um dever ético de ir procurar essa informação; se eles dependem de um informante confidencial, talvez eles tenham que fazer alguma investigação sobre a confiabilidade do fato. Mas, além desses tipos limitados de exceções, não há o dever de investigar ativamente um terceiro que possa ter cometido o crime ou que possa possuir provas de inocência, material de absolvição, que possa ser favorável à defesa. Nada.

Meu entendimento, novamente, é apenas preliminar sobre o Brasil, e entendo que há vários advogados de defesa criminal brasileiros que são oradores nesta conferência. Mas meu entendimento é que o Brasil também tem uma mistura, uma fundação em um sistema inquisitorial que tem elementos de sistema adversarial acrescentados pela Constituição de 1988 e pelo Código de Processo Penal que habilitam a defesa - até certo ponto - a investigar e apresentar provas de inocência. Porém, em qualquer medida em que o procedimento criminal brasileiro se apoie nos advogados de defesa para comprovar a inocência, essas assimetrias de privacidade podem impedir essa função.

Quais são alguns exemplos delas? Bem, deixe-me dar-lhe um exemplo central dos EUA. Este é o *Stored Communications Act*,[3] uma lei federal de privacidade na Internet de 1986 que se destina a proteger a privacidade do conteúdo de comunicações como e-mails, mensagens privadas ou postagens no Facebook, ou o que quer que você tenha enviado através de provedores de serviços através de intermediários terceiros:

3. N/E: Em tradução livre, a "Lei de Comunicações Armazenadas".

THE U.S. STORED COMMUNICATIONS ACT,
18 USC § 2702

(A)(1) A PERSON OR ENTITY PROVIDING AN ELECTRONIC COMMUNICATION SERVICE TO THE PUBLIC SHALL NOT KNOWINGLY DIVULGUE TO ANY PERSON OR ENTITY THE CONTENTS OF A COMMUNICATION...

[EXCEPT TO A "GOVERNAMENTAL ENTITY" PURSUANT TO CERTAIN FORMS OF LEGAL PROCESS]

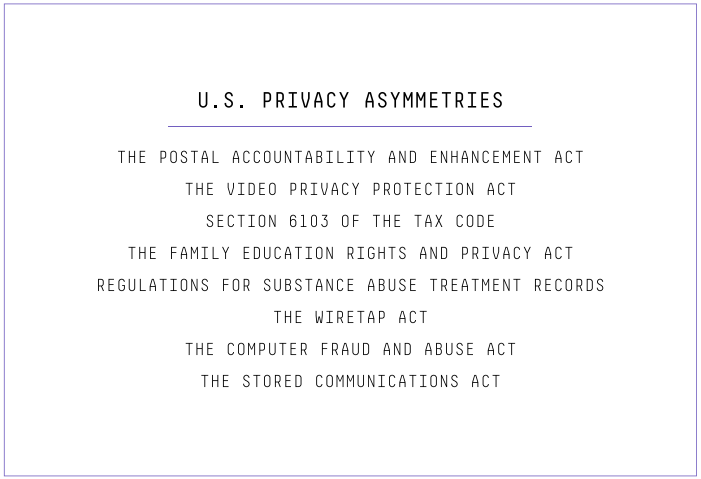
Esta lei começa com uma regra de confidencialidade muito ampla. Ela impõe à empresa de tecnologia, a um prestador de serviços, esta regra de "não divulgar intencionalmente a qualquer pessoa o conteúdo das comunicações que são armazenadas pela empresa". E então a lei enumera uma série de exceções expressas. E eu acabo de colocar aqui, há uma para entidades governamentais, de acordo com certas formas de supervisão judicial.

Na verdade, há muitas outras exceções também. Há exceções para o consentimento do remetente ou destinatário de uma mensagem. Há exceções para o uso comercial da própria empresa de tecnologia. E ainda há silêncio quanto a investigações de defesa criminal no texto da lei. E, com base nesse silêncio, por mais de uma década, todas as principais empresas de tecnologia dos Estados Unidos e o Ministério da Justiça[4] têm argumentado que esta lei proíbe categoricamente que os advogados de defesa criminal solicitem às empresas de tecnologia o conteúdo das comunicações eletrônicas de outra pessoa. E eles acham que esta lei proíbe categoricamente essas intimações, independentemente da necessidade, independentemente do quanto precisamos dessa informação para absolver alguém que é injustamente acusado de um crime.

4. N/E: Em inglês, o *Department of Justice*.

Acontece que eles geralmente vencem nos tribunais dos Estados Unidos. Dos tribunais que decidiram sobre a questão, conheço um tribunal que discordou deles, e aqui está um trecho de sua opinião. Esta é uma ação de desacato ao Facebook e ao Twitter por se recusarem a fornecer provas de impedimento de uma testemunha de acusação em um caso em que dois jovens enfrentavam sentenças de prisão perpétua. Assim, o juiz diz: "O Facebook e o Twitter estão usando indevidamente seus imensos recursos para manipular o sistema judicial e privar esses dois jovens hipossuficientes que enfrentam sentenças de prisão perpétua de seu direito de se defenderem em julgamento". No entanto, além desta opinião do tribunal, a maioria dos tribunais concordou com as empresas de tecnologia e com o Ministério da Justiça.

Agora, o *Stored Communications Act* não está sozinho. Aqui está uma lista de outras assimetrias de privacidade nas leis dos Estados Unidos:



[O documento diz: "Assimetrias de Privacidade nos EUA; Lei de Melhoria e Responsabilidade dos Correios; A Lei de Proteção da Privacidade em Vídeos; Seção 6103 do Código Tributário; A Lei de Direitos Educacionais e Privacidade da Família; Regulamento para Registros de Tratamento de Abuso de Substâncias; A Lei Grampeamento de Comunicações; A Lei de Fraude e Abuso de Computadores; A Lei de Comunicações Armazenadas]

Você verá muitos deles aqui. Uma coisa interessante sobre isso é que estes dispositivos legais, as assimetrias embutidas, parecem ser acidentes. Eles são baseados no silêncio textual da lei, silêncio na história legislativa. E eles são distribuídos aleatoriamente com outros dispositivos de privacidade que são realmente simétricos.

Portanto, voltando a este slide, esses dispositivos que são assimétricos, que têm assimetrias de privacidade. Mas outros dispositivos, como a Lei HIPAA[5] para dados de saúde, são na verdade simétricos. Qualquer pessoa com processo judicial e supervisão suficientes pode intimar um prestador de serviços médicos para esses registros muito sensíveis, mesmo que não sejam seus próprios registros. E assim, com base na distribuição aleatória do silêncio textual, do silêncio legislativo histórico, há uma história que podemos contar sobre como essas coisas podem acontecer como acidentes. Parece que eles proliferam devido à supervisão, não à razão.

5. N/E: A Health Insurance Portability and Accountability Law (em português, Lei de Portabilidade e Prestação de Contas do Seguro de Saúde).

A história é a seguinte. Há legisladores bem intencionados e que querem proteger a privacidade do consumidor, e eles consideram aprovar legislação de privacidade. Enquanto isso, as autoridades têm uma capacidade de *lobby*, e eles vão até o legislador e pedem uma exceção a essa lei. Talvez o legislador pense: "Oh, eu vou dar esta exceção agora, eu vou trocá-la por algo. Mais tarde, eu terei outro Código de Processo Penal que regulará o acesso da justiça separadamente". Mesmo que isso funcione, ninguém ou muito poucas pessoas estão alertando os legisladores para as necessidades dos investigadores da defesa criminal.

Agora novamente, por favor, me dêem paciência por minha ignorância como novata no direito brasileiro, mas tenho esta maravilhosa assistente de pesquisa Alexa Dougherty, que estava me ajudando a me preparar para esta palestra. E ela encontrou algumas leis brasileiras onde ela acha que vocês também podem ter assimetrias de privacidade embutidas em suas leis nacionais. Eu adoraria ouvir de vocês se acham que estas são estas assimetrias de privacidade com as quais vocês devem se preocupar. Mas obrigada à Alexa por encontrar es-

/ MUITOS DESTES DISPOSITIVOS DE PRIVACIDADE CONTÊM EXCEÇÕES EXPRESSAS QUE PERMITEM QUE O PODER DE POLÍCIA CONTINUE ACESSANDO INFORMAÇÕES SENSÍVEIS /

sas possíveis leis brasileiras onde isso também pode ser um problema para vocês.

Então, o que devemos fazer a respeito disso? Bem, eu tenho duas propostas no plano doméstico e depois vou expandir para fluxos de dados transfronteiriços. No plano doméstico, já temos uma lei de privacidade como o *Stored Communications Act* que tem uma exceção expressiva para investigações de autoridades legais, mas faz silêncio em relação à defesa. Acho que os tribunais deveriam tratar isso como uma questão de sigilo profissional. Assim, quando os tribunais constroem qualquer lei para bloquear um processo judicial, uma intimação judicial, o que estão fazendo é criar um sigilo probatório como o sigilo advogado-cliente, o sigilo de comunicação entre cônjuges. Eles estão criando um direito especial para que alguém não forneça provas em resposta a um processo legal de outra forma válido. E, pelo menos nos Estados Unidos, a Suprema Corte diz que os sigilos são realmente um negócio arriscado. Estes são uma derrogação à busca da verdade. Portanto, precisamos interpretá-los de forma muito restrita. Precisamos de uma construção rigorosa ou de uma regra clara.

Os tribunais não devem manter um silêncio ambíguo sobre uma lei com a criação de um sigilo probatório. Se os legisladores quiserem bloquear intimações de defesa criminal ou criar um privilégio que possa bloquear intimações judiciais solicitadas pelos réus, eles devem dizer isso expressamente no texto legal.

A outra solução é para os legisladores. Quando os legisladores estão aprovando essas leis, eles deveriam estar pensando para si mesmos "hmm, se a aplicação da lei está pedindo uma exceção investigativa, talvez o advogado de defesa também precise disso". E se eles estiverem preocupados com isso, podem acrescentar algo como uma disposição modelo ao final da lei que diz que ela não deve proibir uma resposta de boa-fé ao cumprimento de intimações válidas de outra forma, e isto cuidará do problema. Portanto, esta é uma ideia para o que os tribunais e os legisladores poderiam fazer nos EUA, e se vocês acham que os exemplos de assimetrias de privacidade na legislação brasileira são semelhantes, também o que os tribunais e legisladores poderiam estar fazendo no Brasil.

Mas agora, o que acontece quando as investigações se tornam globais? Neste momento, temos uma situação em que estamos todos conectados na Internet e os dados armazenados em uma jurisdição podem ser relevantes para uma investigação criminal em outra jurisdição. Talvez você represente um réu nos Estados Unidos ou no Brasil, mas esteja tentando acessar dados em um servidor estrangeiro. Poderia ser a conta de e-mail de um co-conspirador. Poderia ser alguém que obrigou seus clientes a cometerem crimes sob coação. Talvez sejam provas totalmente absolutórias que poderiam provar um álibi. Informações que poderiam ser causas de impedimento de uma conta financeira de uma testemunha governamental localizada no exterior. Como você pode ter acesso a essas informações?

Bem, antes de meados do século 20, todos estavam 'na mesma' para ter acesso a dados ou provas armazenadas além das fronteiras. Costumávamos chamar isso de "cartas rogatórias", o que é basicamente um processo discricionário. Você iria ao seu tribunal doméstico, e perguntaria "por favorzinho, você pode pedir a outro tribunal na jurisdição estrangeira para fazer homologar minha intimação ali"? E como uma questão de respeito entre as jurisdições, os tribunais podem dizer: "OK, OK, então aqui estão as cartas rogatórias". Mas em meados do século 20, os litigantes civis estavam dizendo "isto é muito, muito lento. Isso pode levar anos. Não é bom o suficiente. Eu quero uma opção melhor". E eles conseguiram a Convenção de Haia.

A Convenção de Haia sobre Provas.[6] Adivinhe o que? Acontece que não está disponível para réus criminais, apenas para casos civis. Tudo bem. Isso não é uma opção. Bem, nos anos 80 os EUA, dou melhor, o governo dos EUA começa a dizer: "precisamos de um processo melhor para a obtenção de dados através das fronteiras. Vamos negociar alguns tratados". E, finalmente, tratados de assistência jurídica mútua. E os três primeiros que negociam: Suíça, Turquia e Holanda, todos eles são simétricos. Assim, alguns tribunais diziam que "os investigadores de defesa criminal podem usar esses também".

6. N/E: A Hague Evidence Convention (em português, Convenção de Haia sobre Provas).

Assim que isso aconteceu, o governo dos Estados Unidos começou a negociar tratados que dizem expressamente que isso é somente para autoridades legais e não para a defesa criminal. Então, aqui está a linguagem do Tratado MLAT Brasil-Estados Unidos: "as disposições deste tratado não darão origem a qualquer direito não existente de outra forma por parte de qualquer pessoa privada, de obter provas localizadas no exterior". Isso significa o advogado de defesa nos Estados Unidos. Tratamos o advogado de defesa como uma pessoa privada, não como uma entidade do governo. E assim, apesar das repetidas críticas no Senado e nos tribunais, os MLATs assimétricos permitem que as autoridades policiais, mas não os réus criminosos, obtenham divulgações de dados transfronteiriços, eles proliferaram e foram mantidos.

OK, agora fica pior, e fica pior por causa dos dados. A ascensão de uma economia global de dados está piorando por duas razões: primeiro, evidências mais relevantes podem ser digitais e podem ser armazenadas no exterior. Agora não estamos mais falando apenas de casos criminais globais, tráfico de terrorismo, crime corporativo global. Estamos falando também de casos de crimes domésticos comuns. Você pode ter um arrombamento doméstico onde alguns supostos co-conspiradores estão em uma jurisdição diferente. Você pode ter dados que são sobre condutas em uma jurisdição que está armazenada no exterior.

E a segunda razão pela qual as assimetrias do MLAT estão piorando é devido às leis de privacidade, proteção e localização de dados que os países estão promulgando em resposta a preocupações válidas sobre a erosão da privacidade e da soberania. Portanto, considere o GDPR da Europa. O GDPR restringe qualquer transferência de dados obtida legalmente pelos EUA, a menos que essas transferências sejam feitas de acordo com um MLAT ou um tratado internacional. Eles não gostam que as autoridades legais dos EUA deem a volta em torno desses tratados. OK. Mas não está claro se o GDPR permite transferências fora desse esquema, ou pelo menos ele potencialmente torna estas transferências muito difíceis e custosas. E isso arrisca deixar o advogado de defesa e suas cartas rogatórias de fora, ao frio.

No Brasil, você tem a lei de proteção de dados, LGPD. E a LGPD exige uma decisão de adequação para transferir livremente os dados para outros países. Em caso de falta de adequação, ela possui outros instrumentos particulares que são necessários. Portanto, a Art. 33 diz que a transferência internacional é OK sem uma decisão de adequação se for necessária para a cooperação entre a inteligência pública, os órgãos de investigação e de acusação, de acordo com os instrumentos do direito internacional. Hmm. As cartas rogatórias contam? O investigador de defesa é um órgão de acusação, para os fins desta disposição? Não tenho certeza de que haja aqui alguma ambiguidade. Vejo que há disposições que também exigem que a autoridade nacional no Brasil emita pareceres técnicos ou recomendações que possam esclarecer essas exceções. E assim talvez a Autoridade Nacional (a ANPD) possa esclarecer

se esta exceção também se aplica a investigações e atividades de defesa criminal.

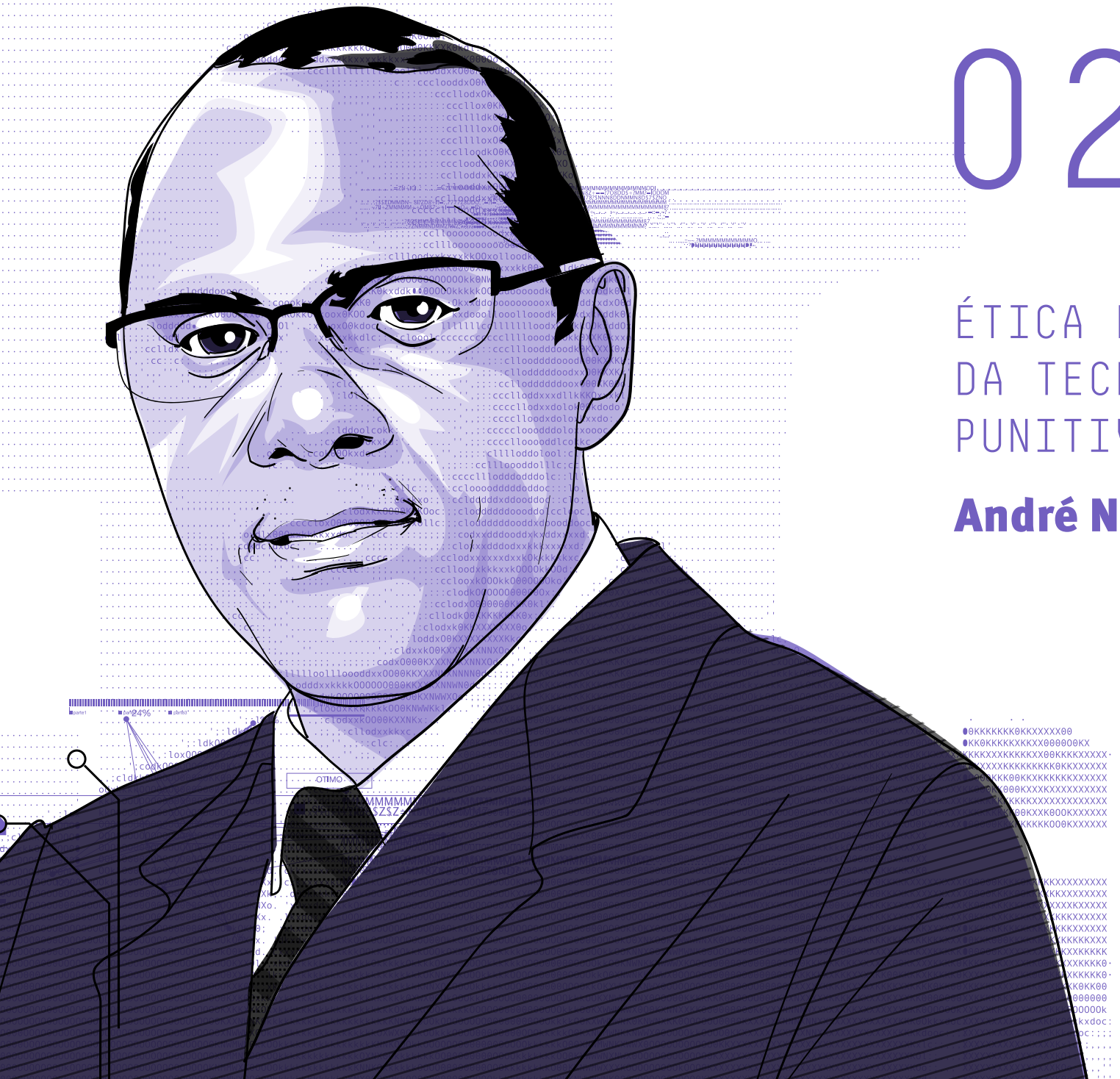
OK, então o que devemos fazer além desse esclarecimento? Bem, eu tenho outro pensamento possível que você pode achar controverso, então eu imagino que eu apenas o compartilharia com vocês e estou ansiosa para ouvir seus pensamentos. Mas outra coisa que está acontecendo nos Estados Unidos é que as autoridades legais decidiram que o processo do MLAT também é muito lento para isso. Ainda assim, não é bom o suficiente. Certo? É muito mais do que [é permitido à] defesa criminal, mas ainda não é bom o suficiente. E assim eles aprovaram o Cloud Act de 2018.

O Cloud Act de 2018 faz duas coisas. Uma *é* permitir que os EUA *negociem* uma série de outros acordos bilaterais com outras nações. O único até agora em vigor é com o Reino Unido, e adivinhe o que? É assimétrica, ela prevê o acesso às autoridades, mas não para a defesa. Mas outra coisa que o Cloud Act faz internamente nos EUA é dizer que as empresas *americanas* ou empresas sujeitas à jurisdição dos EUA devem fornecer dados em resposta às ordens judiciais, mesmo que esses dados sejam armazenados em servidores estrangeiros.

Agora, tecnicamente, [o *Cloud Act*] está fazendo aquele argumento sobre o *Stored Communications Act*, a lei com a qual comecei. E assim você pode interpretá-lo para permitir que a aplicação da lei apenas faça isso obrigando as empresas americanas a divulgar dados armazenados em servidores estrangeiros, mesmo que isso violasse a lei estrangeira. Mas acho que outro efeito dessa lei é que na verdade se trata de um debate que os EUA estava tendo em torno desses pedidos às empresas de tecnologia serm como uma busca e apreensão, que recruta a empresa de tecnologia para realizar uma busca como um agente do governo, ou se são como uma intimação, que permite ou que exige que o destinatário forneça documentos que respondam à ordem judicial.

Mas essa não é realmente uma busca protegida por proteções constitucionais da mesma forma que uma invasão em sua casa seria. E assim, ao descer e dizer que estas são realmente como intimações, o Cloud Act de 2018 diz *"não. Eu acho que quando o governo requer esses dados de uma empresa norte-americana, isto é como uma intimação"*. Bem, adivinhe? O advogado de defesa criminal também pode emitir intimações. Portanto, acho que este estatuto deve significar que os investigadores da defesa criminal nos EUA também podem exigir que empresas americanas ou empresas sujeitas à jurisdição dos EUA divulguem dados armazenados em servidores estrangeiros.

Com isso, vou apenas dizer obrigada.



02.

ÉTICA E ESTÉTICA DA TECNOLOGIA PUNITIVISTA[1]

André Nicolitt

1. Texto que tem por base a transcrição da palestra apresentada por André Nicollit na Sessão de Abertura e lançamento da Obra "Direitos Fundamentais e Processo Penal na Era Digital/Doutrina e Prática/ Vol. 5" no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em 30/08/2021. A transcrição foi revisada pelo autor.

Boa noite a todas e a todos. É uma alegria estar aqui mais uma vez participando deste importante encontro e atividade de reflexão sobre esse tema promovido pela InternetLab. Lamentavelmente não presencial. Estamos chegando numa fase de muitas carências de afeto, de abraços. Mesmo quando nos colocamos presencialmente em algum lugar, exige sempre um distanciamento. Agora, um "soquinho", uma coisa estranha para nós todos que estávamos acostumados a abraçar, apertar as mãos. Enfim, mas é o que temos para hoje e é o que precisamos ter para que possamos sobreviver. Então, é uma alegria estar aqui e para discutir um tema importante como essa questão da proteção de dados do processo penal. Enfim, vou tentar fazer uma reflexão sobre isso.

Eu queria, antes de propriamente enfrentar algumas questões de ordem mais pragmática, trazer uma questão, uma reflexão, uma ordem mais filosófica, digamos, e atravessada pela literatura. E pela literatura nada mais nada menos do que de Machado de Assis. Talvez o maior pensador e a maior referência negra que nós temos em nosso Brasil. Enfim, ele tem um conto fantástico intitulado "Pai Contra Mãe", que é um conto que eu sempre penso quando eu vou trabalhar a questão do poder e a questão das tecnologias. Diz o Machado de Assis, logo na introdução, nas primeiras, nos primeiros parágrafos desse conto:

> "A escravidão levou consigo ofícios e aparelhos, como terá sucedido a outras instituições sociais. Não cito alguns aparelhos senão por se ligarem a certo ofício. Um deles era o ferro ao pescoço, outro o ferro ao pé. Havia também a máscara de folha de flandres. A máscara fazia perder o vício da embriaguez aos escravos, por lhes tapar a boca. Tinha só três buracos, dous para ver, um para respirar, e era fechada atrás da cabeça por um cadeado. Com o vício de beber, perdiam a tentação de furtar, porque geralmente era dos vinténs do Senhor que eles tiravam com que matar a sede, e aí ficavam dois pecados distintos e a sobriedade e a honestidade certas. Era grotesca tal máscara, mas a ordem social e humana nem sempre se alcança sem o grotesco, e algumas vezes o cruel. Os funileiros as tinham penduradas, à venda, na porta das lojas. Mas não cuidemos de máscaras".

Esse conto, então, fala dos equipamentos tecnológicos que serviam à escravidão. Aquilo que servia ao regime escravocrata. Então, para o controle dos negros, destacadamente os fugitivos, ou aqueles escravizados que fugiam, ou que resistiam, ou que bebiam ou que furtavam, você tinha uma série de aparatos, como a máscara, a bola ao ferro, etc.

E, quando nós pensamos nessas tecnologias, nós temos que pensar numa perspectiva estética e numa perspectiva ética. Por que falamos isso? Porque, do ponto de vista das relações sociais que nós vivenciamos, o que nós deixamos para trás, o que se têm, não raro são mudanças estéticas, mas com uma perpetuação de uma ética autoritária e desumanizada, que, no caso da experiência brasileira, sempre foi atravessada e marcada ou estruturada a partir do racismo.

Todos sabemos que o sistema penal nasce, na obra "Cárcere e Fábrica", como um equipamento, como uma tecnologia destinada a assegurar os interesses do capitalismo, do poder econômico. É exatamente com o afloramento do capitalismo que surgem as prisões, etc. Quando nós pensamos na ideia de raça e de racismo, a raça é um termo que não existia antes do século XVI. Ela surge como uma forma, um mecanismo, uma tecnologia de distinguir pessoas, diferenciar pessoas com o objetivo de possibilitar domínios sobre pessoas e territórios. Então ela nasce marcadamente na expansão marítimo co-

mercial. Tudo isso são tecnologias voltadas para a opressão e exploração das pessoas e de territórios com o fim de proteger certos interesses econômicos. Então, o sistema penal surge muito voltado e ligado a essa questão.

E, no Brasil, ganha uma vocação um pouco mais forte com isso, porque, na verdade, o sistema penal é precipuamente cunhado a partir do Código Penal de 1830 e da Constituição de 1824 - documentos jurídicos extremamente liberais, *pero no mucho*, porque eram liberais com os brancos, documentos inspirados em Beccaria.

O Código Penal de 1830 mantinha a pena de morte e os debates que a mantiveram eram exatamente debates fulcrados na questão racial. A lógica era a seguinte: "Se queremos extinguir a pena de morte, não podemos ter escravidão. Se queremos acabar com a pena de morte, temos que acabar com a escravidão". Então, para manter a escravidão, mantiveram a pena de morte, que basicamente era destinada aos escravizados insurgentes.

Depois, com o código de 1890, que é um código pós-abolição e pós-República, nós temos um código que vem controlar. É um código que nasce com a República antes de uma Constituição. A República não trouxe, primeiramente, uma nova Constituição. Trouxe, primeiramente, um novo Código Penal, que buscou dar uma resposta a uma nova estrutura social que não era a República, e, sim, o fim da escravidão. A resposta à nova estrutura republicana veio em 1891, com outra Constituição. Mas a primeira resposta foi à realidade da abolição dos escravizados. O novo código de 1890 tratava dos ex-escravizados, criando o encarceramento dos negros recém libertos através do crime de vadiagem, da criminalização da capoeira, do curandeirismo. Os cultos e as reuniões culturais afro, de matriz africana sendo, através de um processo de criminalização secundária, vistas como perturbação à ordem e ampliando a punição e o encarceramento, que nasce principalmente no início da República e que hoje ganha vultosa quantia de 800.000 presos, preponderantemente negros - pretos e pardos. Essa é a vocação do sistema penal.

Então, não há como se discutir qualquer tema nas ciências criminais sem partir do ponto de vista de que a escravidão é a matriz analítica, crítica analítica, para nós percebermos isso e analisarmos. Eu digo isso porque existe certo fetiche em relação às novas tecnologias e à ideia de civilização, de que elas podem representar uma ideia de racionalidade e de civilização. Mas quando vamos ver a história disso, nós percebemos que se muda a estética, mas as éticas continuam as mesmas. Então, por exemplo, se nós pensarmos na tortura, nós tínhamos um cenário pré-Inquisição, no qual os conflitos eram resolvidos através de juras, de ordálias, de ordálias de fogo, ordálias de água. Então, o grande giro tecnológico ocorreu na Inquisição, em que métodos científicos, estudos anatômicos de medicina demonstravam, às luzes da ciência, sobre os métodos de apuração da verdade por meio da tortura. Quanto tempo, e de que modo se poderia torturar alguém? A tortura não era só selvageria, barbárie, era um método científico. Existiam manuais de tortura e estudos sobre isso. Enfim, hoje nós olhamos para isso e vemos o quão perverso é. Se olharmos o monitoramento eletrônico e a bola de ferro, nós vamos perceber que mudou muito a estética, mas a ética de controle e expansão punitiva de vigilância continua, mais ou menos, o mesmo sistema.

Assim, quando nós vamos pensar em extração coercitiva de DNA e tortura, ou quando nós vamos pensar em delação premiada a partir de uma prisão preventiva prévia, nós vamos ver que todos os elementos éticos de uma tortura, desde lá da Inquisição, estão presentes nesses instrumentos, nessas tecnologias de poder através de uma estética diferenciada. Desse modo, é muito importante a gente perceber isso quando

formos tratar dessas questões tecnológicas: até que ponto a tecnologia pode servir à dignidade humana e até que ponto ela pode reproduzir o atraso, o autoritarismo, a exclusão, a opressão, a crueldade, a desumanização das pessoas.

Nesse contexto, a gente pode pensar a questão da proteção de dados. No Brasil, nós tivemos a LGPD, que, em seu artigo quarto, excluiu expressamente do seu tratamento a investigação criminal, as questões afetas ao sistema penal e relegou a uma lei futura, que ainda não veio.

Hoje, nós temos um anteprojeto de lei, que está sendo estudado por uma comissão de juristas, desde 2019, que vem tentar dar conta desse problema de tratamento de dados. Esse projeto vai beber precipuamente de tudo isso que eu falei antes sobre a escravidão, a questão colonial, a questão de uma perspectiva eurocentrada, etc. Ele parte de uma análise, basicamente, das diretrizes de 2016 da Comunidade Europeia, do Parlamento Europeu. Você vai ver, por exemplo, a lei portuguesa, que trata disso também, é uma cópia dessas diretrizes, e a nossa também bebe muito disso.

A gente percebe uma falta de um olhar periférico. Um olhar de uma cidade, de um país, de um território que é dominado por uma desigualdade abissal, por áreas de profunda exclusão, em que o sistema penal é aplicado numa perspectiva de necropolítica, de controle punitivo e de um processo de genocídio de uma população indesejada - que é a população negra periférica, que é basicamente a clientela do sistema penal. O sistema penal sempre foi destinado e ocupado por pretos pobres periféricos.

Recentemente descobriu-se essa possibilidade de se usar o sistema penal também como *lawfare* para tratar os inimigos políticos. E aí vimos o gracejo do sistema penal para tangenciar personalidades, como empresários, políticos, etc., numa democratização de arbitrariedades, digamos assim, uma "demo-

/ NÃO HÁ COMO SE DISCUTIR QUALQUER TEMA NAS CIÊNCIAS CRIMINAIS SEM PARTIR DO PONTO DE VISTA DE QUE A ESCRAVIDÃO É A MATRIZ ANALÍTICA /

/ NESSAS TECNOLOGIAS DOMINADAS POR UMA NOVA ESTÉTICA, POR UMA ESTÉTICA DIGITAL, PRECIPUAMENTE, SE ESCONDE UMA ÉTICA AUTORITÁRIA PERVERSA /

cratização" seletiva de ilegalidade; expandindo-se abusos do sistema penal para os inimigos políticos, empresários, etc, etc.

Mas, principalmente, esse sistema penal sempre foi voltado para pretos pobres periféricos, de modo que, quando a gente olha esse projeto de lei, vimos que apesar dele fazer menção a uma questão racial, etc., ele não enfrenta alguns aspectos práticos.

Precisamos parar para pensar que a Lei Geral de Proteção de Dados é uma coisa que parte muito, digamos assim, de uma perspectiva burguesa, de uma Europa. Por quê? Porque lá no Jacarezinho não tem proteção de domicílio e proteção de dados. É pé na porta. A coisa lá é um território de necropolítica profunda.

Então, é óbvio que essa preocupação de proteção de dados, como outras proteções de outras garantias fundamentais, é uma proteção que toca mais a nós incluídos, a nós cidadãos. Não estou dizendo que isso não seja importante, mas estou dizendo o quanto a gente tem que radicalizar essa questão e trazer para uma realidade nacional, uma realidade brasileira, para uma realidade de um país periférico como o nosso.

É óbvio que a nossa lei faz menção à questão racial. Mas ela está, digamos assim, muito voltada para essas diretrizes gerais, dessas inspirações, e não abordou questões importantes que vão ingressar. Porque a tecnologia ingressa no Brasil sem controle. A polícia já tem os seus programas, os seus bancos de dados, as suas tecnologias, seus *softwares* operando, e a gente aqui. A regulação não chegou nesses detalhes.

Então, você tem, por exemplo, uma questão que é ainda do século 19, mas que já nos causa problema, e que vai ganhar dimensões ainda maiores com o desenvolvimento tecnológico que é, por exemplo, a questão do reconhecimento fotográfico. O reconhecimento fotográfico analógico é nefasto, é uma catástrofe que encarcera injustamente pessoas no Brasil. E não tem um regramento no Código de 1941 sobre esse tema. Isso

agora ganha contornos, porque é esse reconhecimento que passa a contar com mecanismos tecnológicos: reconhecimento por rede social, extração ou construção de bancos de dados digitais de imagem de pessoas e etc. E aí não temos verdadeiramente o reconhecimento fotográfico em que a nossa lei, e nem mesmo a doutrina, consegue distinguir o reconhecimento fotográfico por alinhamentos da identificação fotográfica por álbum suspeito, que são coisas absolutamente diferentes. Mas o fato é que nós já temos nas delegacias os álbuns de suspeitos. Esses álbuns de suspeitos não raro são utilizados como pontos de partida para uma investigação.

Diferentemente do reconhecimento fotográfico por alinhamento, em que nós temos um suspeito que, muitas das vezes, vai ter a sua imagem exposta ali ao lado de outros inocentes, para ser reconhecido. Não há nenhuma distinção sobre isso. A doutrina pouco cuida. E aí nós começamos a pensar: ora, a Argentina teve um problema sobre isso (álbuns de suspeitos), em que se questionou lá e etc., e chegaram até um acordo para resolver esta questão. E nós aqui temos, em cada delegacia, e, muitas das vezes, em cada estado, efetivamente, álbuns, que hoje têm um caráter de armazenamento digital, que a gente não sabe como se alimentam, como a pessoa ingressa neles, quanto tempo vai ficar, qual a forma de controle, quem controla, quem trata os dados e o Projeto de Lei não fala sobre isso, por exemplo. Fala de um modo geral de tratamento de dados, mas nós temos esses dados que estão colocados na mão da polícia, que já estão encarcerando pessoas, colocando pessoas para serem presas e processadas cotidianamente.

Então nós temos aí perspectivas de investigação preditiva, de reconhecimentos faciais, de monitoramentos faciais, etc. Uma série de tecnologias e os algoritmos grassando pelas nossas mãos, possibilitando uma série de práticas que, no nosso sistema, vão ser inevitavelmente utilizadas sempre com o cariz da seletividade racial, alimentando esse sistema punitivo que reproduz uma lógica escravagista.

Quando a gente pensa nessa tecnologia como avanço ou como proteção, a gente tem que ter sempre uma preocupação muito grande, porque o sistema penal é, potencialmente, essencialmente, algo que avilta os direitos fundamentais. Vou dar um exemplo para terminar e concluir. Tivemos um caso recente do Matheus. Matheus, que passou no Fantástico, o programa da Rede Globo. Aquele garoto que estava com uma bicicleta na frente do Leblon e foi abordado por um casal de pessoas brancas para questioná-lo sobre o furto da bicicleta. E esse rapaz, esse jovem negro entra virtualmente, isto é, faz um boletim de ocorrência virtual. Ele ingressa nessa delegacia, faz um B.O. pela internet, dizendo que foi vítima de uma atitude racista e queria providência da autoridade policial. A autoridade policial, então, capitula inicialmente aquilo como calúnia e começa a investigar o casal e, de repente, esse jovem, que se dizia se sentir vítima de uma atitude racista, é chamado na delegacia para prestar esclarecimentos de como comprou a bicicleta dele, qual era a bicicleta dele, ele começa a ser investigado. Ele passa a ser suspeito de uma receptação, porque ele comprou a bicicleta pela OLX, ou seja, pela internet. Da mesma forma que ele comprou pela internet, ele registrou o boletim pela internet e aí foi exigido dele nota fiscal, preço, enfim como é que ele comprou. Então, ele "vai" à Delegacia reclamar de um tratamento, digamos assim, de uma atitude racista, como vítima e sai de lá indiciado como receptador. Notem: o inquérito da suposta calúnia sequer encerrou e, antes disso, o inquérito de receptação terminou com uma conclusão de que ele deveria ser indiciado por receptação. Depois disso, encerrou-se o inquérito da calúnia com uma conclusão de arquivamento.

O que eu quero dizer com isso? A lógica do sistema penal na escravidão era: o negro não tinha proteção jurídica, o escravizado não tinha proteção jurídica. Então, se alguém fazia alguma coisa contra ele, respondia por dano, por furto, etc. O negro não era visto como pessoa, mas ele tinha responsabilidade criminal. Se ele cometesse um crime de homicídio, ele respondia por homicídio. Então nós vemos que essa lógica persiste até hoje. As injúrias raciais, ao fim e ao cabo, são sempre resolvidas por arquivamentos ou absolvições ou "não houve nada disso". Tem uma racionalidade garantista correta. Mas quando o negro é suspeito, hoje, essa racionalidade não lhe assiste, porque a racionalidade que lhe assiste é a punitivista. Tanto é assim que ele entra como vítima e sai como suspeito.

Mesmo um sistema que, pós-constituição, criminaliza o racismo, tem uma lei de racismo, tem uma lei de injúria com conteúdo racial, mas a funcionalidade disso não está aí para proteger a vulnerabilidade. Por isso é um equívoco, a meu sentir, essa proposta de criminalização, seja do movimento negro, seja do movimento LGBT, seja do movimento de mulheres. Porque o direito penal, o sistema penal não serve para proteger vulnerabilidades. Ele serve, ao contrário, para oprimi-las. Então, quando o incremento tecnológico se junta a isso, é muito difícil criarmos uma cultura, uma ambiência, uma leitura crítica para utilizar esses mecanismos em defesa dessas vulnerabilidades.

O grande desafio de uma lei de proteção de dados, ou de qualquer lei que venha regular as tecnologias de processo penal, no sistema penal, na investigação, é uma tecnologia que sirva eminentemente menos a uma pensada eficiência penal e que pense mais efetivamente em uma inibição de práticas efetivamente racistas e seletivas que incrementam o sistema penal, o encarceramento de pessoas e de pessoas preponderantemente negras e periféricas. Então, temos que ver, nessas tecnologias dominadas por uma nova estética, por uma estética digital, precipuamente, se esconde uma ética autoritária perversa, de uma racionalidade que há muito vem pautando as práticas de poder no Estado. Acho que é esse o grande desafio: uma percepção crítica de tudo o que possa ser construído nessa seara. Muito obrigado.

03.

O DEBATE CONSTITUCIONAL SOBRE FLAGRANTES EM REDES SOCIAIS

Marta Saad

1. INTRODUÇÃO

Em 16 de fevereiro de 2021, no curso do Inquérito Policial originário de n. 4781, conhecido como inquérito das *fake news*, o Ministro Alexandre de Moraes, do Supremo Tribunal Federal, decretou a prisão em flagrante delito do Deputado Federal Daniel Silveira.

Chegara ao conhecimento daquela Corte vídeo publicado pelo Deputado Federal, disponível no *YouTube*, no canal denominado "Política Play", em que o Parlamentar fazia graves ameaças e ofensas à honra dos Ministros do Supremo Tribunal Federal, propagando a adoção de medidas antidemocráticas, como a defesa do AI-5, propondo a substituição imediata de todos os Ministros daquele Tribunal, bem como instigando a adoção de medidas violentas contra a vida e a segurança dos Ministros.

Diante destes fatos bastante graves, o Ministro Relator assinalou a necessidade de "medidas enérgicas para impedir a perpetuação da atuação criminosa de parlamentar visando a lesar ou expor a perigo de lesão a independência dos Poderes instituídos e ao Estado Democrático de Direito", entendendo que "as condutas criminosas do parlamentar configuram flagrante delito, pois verifica-se, de maneira clara e evidente, a perpetuação dos delitos acima mencionados, uma vez que o referido vídeo permanece disponível e acessível a todos os usuários da rede mundial de computadores, sendo que até o momento, apenas em um canal que fora disponibilizado, o vídeo já conta com mais de 55 mil acessos".

O Ministro assinalou que o Deputado, ao postar e permitir a divulgação do vídeo, que permanecia disponível nas redes sociais, "encontra-se em infração permanente e consequentemente em flagrante delito, o que permite a consumação de sua prisão em flagrante".

Entendeu então haver possibilidade constitucional de prisão em flagrante delito do Parlamentar pela prática de crime inafiançável, nos termos do § 2º, do artigo 53 da Constituição da República, e lhe decretou a prisão em flagrante.

No dia seguinte, referida decisão foi referendada por unanimidade pelo Plenário do Supremo Tribunal Federal, mantendo-se a prisão em flagrante do Deputado, em acórdão cuja ementa sintetiza que "as condutas praticadas pelo parlamentar foram perpetradas em âmbito virtual, por meio da publicação e divulgação de vídeos em mídia digital ('YouTube') durante todo o dia, com constante interação do mesmo, situação que configura crime permanente enquanto disponível ao acesso de todos, ainda que por curto espaço de tempo, permitindo a prisão em flagrante do agente".[1]

1. STF, Inq 4781, Rel. Min Alexandre de Moraes, DJe de 14.05.2021.

O que este pequeno texto pretende analisar são as repercussões, penais e processuais penais, de se considerar crime praticado em meio virtual como crime permanente, tal como o fez o Supremo Tribunal Federal neste julgado paradigmático.

2. CRIME PERMANENTE E PRISÃO EM FLAGRANTE DELITO

Flagrante significa inflamado, manifesto, evidente, ardente, queimante. A prisão em flagrante delito empresta esta ideia, por meio da alusão metafórica de chama indicativa de certeza visual de combustão: o fato ilícito penal está acontecendo e, como tal, exige atuação imediata do aparato estatal.[2]

A prisão em flagrante inicia-se como uma medida administrativa, logo depois jurisdicionalizada.[3] Ou seja, é tomada como pré-cautela, sujeita depois à análise judicial. Tem por finalidades fazer cessar a atuação delitiva, impedir a consumação ou exaurimento do delito, deter

2. MORAES, Rafael Francisco Marcondes de. *Prisão em flagrante delito constitucional*. São Paulo: Juspodivm, 2018.

3. BADARÓ, Gustavo Henrique. *Processo penal*. 9. ed. São Paulo: Revista dos Tribunais, 2021.

seu autor e auxiliar na pronta colheita de elementos informativos acerca da ocorrência do crime e sua autoria. A prisão em flagrante envolve, assim, as ideias de atualidade e visibilidade, bem como reação imediata para fazer cessá-la.

A Constituição da República permite a prisão em flagrante delito como uma exceção à exigência de ordem escrita e fundamentada da autoridade competente para a imposição de privação de liberdade. Estabelece no artigo 5º, inciso LXI, que "ninguém será preso senão em flagrante delito ou por ordem escrita e fundamentada de autoridade judiciária competente, salvo nos casos de transgressão militar ou crime propriamente militar, definidos em lei". Além do dever das autoridades, qualquer um do povo pode prender em flagrante delito, nos termos do artigo 301 do Código de Processo Penal.

O Código de Processo Penal prevê, no artigo 302, as hipóteses de flagrância: considera-se em flagrante delito quem está cometendo a infração penal, quem acaba de cometê-la, quem é perseguido, logo após, pela autoridade, pelo ofendido ou por qualquer pessoa, em situação que faça presumir ser autor da infração, ou, por fim, quem é encontrado, logo depois, com instrumentos, armas, objetos ou papéis que façam presumir ser ele autor da infração.

São as chamadas situações de flagrante real ou próprio (o sujeito está cometendo ou acabou de cometer a infração penal) e virtual (impróprio ou quase flagrante: o agente é perseguido logo após; ou flagrante presumido: o sujeito é encontrado, logo depois, com instrumentos, armas, objetos ou papéis que façam presumir ser o autor da infração).

Importa, assim, analisar a consumação do delito, para verificação de hipótese ou não de flagrância, para fins de prisão. Para isso, importante verificar se o crime é instantâneo, permanente ou instantâneo com efeito permanente, porque isso repercute na questão da consumação e, portanto, na possibilidade de flagrância.

Crime instantâneo é aquele que se consuma em momento determinado, sem qualquer prolongamento. Esgota-se com a ocorrência do resultado. Não significa que ocorre rapidamente, mas que, uma vez reunidos seus elementos, a consumação ocorre peremptoriamente e nada poderá ser feito para impedir sua ocorrência.[4]

Crime instantâneo de efeito permanente é crime de consumação imediata, cujo resultado se prolonga no tempo.[5] Tanto a ação como a lesividade ao bem jurídico se exaurem instantaneamente, mas seus efeitos se fazem sentir de maneira perene ou alongada. Assim, o homicídio é um crime instantâneo, na medida em que a ação se encerra com a morte, mesmo que os efeitos daí decorrentes sejam observáveis de forma perene. A mesma coisa com o furto, em que o sujeito pode continuar eventualmente se beneficiando do resultado. Mas isso não altera a qualidade do delito, que é instantâneo. Não há, neste caso, lesão alongada ao bem jurídico.

Já o crime permanente é aquele em que o momento consumativo se alonga e se protrai no tempo, por vontade do agente. Enquanto o sujeito permanece em sua ação, a consumação do delito se estende. É, em verdade, um delito cuja ação é permanente. O bem jurídico protegido pela norma incriminadora encontra-se permanentemente ofendido.

Geralmente, as ações nucleares do tipo penal determinam se a infração pode ser considerada instantânea, permanente ou instantânea de efeito permanente. São exemplos de condutas permanentes o privar alguém de sua liberdade, mediante sequestro ou cárcere privado (artigo 148 do Código Penal), o

4. BITTENCOURT, Cezar Roberto. *Tratado de direito penal*. Vol. 1. Parte Geral. 28. ed.. São Paulo: Saraiva, 2022.

5. DOTTI, René Ariel. *Curso de direito penal*. Parte geral. 8ª. ed. São Paulo: Revista dos Tribunais, 2022.

transportar, conduzir ou ocultar coisa que sabe se produto de crime (artigo 180 do Código Penal), o ocultar cadáver (artigo 211 do Código Penal), o possuir, portar e manter sob sua guarda arma de fogo, da posse irregular e porte ilegal (artigos 12 e 14 do Estatuto de Desarmamento - Lei n. 10.826/2003), o trazer consigo, guardar e ter em depósito drogas, no porte para consumo pessoal e de comércio de substâncias ilícitas (artigos 28 e 33 da Lei de Drogas - Lei n. 11.343/2006), o ocultar bens, direitos e valores provenientes de infração penal (artigo 1º da Lei de Lavagem - Lei n. 9.613/1998), o manter no exterior depósitos não declarados à repartição federal competente (artigo 22, parágrafo único, da Lei n. 7.492/86).

Em todos estes casos, a ação delitiva se prolonga no tempo. Justamente por isso, a prisão em flagrante delito nos crimes considerados permanentes apresenta peculiaridades, por conta da sua consumação que se estende no tempo e, igualmente, fazendo com que exista um estado de flagrância igualmente prolongado. Neste sentido, é cabível a prisão em flagrante delito em relação ao crime permanente a qualquer momento, enquanto perdurar a ação ilícita. É o que estabelece o artigo 303 do Código de Processo Penal: "nas infrações permanentes, entende-se o agente em flagrante delito enquanto não cessar a permanência". Enquanto durar a permanência, o sujeito pode ser preso em flagrante delito, porque se considera que o agente "está cometendo a infração penal", nos termos do que prevê o artigo 302, inciso I, do Código de Processo Penal.

Assim, o Supremo Tribunal Federal, ao asseverar que a disponibilização de vídeo com conteúdo criminoso na rede mundial de computadores tem o condão de tornar as condutas ilícitas ali praticadas, os crimes de manifestação (crimes contra a honra e crimes contra o Estado Democrático de Direito), em crimes permanentes, autoriza-se que, enquanto o vídeo esteja veiculado, seja possível a prisão em flagrante delito.

Como medida excepcional à determinação de que toda restrição de direito fundamental depende de prévia autorização judicial, tem-se que as situações que autorizam a prisão em flagrante devem ser típicas e taxativas e interpretadas restritivamente (artigo 5º, LXVI, da Constituição da República), o que parece não ocorrer com tal interpretação alargada acerca da configuração de crime praticado via internet como crime permanente.

As repercussões de se considerar o crime cibernético como crime permanente, porém, não param por aí.

3. CRIME PERMANENTE, PRISÃO EM FLAGRANTE DELITO E INVIOLABILIDADE DOMICILIAR

Considerar que o sujeito que pratica crime permanente está em flagrante delito também repercute na possibilidade, nestes casos, de busca e apreensão domiciliar sem prévia autorização judicial.

A inviolabilidade do domicílio recebe especial tutela no artigo 5º, inciso XI, da Constituição da República, que preceitua que "a casa é 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".

Dentre as exceções arroladas pela Constituição da República à regra da inviolabilidade domiciliar, encontra-se justamente a flagrância delitiva, razão pela qual o ingresso em residência para interromper prática criminosa em estado flagrancial consubstancia causa excludente de ilicitude dos crimes de violação de domicílio (artigo 150 do Código Penal) e de abuso de autoridade (artigo 22 da Lei n. 13.869/2019), nos termos do artigo 23, inciso III, do Código Penal.

Isso significa dizer que, adotada a premissa expressa pelo Supremo Tribunal Federal de que o crime cibernético é crime permanente, seria possível a realização de busca e apreensão sem autorização judicial para apuração deste delito, bastante para isso que a entrada forçada em domicílio sem ordem judicial fosse escorada em fundadas razões indicativas da situação de flagrância delitiva no interior da residência, devida e posteriormente justificadas para moderação pelo Poder Judiciário.

4. CRIME PERMANENTE E QUESTÕES PENAIS: INÍCIO DA CONTAGEM DO PRAZO PRESCRICIONAL E POSSIBILIDADE DE APLICAÇÃO DE LEI PENAL POSTERIOR MAIS GRAVE

Considerar que o crime praticado na internet é, por si, crime permanente também tem repercussões importantes do ponto de vista do direito penal material, tanto em relação ao termo inicial de contagem do prazo prescricional quanto também da lei aplicável, caso haja superveniência de lei posterior mais gravosa.

Em regra, o termo inicial da prescrição é o da consumação do crime. Tendo em conta que o crime permanente é aquele em que o momento consumativo se alonga e se protrai no tempo, por vontade do agente, o bem jurídico protegido pela norma penal incriminadora encontra-se permanentemente ofendido.

Daí a razão da regra prevista no artigo 111, inciso III, do Código Penal, que impõe que o início do cálculo prescricional, em caso de crime permanente, se dê apenas com a cessação da permanência. Alonga-se, desta forma, a consumação, e, consequentemente, a possibilidade de início de contagem do prazo prescricional.

Ademais, também sob o ponto de vista penal, há mais uma repercussão, no tocante à possibilidade de aplicação de lei penal mais gravosa. A Constituição da República estabelece, no artigo 5º, inciso XL, que "a lei penal não retroagirá, salvo para beneficiar o réu". Tem-se, assim, a irretroatividade da lei penal, salvo quando a lei nova seja benéfica ao acusado.

O verbete da Súmula n. 711, do Supremo Tribunal Federal, porém, diz que "a lei penal mais grave aplica-se ao crime continuado ou ao crime permanente, se a sua vigência é anterior à cessação da continuidade ou da permanência".

O crime permanente é único, de execução alongada no tempo. A consumação, marcada pela permanência, pode começar enquanto vigente uma lei e se estender até que outra lei, mais grave, entre em vigor. Neste caso, o crime, único, também foi praticado sob a égide da lei mais gravosa. E, por isso, sendo um crime único, deve ser regido por uma única lei. Neste caso, segundo o entendimento consolidado na Súmula 711 do Supremo Tribunal Federal, a lei que se aplicará é aquela que estiver vigente quando a permanência cessar, ainda que seja mais grave, de aplicação imediata, porque o fato, em sua integralidade, ainda está sendo executado.[6]

6. BITTENCOURT, Cezar Roberto. *Tratado de direito penal*. Vol. 1. Parte Geral. 28. ed.. São Paulo: Saraiva, 2022.

As repercussões, portanto, são muitas, a partir do entendimento de que o crime praticado na internet é permanente. Com este entendimento, criam-se possibilidades de atuação estatal sem autorização judicial (prisão em flagrante e busca e apreensão) e incrementa-se o poder punitivo, seja pela questão de fixação prolongada do termo inicial de contagem do prazo prescricional (não da conduta em si, mas sim da cessação da alegada permanência) e da possibilidade de aplicação de lei penal porventura mais gravosa, enquanto não cessada a permanência.

5. AFINAL, A INTERNET REMODELA CONCEITO DE PERMANÊNCIA, PARA FINS PENAIS?

Diante disso, de se perguntar se, de fato, por graves que sejam os fatos sob apuração, a internet tem capacidade de remodelar o conceito de permanência, do ponto de vista penal.

Cada vez mais, a internet tem sido meio, instrumento, forma ou veículo para condutas criminosas, que tensionam o aparato estatal de investigação e apuração de condutas e sua autoria.

Além do julgado paradigmático do Supremo Tribunal Federal acima mencionado, houve inclusive Projeto de Lei em tramitação, registrado sob o n. 5.463/2016, de iniciativa do Deputado Roberto Alves, hoje apensado ao Projeto de Lei n. 8.045/2019, que objetiva a reforma global do Código de Processo Penal.

Este projeto pretendia incluir, dentro da previsão da prisão em flagrante no caso de infrações permanentes, já constante no artigo 303 do Código de Processo Penal, os crimes cibernéticos cuja consumação se estendesse no tempo, seja pela permanência da publicação original em determinado sítio eletrônico, seja pela disseminação e replicação do conteúdo delituoso na rede mundial de computadores, ainda que houvesse exclusão, posterior ao flagrante, do conteúdo.

Desta forma, estando o conteúdo ou ação delituosa ainda disponível de alguma forma na internet, o sujeito estaria em situação flagrancial. O artigo 303 do Código de Processo Penal, que já prevê que "nas infrações permanentes, entende-se o agente em flagrante delito enquanto não cessar a permanência", ganharia então dois parágrafos adicionais: "§ 1º. Considera-se, também, como infração permanente o crime cibernético cujo conteúdo permaneça na internet, ainda que excluída a publicação original, mas, em razão de sua disseminação ou de qualquer outro motivo determinante, tenha havido a replicação e a permanência do conteúdo delituoso

/ A PRISÃO EM FLAGRANTE ENVOLVE, ASSIM, AS IDEIAS DE ATUALIDADE E VISIBILIDADE, BEM COMO REAÇÃO IMEDIATA PARA FAZER CESSÁ-LA /

na rede mundial de computadores"; e "§ 2º. Entende-se o agente em flagrante delito enquanto houver a permanência do conteúdo delituoso na internet, nos termos do parágrafo anterior".

Seria o chamado "flagrante digital", "ampliando a dogmática penal com o escopo de atingir as novas modalidades de crimes digitais".[7]

Em favor da consideração do crime cibernético como crime permanente e do empréstimo do tratamento jurídico conferido a esta espécie de crime, alega-se que existem singularidades jurídicas na internet, que justificariam o tratamento diferenciado: (i) ínfimas possibilidades de identificação de autoria, em razão o anonimato dos usuários, (ii) irreversibilidade espaço-temporal, já que a violação da honra e da privacidade na internet tornam-se irreversíveis visto que as informações ficam permanentemente lá gravadas e alcançam inúmeros indivíduos, (iii) permanência eterna da informação e do dano, (iv) multiníveis de responsabilidades, em razão da variedade de provedores e prestadores de serviços na internet, (v) perecibilidade das provas e, por fim, (vi) internacionalização das condutas.[8]

Daí o reclamo por maior severidade e celeridade na apuração de condutas praticadas por meio da internet.

Não pode, porém, uma lei, por arranjo político-criminal, de medida político-legislativa, criar uma ficção, tornando condutas ilícitas idênticas às praticadas em meio físico ou analógicas (como os crimes contra a honra[9] ou os crimes contra o Estado Democrático de Direito, para ficar em exemplos acima tratados) crimes permanentes, unicamente porque praticadas em meio virtual.

A disponibilidade em rede social não torna a conduta, em si, permanente. A permanência existe na conduta, não é dada por lei. Nem é a lei que define se o crime é ou não permanente.

E mais: o incremento punitivo não passa necessariamente por esta criação ficcional. Se os crimes são graves em razão do alcance que possuem, isso não atinge a natureza do ato, transmudando-o de instantâneo em permanente.

Se é exigida efetiva e maior punição, melhor tratar este dado cerca do alcance considerável da conduta como fator de incremento da punição, tal como hoje acontece com o artigo 122, § 4º e § 5º do Código Penal (que prevê aumento da pena em caso de induzimento, instigação ou auxílio a suicídio ou a automutilação, quando praticada por rede de computadores, rede social ou transmitida em tempo real ou quando ainda o agente é líder ou coordenador de grupo ou rede virtual) e artigo 141, § 2º, do Código Penal (penas aumentadas, se o crime contra a honra é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores).

Ainda, se é necessária melhor investigação, existem instrumentos processuais perfeitamente ao alcance das autoridades para apuração da conduta ilícita, dependentes de autorização judicial, como, aliás, deve ser. Assim, é possível a decretação de busca e apreensão mediante decisão judicial, desde que presentes os pressupostos e requisitos autorizadores, que devem ser analisados por juiz competente. Também é possível a supressão de liberdade, por meio de prisão processual, caso presentes os requisitos que permitem a decretação da medida.

Ao se lançar mão, porém, de considerar o crime cibernético como crime permanente, abre-se caminho para atuação estatal

7. Parte da justificada apresentada pelo Deputado Roberto Alves, ao propor o Projeto de Lei n.5.463/2016.

8. MORAES, Felipe Otávio. Cibercrime como crime permanente. Disponível em https://bit.ly/3NbBN5k. Acesso em 17.jun.2022.

9. "Faz-se uma analogia. Com a inconstitucionalidade da Lei da Imprensa, a difamação por meio de jornais possui a mesma tipificação (art. 139 c/c 141, III). É uma manifestação que também possui permanência. Deve o crime ser considerado como tal enquanto existir qualquer cópia do jornal em circulação? Qualquer cópia arquivada? Enquanto uma única banca de jornal ainda possuir um exemplar exposto, a venda, continuará o autor em situação de flagrância? Tal situação é inaceitável" (BARBOSA, Rodrigo Pedroso. Sobre a permanência dos crimes on-line: entre a consumação e o exaurimento. Disponível em: https://bit.ly/3NbC5ZY. Acesso em 16.jun.2022).

desenfreada, que pode levar indivíduo a ser preso em flagrante delito por afirmações feitas em passado longínquo.[10] Pode inclusive ser preso por qualquer um do povo, autorizada a prisão em flagrante.

Ademais, seria possível busca e apreensão domiciliar sem autorização judicial. A prescrição sequer começaria a correr, porque a rigor não estaria cessada a permanência enquanto o vídeo existisse, criando um crime na prática imprescritível e que, a despeito da vontade do autor, continua a ser praticado, caso a disponibilização na internet fugisse a seu controle.[11]

Crimes contra a honra ou crimes contra o Estado Democrático de Direito, praticados na internet, devem ser tidos como instantâneos. A contínua disponibilidade, caso existente, deve ser considerada exaurimento, não consumação do delito.[12]

Do contrário, a fim de permitir resposta estatal e mecanismos eficientes de política criminal, por meio de contorcionismos artificiais como a atribuição do regime de crime permanente a tais delitos cibernéticos, ter-se-ia por escalada, além da solução imediatamente almejada - a prisão em flagrante do sujeito investigado –, a ocorrência de tantas outras repercussões importantes, em detrimento das garantias que seriam ordinariamente aplicáveis ao caso.

Enfim, por melhores que sejam as intenções e por maiores que sejam os reclamos por apuração e punição efetiva de crimes cibernéticos, mostra-se temerário, em um Estado Democrático, considerá-los crime permanente sem que ontologicamente o sejam.

10. MAFEI, Rafael. Agora, quem tem Twitter tem medo. Disponível em: https://bit.ly/3bjoz9H. Acesso em 03.jun.2022.

11. "Conteúdos disponibilizados na internet fogem do controle do autor, sendo arquivados e redistribuídos. Cita-se, *exempli gratia*, o *Internet Archive* que tem como proposta armazenar um conteúdo perpetuamente. Outras pessoas podem ter copiado e salvo, repostando. O provedor de conteúdo pode se recusar a tirar o conteúdo do ar, mesmo a pedido do autor. Repete-se: atribuir-se a classificação de crime permanente a crimes praticados por conteúdo disponibilizado na internet significa transformar tais crimes em uma novel classificação: crimes eternos" (BARBOSA, Rodrigo Pedroso. Sobre a permanência dos crimes on-line: entre a consumação e o exaurimento. Disponível em: https://bit.ly/3NbC5ZY. Acesso em 16.jun.2022).

12. BARBOSA, Rodrigo Pedroso. Sobre a permanência dos crimes on-line: entre a consumação e o exaurimento. Disponível em: https://bit.ly/3NbC5ZY. Acesso em 16.jun.2022.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BADARÓ, Gustavo Henrique. Processo penal. 9. ed. São Paulo: Revista dos Tribunais,

BARBOSA, Rodrigo Pedroso. Sobre a permanência dos crimes on-line: entre a consumação e o exaurimento. Disponível em: https://bit.ly/3NbC5ZY. Acesso em 16.jun.2022.

BITTENCOURT, Cezar Roberto. Tratado de direito penal. Vol. 1. Parte Geral. 28. ed.. São Paulo: Saraiva, 2022.

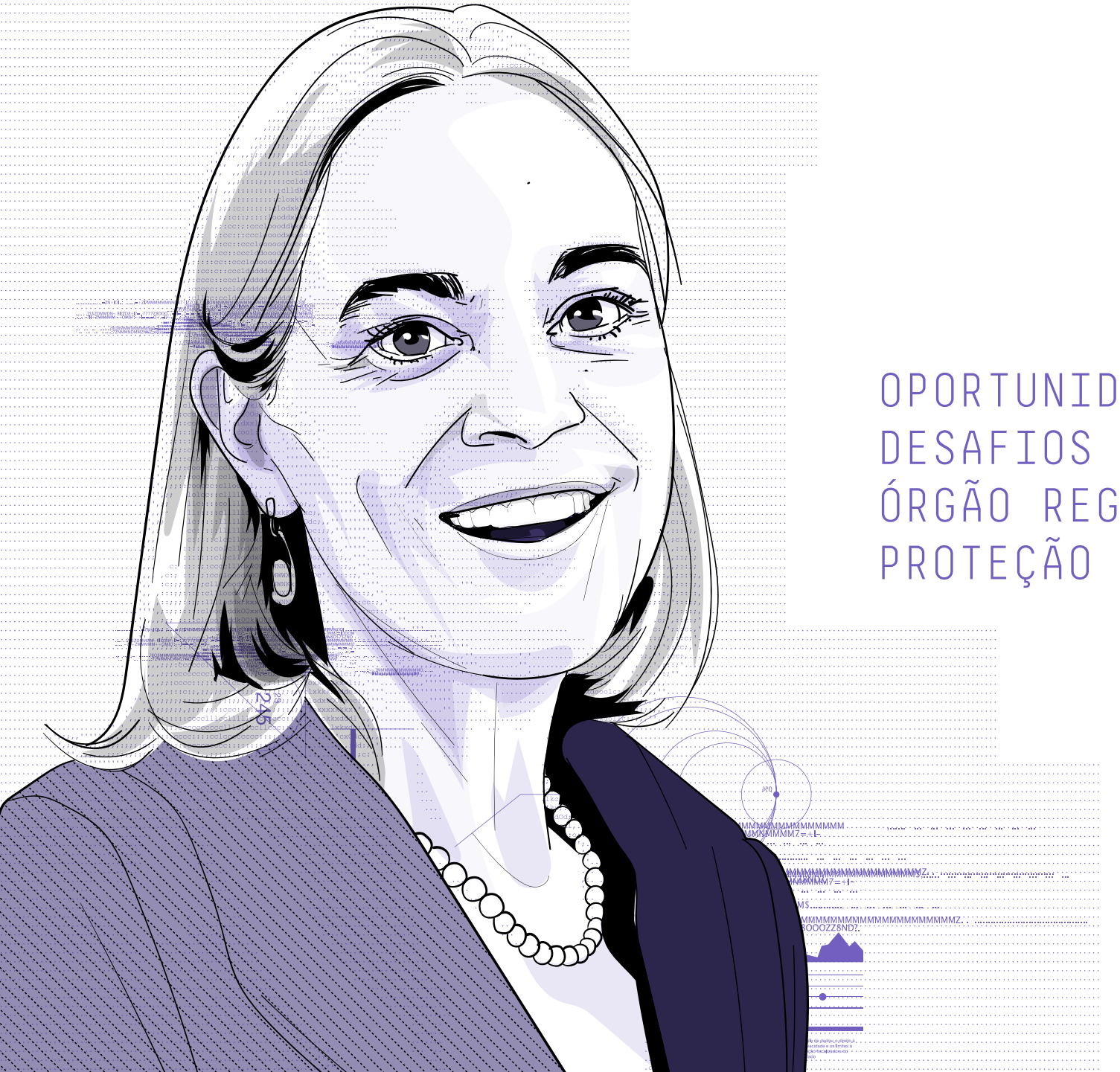
DOTTI, René Ariel. Curso de direito penal. Parte geral. 8ª. ed. São Paulo: Revista dos Tribunais, 2022.

MAFEI, Rafael. Agora, quem tem Twitter tem medo. Disponível em: https://bit.ly/3bjoz9H. Acesso em 03.jun.2022.

MORAES, Felipe Otávio. Cibercrime como crime permanente. Disponível em https://bit.ly/3NbBN5k. Acesso em 17.jun.2022.

MORAES, Rafael Francisco Marcondes de. Prisão em flagrante delito constitucional. São Paulo: Juspodivm, 2018.

STF, Inq 4781, Rel. Min Alexandre de Moraes, DJe de 14.05.2021.



04.

OPORTUNIDADES E DESAFIOS DO CNJ COMO ÓRGÃO REGULADOR DE PROTEÇÃO DE DADOS

Maria Thereza De Assis Moura

1. CONTEXTUALIZAÇÃO INICIAL.

O presente texto é fruto da participação no Congresso **"Direitos Fundamentais e Processo Penal na Era Digital"**, realizado em 1º de setembro de 2021.

No painel em que tive a satisfação de participar, foi abordado o tema **"Proteção de dados e Justiça Criminal: qual o papel a ser exercido pelo CNJ"**, o qual foi debatido juntamente com a Professora Doutora Laura Schertel Mendes e o Defensor Público do Estado de São Paulo Renato de Vitto.

Destaco a relevância do evento para a compreensão da tutela dos direitos fundamentais no processo penal, no contexto da era digital, notadamente por considerar que aperfeiçoamento decorrente do debate a respeito dos temas de interesse contemporâneo, seja à vista da necessidade de contínuo aprimoramento, seja em razão da superveniência de novos diplomas ou de propostas legislativas, constitui premissa fundamental para a busca da excelência das atividades inerentes ao sistema de justiça criminal.

Em particular, diante do advento da Lei Geral de Proteção de Dados Pessoais, muitas questões, de fato, se põem à discussão, motivo pelo qual deixo, aqui, sem qualquer pretensão de esgotar a matéria, algumas impressões iniciais acerca do papel atribuído ao Conselho Nacional de Justiça no Anteprojeto da LGPD Penal.

2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: GENERALIDADES.

A Lei 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais - LGPD, traz à luz um novo paradigma no tratamento das informações pessoais dos cidadãos, com profundas repercussões nas atividades judiciais e investigativas, especialmente diante da publicização dos atos que nesta seara se praticam e dos dados que nela são tratados.

Com efeito, o legislador constituinte originário erigiu a publicidade dos atos processuais à condição de regra geral, a ser excepcionada pela lei tão somente quando imprescindível à salvaguarda da defesa da intimidade ou do interesse social (art. 5º, LX).

A proteção à intimidade, privacidade e ao sigilo de dados, por seu turno, também constitui objeto de tutela constitucional (art. 5º, X e XII), tendo sido promovida recente alteração na Constituição Federal[1] para incluir expressamente a proteção de dados pessoais, inclusive nos meios digitais, dentre os direitos e garantias fundamentais (art. 5º, LXXIX) assim como para fixar a competência privativa da União para legislar sobre o tema (art. 22, XXX). Em conformidade com a referida Emenda Constitucional, atribui-se, outrossim, à União a competência para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (art. 21, XXVI).

1. Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

3. AÇÕES DO CONSELHO NACIONAL DE JUSTIÇA À LUZ DO ADVENTO DA LGPD

A partir do advento da Lei Geral de Proteção de Dados Pessoais, o Conselho Nacional de Justiça instituiu um Grupo de Trabalho, pela Portaria n. 63, de 26 de abril de 2019,[2] visando a elaboração de estudos e propostas voltadas à política de acesso às bases dos dados processuais dos tribunais, especialmente no que diz respeito à consulta e coleta de dados destinados a fins comerciais.

2. Disponível em: https://bit.ly/3KSTQG5, acesso em 16/03/2022.

Com apoio nas atividades desenvolvidas pelo referido grupo, foi editada, em 20 de agosto de 2020, a Recomendação n.

73/2020,[3] instando os órgãos do Poder Judiciário brasileiro à adoção de medidas preparatórias e ações iniciais para a adequação às disposições contidas na LGPD.

Considerou-se, na oportunidade, a crescente utilização da Internet e de modelos computacionais estruturados para acessos e processamento de dados disponibilizados pelos órgãos do Poder Judiciário, bem assim a necessidade de proteção da privacidade e dos dados pessoais de jurisdicionados e outros sujeitos identificados ou identificáveis nos atos processuais.

Em conformidade com o referido ato normativo, foi recomendada, em síntese:

< A > a elaboração de um plano de ação por cada órgão do Poder Judiciário brasileiro;

< B > a disponibilização ao público de informações sobre a aplicação da LGPD e de formulário para o exercício dos direitos dos titulares de dados pessoais;

< C > a elaboração e publicação de política de privacidade e o registro dos tratamento dos dados pessoais; e

< D > a constituição de Grupo de Trabalho para estudo e identificação das medidas necessárias à implementação da LGPD no âmbito do respectivo tribunal, cujo relatório subsidiará a elaboração de uma política nacional pelo Conselho Nacional de Justiça.

Posteriormente, em 15 de outubro de 2020, sobreveio a edição da Portaria n. 212/2020,[4] que, revogando a Portaria 63/2019, instituiu um novo Grupo de Trabalho, também com o propósito da elaboração de estudos e propostas voltadas à adequação

3. Disponível em: https://bit.ly/3MUSGT1, acesso em 16/03/2022.

/ O ANTEPROJETO VEM A INTEGRAR UM VERDADEIRO MICROSSISTEMA QUE DISCIPLINA A PROTEÇÃO DE DADOS PESSOAIS NO SISTEMA DE JUSTIÇA CRIMINAL /

/ O EXERCÍCIO DE TAIS INCUMBÊNCIAS DEMANDARIA IMPORTANTE REESTRUTURAÇÃO, AMPLIANDO-SE A RETAGUARDA MATERIAL E FUNCIONAL NO ÂMBITO DO CNJ /

dos tribunais à Lei Geral de Proteção de Dados Pessoais.

Os trabalhos realizados culminaram com edição, em 12 de janeiro de 2021, pelo Plenário do CNJ, da Resolução n. 363/2021,[5] responsável pelo estabelecimento de medidas para o processo de adequação da LGPD, a serem adotados pelos tribunais.

Dentre as medidas contempladas na Resolução n. 363/2021, destacam-se a determinação da criação de um comitê gestor de proteção de dados pessoais, responsável pela implementação da LGPD em cada tribunal; a criação de site com informações sobre a aplicação da LGPD; a disponibilização de informações adequadas sobre o tratamento de dados pessoais; a revisão dos modelos de minutas de contratos e convênios que autorizem o compartilhamento de dados e a elaboração de orientações para contratações futuras, entre outras.

Também no âmbito da Corregedoria Nacional, a quem, regimentalmente, incumbe a expedição de atos normativos destinados ao aperfeiçoamento das atividades dos serviços notariais e de registro, foi expedida a Portaria 60/2020,[6] instituindo Grupo de Trabalho para a elaboração de estudos e propostas voltadas à adequação dos serviços prestados pelas unidades extrajudiciais à LGPD, cujas atividades culminaram com a apresentação de uma proposta de ato normativo, que foi submetido a consulta pública,[7] encontrando-se as atividades referido grupo de trabalho, atualmente, em fase de encerramento.

Por fim, foi aprovada, pelo 15º Encontro Nacional do Poder Judiciário, uma Diretriz Estratégica para o ano de 2022,[8]

4. Disponível em: https://bit.ly/3Jg7J7n, acesso em 16/03/2022.

5. Disponível em: https://bit.ly/3q9r7vv, acesso em 16/03/2022.

6. Disponível em: https://bit.ly/363HEKr, acesso em 16/03/2022.

7. Disponível em: https://bit.ly/3t0ER7u acesso em 20/03/2022.

8. Disponível em: https://bit.ly/3u5eJ08>, acesso em 16/03/2022.

proposta pela Corregedoria Nacional, instando as Corregedorias dos Tribunais de Justiça dos Estados e Distrito Federal, a fim de regulamentar e promover a adequação dos serviços notariais e de registro às disposições contidas na Lei Geral de Proteção de Dados e supervisioná-los nesta seara, inclusive mediante verificação nas inspeções ordinárias.

Verifica-se, assim, que o Conselho Nacional de Justiça, à vista das competências que lhe foram atribuídas pelo artigo 103-B da Constituição Federal, assumiu postura protagonista no que diz respeito ao implemento dos comandos vertidos na Lei Geral de Proteção de Dados Pessoais nas atividades desempenhadas, tanto pelo Poder Judiciário, quanto pelos órgãos prestadores de serviços notariais e de registro que atuem por delegação do poder público ou oficializados.

9. A inaplicabilidade da LGPD às matérias arroladas no art. 4º, III, não chega a ser absoluta, porquanto seguirá a incidência dos princípios gerais de proteção ao titular dos dados previstos nos artigos 6º, 17 e 18 – adequação, necessidade, transparência e não discriminação – dispondo o titular dos dados, ainda, do direito de acesso, correção, anonimização e eliminação de informações inadequadas (MENEZES, Joyceane Bezerra; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato [Coords.]. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 183).

4. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A JUSTIÇA CRIMINAL.

A superveniência da Lei Geral de Proteção de Dados Pessoais foi, de fato, disruptiva, ao alterar, em certa medida, o tradicional paradigma inerente à publicidade dos dados pessoais no âmbito da justiça criminal, ao tempo em que deixou a cargo de futura legislação específica[9] a disciplina do tratamento dos dados pessoais no contexto da segurança pública e das atividades de investigação e repressão a infrações penais, mediante a observância do devido processo legal, dos princípios gerais de proteção e dos direitos do titular por ela estabelecidos.

É certo que a evolução tecnológica propiciou o advento de novos mecanismos de interconexão e transmissão de informações em tempo real, emergindo, por conseguinte, uma nova face da criminalidade que fulminou a eficiência dos mecanismos tradicionais de investigação, que precisaram ser aprimorados.

Desse modo, também no campo da investigação e repressão às infrações penais,[10] o implemento das novas tecnologias se fez necessário para agregar a necessária eficiência, efetividade e celeridade capazes de obstar a deterioração da prova material dos crimes.

Não há dúvida, entretanto, de que a restrição aos direitos fundamentais se verifica, em maior ou menor grau, na exata medida em que a tecnologia avança como mecanismo de combate ao crime, aspecto em que se faz de rigor o estabelecimento de limites aos poderes de investigação do Estado, como forma de tutela dos direitos fundamentais dos titulares dos dados pessoais.

Com efeito, no âmbito do sistema de justiça criminal, ordinariamente são acessadas informações pessoais relativas aos investigados e terceiros, as quais são registradas, conservadas e, muitas vezes, intercambiadas. Até mesmo "os dados pessoais mais ordinários, se combinados e associados a outros por mecanismos computacionais, também podem revelar informações valiosas sobre o titular"[11].

10. O tratamento dos dados tem sido decisivo no contexto da investigação criminal, a exemplo do rastreio da localização de pessoas "a partir do endereço de IP utilizado em ações criminosas, análise de dados informativos de mensagens de aplicativos, entre outras modernas técnicas de investigação que auxiliam na solução de crimes. Inegavelmente, portanto, há um interesse público para a persecução penal tenha acesso a essa nova tecnologia (inclusive, para fornecer uma resposta penal adequada e atual)" (FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*. vol. 185. ano 29. São Paulo: Ed. RT, novembro 2021, p. 120).

11. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo, *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons. 1. ed. 2021, p. 161.

A publicidade, inerente, como regra geral, às atividades do sistema de justiça criminal, não permite, todavia, que haja divulgação e disseminação imoderada[12] dos elementos de informação que consubstanciam as atividades de combate ao crime e que lhe articulam e dão sentido.

Com efeito, a manipulação indiscriminada de dados em investigações criminais pode importar em risco efetivo a princípios do Estado Democrático de Direito e do Direito Penal, na medida em que:

> (...) a quantidade de dados a que agências de segurança tratam pode gerar uma situação de vigilância permanente dos cidadãos, bem como expandir os problemas já existentes no sistema de justiça criminal. Tratar dados pessoais de maneira massiva tem relação com a utilização de dados pessoais para categorizar indivíduos (*profiling*) ou determinados grupos (*grouping*). Tem estrita relação com a tomada de decisões por sistema automatizados e oferecem uma aparência de neutralidade, mas que já demonstrou tomar decisões discriminatórias e potencialmente perigosas para os sistemas democráticos (...). Rapidamente, podemos elencar alguns usos de dados pessoais no sistema de justiça criminal: interceptação ou requisição de dados para investigações criminais; polícia preditiva (*big data policing*); utilização de novas tecnologias de vigilância (como reconhecimento facial); gerenciamento de decisões no sistema de justiça criminal (decisões do Poder Judiciário tomadas por algoritmos) e, ainda, técnicas de data mining em situações de *dragnet policing*, ou seja: quando há um tratamento de dados pessoais de um sem-número de pessoas para buscar a autoria de determinado delito. *Dragnet policing* são ações coordenadas da polícia para a captura de suspeitos (por exemplo, barricadas em estradas), os quais já atingem também meios tecnológicos (...): obtenção de uma série de dados pessoais, de um sem-número de cidadãos, a fim de tentar individualizar uma conduta.

Em se tratando de gestão da segurança pública, o registro e o tratamento indiscriminado de informações atingem uma dimensão individual, na reprodução massiva e automatizada de padrões que, diga-se, já existiam no direito penal (por exemplo de seletividade). Assume, também, uma dimensão coletiva a partir da ideia de uma vigilância constante, perigoso fenômeno que só é possível a partir do uso de novas tecnologias computacionais (...). [13]

É fundamental, nesse contexto, que o sistema jurídico garanta "as condições materiais para que o indivíduo possa *decidir*, por conta própria, quem deve, em que circunstância e tempo, saber o que a seu respeito. E, para isso, ele também precisa *saber* quem sabe o que a seu respeito".[14]

Também em se tratando de segurança pública[15] há múltiplos exemplos de tratamento de dados penais, tais como a utilização de sistemas decisões automatizadas, uso de tecnologia de reconhecimento facial e táticas de polícia preditiva.[16]

Note-se que, particularmente no que diz respeito a atividades de segurança pública e persecução penal, os direitos

12. No contexto do Banco Nacional de Perfil Genético e do Banco Nacional Multibiométrico e de Impressões Digitais, este decorrente da alteração da Lei 12.037/2009 pela Lei Anticrime, "será premente observarem-se os direitos dos titulares das informações colecionadas, ainda que venham a ser tratadas para fins de segurança pública e de investigação de infrações", dado que o direito à privacidade e os princípios conexos à proteção de dados salvaguardam as pessoas em face do Estado de Vigilância (MENEZES, Joyceane Bezerra; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato [Coords.]. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 183).

13. FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*. vol. 185. ano 29. São Paulo: Ed. RT, novembro 2021, p. 136/137.

14. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo, *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons. 1. ed. 2021, p. 161.

fundamentais "erguem, no entorno de seu objeto de proteção, barreiras contra ações estatais interventivas. Essas barreiras equivalem a exigências mínimas que o Estado deve cumprir para que sua ação interventiva esteja justificada". [17]

Assim, a ressignificação da gestão da segurança pública e dos métodos de combate ao crime, de modo a compatibilizar o princípio da publicidade ao direito à autodeterminação informacional,[18] desponta, na contemporaneidade, como necessidade intransponível.

5. O ANTEPROJETO DA LGPD PENAL

Em conformidade com o artigo 4º, III, da LGPD,[19] o diploma legal não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão a infrações penais.

Outrossim, estabelece o parágrafo primeiro do referido dispositivo legal que o tratamento de dados pessoais referidos no inciso terceiro será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.

15. Temas sensíveis consistem "em confiar o controle de complexos sistemas de vigilância correlacionados à segurança pública/estatal, de investigação e de repressão penal, às pessoas jurídicas de direito privado sujeitas às livres regras de mercado" (MENEZES, Joyceane Bezerra; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato [Coords.]. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 185).

16. Policiamento preditivo "é a série de tratamentos utilizados para 'antecipar' ou 'prever' crimes, ou, ainda, dar uma resposta mais efetiva à questão criminal no futuro. Esses sistemas são baseados em algoritmos que criam padrões de consumo, ou outros tipos de perfilização, e já são implementados em polícias no mundo para, inclusive, prever quais cidadãos têm mais tendência de cometer crimes" (FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*. vol. 185. ano 29. São Paulo: Ed. RT, novembro 2021, p. 141).

Desse modo, à vista das especificidades inerentes a essa seara, a LGPD, no que importa para os fins da temática em exame, deixou o tratamento da matéria concernente à segurança pública e às atividades de investigação e repressão de infrações penais, a cargo de legislação específica. Sem embargo, conforme já explicitado, cuidou de fixar os parâmetros a serem seguidos no bojo da referida legislação, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular estabelecidos por aquele diploma.

Sob tal perspectiva,[20] foi instituída, por ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019, uma Comissão de Juristas,[21] que apresentou o anteprojeto, conhecido como "LGPD Penal", dispondo sobre a proteção e o tratamento dos dados pessoais no contexto da segurança pública e persecução penal.

A Comissão de Juristas foi presidida por Nefi Cordeiro e teve como vice-presidente Antonio Saldanha Palheiro, contando, ainda, com os seguintes membros: Laura Schertel Mendes (relatora), Pedro Ivo Velloso (secretário), Danilo Doneda, Davi Tangerino, Eduardo Queiroz, Heloisa Estellita, Humberto Barrionuevo Fabretti, Ingo Sarlet, Jacqueline

17. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo, *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons. 1. ed. 2021, p. 162.

18. Na seara do direito penal, "o devido processo legal, a presunção de inocência, a mínima intervenção, a justa causa para a persecução penal, entre outros direitos já assegurados se relacionam diretamente com o âmbito subjetivo da autodeterminação informativa, na medida que ele confere uma maior proteção à utilização de dados quanto maior for o risco de violação dos direitos individuais". (FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*. vol. 185. ano 29. São Paulo: Ed. RT, novembro 2021, p. 147).

19. Conforme pontuado na exposição de motivos do Anteprojeto da LGPD Penal, "trata-se de um mandamento legal para legislar sobre a matéria, a partir da constatação de que está sujeita a ponderações específicas sobre o uso de dados pessoais e que expressa reivindicação da sociedade e das autoridades competentes para regulação do tema, surgida no processo de debate da própria LGPD" (Disponível em: <https://bit.ly/3wf2kdc>, acesso em 15/03/2022).

Abreu, Jorge Octávio Lavocat Galvão, Juliana Abrusio, Tércio Sampaio Ferraz Júnior e Vladimir Aras.

Sintetiza a Exposição de Motivos do Anteprojeto que restou consolidada uma base principiológica, alinhada à LGPD, capaz de conformar todas as etapas e as cadeias do tratamento de dados pessoais no âmbito da investigação:

> No ponto, o artigo 6º, do anteprojeto, elenca uma série de princípios, os quais, em síntese, vinculam o seguinte conteúdo: (I) licitude: embasamento do tratamento em hipótese legal; (II) finalidade: fins devem ser legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; (III) adequação: pertinência do tratamento com suas finalidades; (IV) necessidade: o dados devem ser o mínimo suficiente para consecução dos objetivos do tratamento; (V) proporcionalidade: compatibilidade do tratamento com seus objetivos; (VI) livre acesso: garantia de facilidade e gratuidade aos titulares ao acesso às informações do tratamento de seus dados; (VII) qualidade dos dados: garantia aos titulares de dados de exatidão, clareza, relevância e atualização dos seus dados; (VIII) transparência: garantia aos titulares de informações claras, precisas e acessíveis sobre o tratamento e seu responsável; (IX) segurança: utilização de medidas técnicas e administrativas para a não violação de dados; (X) prevenção: adoção de medidas de prevenção de violações; (XI) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (XII) responsabilização e prestação de contas: demonstração de medidas que comprovem a observância e a eficácia das normas de proteção de dados.

Ao lado da LGPD, da Lei das Interceptações Telefônicas (Lei 9296/1996), da Lei do Marco Civil da Internet (Lei 12.965/2014), do disposto no Código Penal, no Código de Processo Penal e em outras leis extravagantes, o anteprojeto vem a integrar um verdadeiro microssistema que disciplina a proteção de dados pessoais no sistema de justiça criminal.

6. REFLEXÕES SOBRE O PAPEL ATRIBUÍDO AO CONSELHO NACIONAL DE JUSTIÇA NO ANTEPROJETO DA LGPD PENAL: UMA ANÁLISE CRÍTICA

O Anteprojeto da LGPD Penal alçou o Conselho Nacional de Justiça à condição de autoridade destinada à aplicação, supervisão e monitoramento (*enforcement*) da lei em todo o território nacional, por intermédio de uma unidade específica a ser, em tese, edificada, denominada Unidade Especial de Proteção de Dados em Matéria Penal – UPDP.

A opção eleita pelo anteprojeto foi diversa da LGPD, que instituiu, para a função de Autoridade Nacional de Proteção de Dados – ANPD, um órgão da administração pública federal, integrante da Presidência da República, que poderá ser transformado, em até 2 (dois) anos da data da entrada em vigor da estrutura regimental, em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.[22]

20. Considerou-se, na oportunidade, a par da previsão expressa contida no artigo 4º, parágrafo 1º, da LGPD, que "os órgãos de segurança pública e de investigação e repressão de infrações penais não podem prescindir de uma legislação que assegure a circulação de dados pessoais entre autoridades, ao mesmo tempo em que se observa a tendência de que mecanismos de cooperação internacional em matéria criminal exijam práticas de proteção de dados" e que "os dados pessoais traduzem projeção da personalidade do indivíduo, seu tratamento por meio de ferramentas de tecnologia da informação deve sempre observar a preservação da privacidade dos cidadãos, tanto o mais quando o risco recai sobre o *status libertatis*" (Disponível em: https://bit.ly/3wb05Lo, acesso em 15/03/2022).

21. Disponível em: https://bit.ly/3wb05Lo, acesso em 15/03/2022.

Erigido ao *status* de autoridade nacional pelo anteprojeto da LGPD Penal,[23] a exposição de motivos explica que a escolha do Conselho Nacional de Justiça para a função deu-se "em razão da sua autonomia e da pluralidade de sua composição".

Ponderou-se, na oportunidade, que "a autonomia e imparcialidade do órgão supervisor é fundamental para que um país esteja apto a pleitear uma decisão quanto à adequação de sua legislação de proteção de dados ao nível de proteção europeu, que permitiria às autoridades de investigação no país acessar e compartilhar uma maior quantidade de dados com autoridades e instituições europeias, como Europol, Interpol e Eurojust".

Justificou-se, ainda, que a indicação do CNJ como órgão supervisor é importante na medida em que:

< I > evita o dispêndio de novos gastos com a criação de um órgão específico;

< II > aproveita a expertise dos setores, dos Conselheiros e dos servidores do CNJ que já vêm expedindo atos normativos importantes sobre a proteção de dados no âmbito brasileiro (v.g. Recomendação CNJ n. 73, de 20/08/2020 e Portaria CNJ n. 63/2019); e

< III > permite a formulação de políticas públicas uniformes para todo território nacional, a partir de uma composição plural e independente com membros de instituições diversas à luz do art. 103-B, da Constituição Federal (v.g. Poder Judiciário estadual, federal e trabalhista, Ministério Público estadual e federal, Ordem dos Advogados do Brasil, Câmara dos Deputados e Senado Federal).

22. N/E: Em 13 de junho de 2022, foi publicada e Medida Provisória do Presidente Jair Bolsonaro, propondo a conversão da ANPD em autarquia federal independente. A MP segue em apreciação pelo Congresso Federal. Acessível em: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.124-de-13-de-junho-de-2022-407804608.

23. Disponível em: https://bit.ly/3wf2kdc, acesso em 15/03/2022.

O anteprojeto fixou à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) incumbências, a serem exercidas no âmbito da segurança pública e persecução penal, nos seguintes termos:

> Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):
>
> < I > zelar pela proteção dos dados pessoais na segurança pública e persecução penal, nos termos da legislação;
>
> < II > fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> < III > apreciar petições de titular contra o controlador no prazo estabelecido em regulamentação;
>
> < IV > promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais na segurança pública e persecução penal;
>
> < V > promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais na segurança pública e persecução penal;
>
> < VI > promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
>
> < VII > solicitar, a qualquer momento, às autoridades competentes submetidas a esta lei informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
>
> < VIII > editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade na segurança pública e persecução penal;

< IX > solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco aos direitos previstos nesta Lei;

< X > ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

< XI > realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais efetuado pelas autoridades competentes;

< XII > comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

< XIII > comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei pelas autoridades competentes;

< XIV > implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; e

< XV > elaborar relatórios de gestão anuais acerca de suas atividades.

A amplitude das atribuições a serem exercidas, à luz do Anteprojeto, pela Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) evidenciam, desde logo, que as atividades desenvolvidas no âmbito da segurança pública e persecução penal envolvem muitos atos de compartilhamento de dados pessoais.

O tema é candente e, por certo, não faltam questões passíveis de discussão, a exemplo do risco de redução da eficiência estatal no enfrentamento à criminalidade ou do desenvolvimento e implantação de ferramentas de inteligência artificial, em decorrência da instituição de mecanismos de controle da persecução penal com vistas à proteção da privacidade e autodeterminação informacional.

Para além dessas relevantes questões, não há olvidar, entretanto, que, em que pese a opção eleita pela Comissão de Juristas, o Conselho Nacional de Justiça não foi originariamente criado para a função de autoridade controladora de dados. Incumbe-lhe, com efeito, nos termos do artigo 103-B, parágrafo 4º, da Constituição Federal, o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes.

A esfera de atuação do Conselho Nacional de Justiça, assim, diz respeito exclusivamente à atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes, não podendo, portanto, ser ampliada, para além dos órgãos do Poder Judiciário e seus serviços auxiliares, de modo a irradiar efeitos sobre os órgãos de segurança pública e da polícia judiciária.[24]

O Anteprojeto da LGPD Penal atribuiu à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) incumbências, a serem exercidas no âmbito da segurança pública e persecução penal, dentre as quais podem ser citadas, exemplificativamente, a de zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções, apreciar petições de titular contra o controlador, promover ações de cooperação nacional e internacional, editar regulamentos e procedimentos, realizar ou determinar a realização de auditorias, implementar mecanismos simplificados para o registro de reclamações sobre o tratamento de dados pessoais e elaborar relatórios de gestão anuais acerca de suas atividades, dentre outros tantos que, conforme já assinalado, parecem não se amoldar, propriamente, às competências constitucionais atribuídas ao Conselho Nacional de Justiça.

24. Confira-se, neste aspecto, exemplificativamente, o teor do art. 62, II do Anteprojeto, ao incumbir o Conselho Nacional de Justiça de fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso.

É importante ressaltar, por outro lado, que o exercício de tais incumbências demandaria uma importante reestruturação, ampliando-se a retaguarda material e funcional no âmbito do CNJ, de modo a abarcar as novas atribuições.

Registra-se, neste aspecto, que a Autoridade Nacional de Proteção de Dados, é atualmente integrada, em sua estrutura organizacional vertida no Decreto legislativo n. 10.474, de 26 de agosto de 2020, pelos seguintes órgãos: I. Conselho Diretor; II. órgão consultivo: Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - órgãos de assistência direta e imediata ao Conselho Diretor: a) Secretaria-Geral; b) Coordenação-Geral de Administração; e c) Coordenação-Geral de Relações Institucionais e Internacionais; IV - órgãos seccionais: a) Corregedoria; b) Ouvidoria; e c) Assessoria Jurídica; e V - órgãos específicos singulares: a) Coordenação-Geral de Normatização; b) Coordenação-Geral de Fiscalização; e c) Coordenação-Geral de Tecnologia e Pesquisa.

Esse ponto é de extrema relevância, na exata medida em que, sendo necessária, para o exercício das atribuições de Unidade Especial de Proteção de Dados em Matéria Penal, a ampliação da estrutura organizacional do Conselho Nacional de Justiça, edificada ao logo de mais de quinze anos de existência e devidamente alicerçada em seu regimento interno, cai por terra a justificativa, constante da exposição de motivos do Anteprojeto, relativa à ausência de dispêndio de novos gastos com a criação de um órgão específico.

Outrossim, a autonomia técnica e decisória conferida pelo parágrafo 1º do art. 60 da LGPD Penal à cogitada Unidade Especial de Proteção de Dados em Matéria Penal desponta, a princípio, incompatível com o controle que o Plenário do Conselho Nacional de Justiça exerce sobre o ato de seus órgãos internos.[25]

25. Ponto questionado na nota técnica oferecida pela LAPIN – Laboratório de políticas públicase internet (https://bit.ly/2Wurc1k).

Nota-se, ainda, que, a par das competências atribuídas à Unidade Especial de Proteção de Dados em Matéria Penal no capítulo próprio (capítulo X), o anteprojeto atribui ao Conselho Nacional de Justiça, em dispositivos esparsos, outras tantas, a exemplo do recebimento de informes (artigos 10, 13, § 3º do art. 20, § 1º do art. 23 e 49) e o estabelecimento de procedimento simplificado para a tomada de decisão sobre o nível de adequação de um país, quando este for um Estado Parte da Convenção do Conselho da Europa, de 1981 e de seus protocolos, atividades que, de igual modo, parecem superar os restritos limites da sua esfera constitucional de atuação.

Nessa medida, os poderes que foram outorgados ao Conselho Nacional de Justiça pelo poder constituinte derivado não se compatibilizam com o desempenho das funções de aplicação, supervisão e monitoramento da LGPD Criminal.

7. CONSIDERAÇÕES FINAIS

Conquanto suas competências constitucionalmente atribuídas não abarquem a função de autoridade controladora de dados, não há olvidar que, na condição de órgão do Poder Judiciário, o Conselho Nacional de Justiça ostenta condições de contribuir – e certamente o fará, tal como, aliás, já vem procedendo, conforme detalhado no item "3" supra – com todas as medidas necessárias, pertinentes à respectiva esfera de atuação, observados os limites dos poderes que lhe foram constitucionalmente outorgados, para a fiel observância da futura lei em todo o território nacional.

Com efeito, a expertise desenvolvida na função regulatória e no direcionamento das atividades que já estão em andamento visando a adequação dos órgãos do Poder Judiciário e seus serviços auxiliares às diretrizes da LGPD, demonstram que o Conselho Nacional de Justiça, não no papel de Autoridade

Nacional, mas no rigoroso exercício das competências que constitucionalmente lhe foram outorgadas, contribuirá com a implementação da futura LGPD Criminal no país.

Afinal, a evolução tecnológica, cada vez mais sofisticada, impacta todos os segmentos e cumpre ao sistema jurídico a adequação de seus mecanismos à garantia do exercício dos direitos fundamentais aos titulares de dados pessoais, especialmente no que concerne à intimidade, privacidade e dignidade da pessoa humana.

Não é demais lembrar que, para além da efetividade do processo, a eficiência no combate à criminalidade, aliada à segurança jurídica inerente à tutela legal ao direito à autodeterminação informacional, produz reflexos no ambiente de negócios e, por conseguinte, na economia e no crescimento do país. E essa deve ser, de fato, a resultante de uma proposição legal a ser objeto de salutar debate pela comunidade acadêmica.

8. REFERÊNCIAS BIBLIOGRÁFICAS.

FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*. vol. 185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro 2021.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo, O direito de proteção de dados no processo penal e na segurança pública. Rio de Janeiro: Marcial Pons. 1. ed. 2021.

LAPIN, Laboratório de Políticas Públicas e Internet, Nota Técnica sobre o anteprojeto de lei de proteção de dados para a segurança pública e investigação criminal. Disponível em: https://bit.ly/2Wurc1k

ATOS NORMATIVOS

CÂMARA DOS DEPUTADOS. Ato do Presidente, de 26 de novembro de 2019. Disponível em: https://bit.ly/3wb05Lo

_____, Comissão de Juristas. Exposição de Motivos. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em: https://bit.ly/3wf2kdc

CONSELHO NACIONAL DE JUSTIÇA, 15º Encontro do Poder Judiciário, Diretrizes Estratégica para 2022, propostas pela Corregedoria Nacional. Disponível em: https://bit.ly/3u5eJ08

_____, Portaria n. 63, de 26 de abril de 2019. Disponível em: https://bit.ly/3KSTQg5

_____, Portaria n. 212/2020, 15 de outubro de 2020. Disponível em: https://bit.ly/3Jg7J7n

_____, Recomendação n. 73/2020, de 20 de agosto de 2020. Disponível em: https://bit.ly/3Jg7J7n

_____, Resolução n. 363/2021, 12 de janeiro de 2021. Disponível em: https://bit.ly/3q9r7vv

CORREGEDORIA NACIONAL DE JUSTIÇA, Portaria 60/2020, de 18 de dezembro de 2020. Disponível em: https://bit.ly/363HEKr

05.

AUTORIDADE DE PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA: REFLEXÕES SOBRE O CNJ

Laura Schertel Mendes

Muito obrigada, Artur. Queria em primeiro lugar cumprimentar você, a ministra Maria Thereza e o doutor Renato De Vitto, e dizer que é um prazer e uma alegria muito grande poder compartilhar esse painel com todos num tema tão desafiador, como bem explanou a ministra Maria Thereza. Queria também agradecer ao InternetLab por esse convite e parabenizá-los por mais um congresso sobre esse tema tão relevante e para o qual ainda temos tantas lacunas. Então, acho que esse é o grande objetivo do debate.

Eu queria, muito rapidamente, falar um pouco da própria lógica, o porquê desse anteprojeto, para em seguida falar sobre por quê o CNJ acabou sendo escolhido nessa comissão como uma autoridade. E, nesse sentido, dialogar um pouco com o que a ministra Maria Thereza trouxe.

Como todos nós sabemos e temos discutido ao longo desses anos, o InternetLab tem feito um enorme trabalho e tem sido uma liderança nessa área. Nós temos hoje uma grande lacuna em termos de proteção de dados no Brasil para a área criminal e para a área de segurança pública. Isso porque, embora a Lei Geral de Proteção de Dados tenha sido aprovada, e a Autoridade Nacional de Proteção de Dados tenha sido criada, fato é que a lei não se aplica a essa esfera, porque a própria Lei Geral de Proteção de Dados indicou que uma lei específica trataria desses temas.

E foi em razão disso que o então presidente da Câmara dos Deputados, deputado Rodrigo Maia, criou essa comissão de juristas presidida pelos ministros Nefi Cordeiro e Antonio Saldanha, comissão na qual tive a honra de ser relatora. Nós tivemos cerca de um ano e meio de trabalho, e não foi uma tarefa fácil criar esse anteprojeto, que foi chamado de "LGPD Penal". Vale a pena lembrar que a gente chama de anteprojeto porque ainda não foi apresentado formalmente por nenhum congressista.

Então é um anteprojeto ainda, e inclusive espero que nossos debates possam incentivar essa discussão no âmbito da Câmara dos Deputados e do nosso Congresso brasileiro, exatamente para que um projeto venha a ser de fato proposto e ele possa tramitar, e para que a gente possa ter esse debate, digamos, legislativo, já em âmbito oficial. Acho que isso seria muito importante.

E por que eu sempre falo muito dessa lacuna, por que isso é uma lacuna? O que nós temos hoje, e eu sempre gosto de citar as palavras da nossa querida Jacqueline Abreu, que também já foi do InternetLab, no âmbito criminal e penal, é um direito relativo ao sigilo, ao segredo. No fim, é um direito à quebra do sigilo. Isso nós temos em várias leis, a Lei de Interceptação Telefônica talvez seja a principal delas. Então, o que nós temos hoje no Brasil é uma proteção em relação a esse sigilo e aos momentos de sua quebra. O que nós não temos é uma regulação geral sobre os dados pessoais, de como esses dados fluem no âmbito criminal e no âmbito da segurança pública.

Isso significa que todos os dados que não estão protegidos pelo sigilo, seja pela Constituição Federal, seja pelo Código Penal, seja por leis especiais ou mesmo pelo Código de Processo Penal, a gente não tem uma proteção em relação a esses dados. Talvez o maior exemplo em relação a isso sejam as várias reportagens mostrando como diversas pessoas têm sido presas com base em fotos que estavam na delegacia e ninguém sabe como essas fotos foram parar lá. Pessoas, muitas vezes, sem nenhum antecedente criminal.

Até entendo que hoje a gente tem essa proteção garantida em termos constitucionais em razão do direito fundamental reconhecido pelo Supremo Tribunal Federal e ontem aprovado, como a ministra aqui trouxe para todos nós, na Câmara dos Deputados, discussão que agora vai para o Senado. Esse

direito fundamental à proteção de dados certamente abrange todas as áreas.

É claro que a área criminal não está excluída desse direito fundamental, mas em termos legais infraconstitucionais nós não temos uma regulação geral que proteja dados não sigilosos, dados não sensíveis, e eu diria que toda essa teoria, toda a história da proteção de dados desde a década de 70 na Europa, nos Estados Unidos e já há mais de uma década no Brasil, vem nos mostrar que são exatamente dados não sensíveis, não sigilosos e aparentemente insignificantes que podem, sim, ter uma posição muito relevante na hora que os juntamos, quando fazemos uma análise e cruzamos esses dados, ou quando os analisamos em diversos contextos - e eles podem trazer informações muito relevantes sobre as pessoas.

E é claro que isso também é utilizado no âmbito criminal com efeitos muito mais graves para o indivíduo do que os prejuízos econômicos ou a vigilância que a gente já encontra, e são riscos que visam ser enfrentados pela LGPD. Então, o que nós temos hoje, pensando na área criminal, é essa grande lacuna em que não há uma regulação sobre todos os dados que não são sensíveis e que não são sigilosos.

E essa certamente é uma grande lacuna, seja para o cidadão, em especial porque o risco é grande - no fim o que está em jogo é a sua própria liberdade - mas também para o próprio Estado que, como a ministra Maria Thereza trouxe, de fato encontra dificuldades na relação com outros países, porque não consegue fazer uma cooperação jurídica plena, exatamente porque nós não temos hoje uma proteção de dados robusta nesse âmbito. Então, eu acho que essa lacuna traz prejuízos muito claros, tanto para o cidadão quanto para o próprio Estado investigador, o Estado da persecução criminal.

Dada essa introdução, a comissão de juristas, inclusive, teve muitos integrantes de diversas universidades do país

/ TEMOS O FATO DE QUE O CNJ NÃO ESTÁ SUBORDINADO A NENHUM OUTRO ÓRGÃO, ENTÃO ESSA INDEPENDÊNCIA TAMBÉM NOS CHAMOU MUITO A ATENÇÃO /

todo, além de membros tanto do Ministério Público Federal quanto do Ministério Público Estadual. E aí, chegamos talvez num dos pontos mais relevantes da discussão: a lei precisa de um órgão supervisor, isso é fundamental. É da natureza da proteção de dados constituir um órgão supervisor. Então, nos deparamos com vários argumentos trazidos pelos integrantes e que foram levados em consideração para construir a solução de uma unidade especial de proteção de dados, que viesse a ser constituída no âmbito do CNJ.

Ministra, nós sabíamos que essa proposta era desafiadora e polêmica. Mas, como a senhora e todos que nos ouvem sabem (e o doutor Renato, certamente), ela não é fácil. Tivemos também a Defensoria representada na comissão, e não é fácil conseguir um consenso nessas condições tão plurais, ainda mais com um tema tão complexo, e ainda não tão debatido no Brasil.

Então, acho que o primeiro ponto levantado foi de fato: hoje temos uma Autoridade Nacional de Proteção de Dados. A sua estrutura é muito diferente daquela que foi idealizada por todos nós que trabalhamos na aprovação da Lei Geral de Proteção de Dados nessa última década. Eu trabalhei [nisso] desde de o início, lá em 2010, 2009, e de fato a gente sempre idealizou - e eu vejo isso em todos os setores (academia, setor privado) - uma autoridade independente, uma autarquia verdadeiramente dita, que pudesse ser constituída talvez nos moldes das agências reguladoras (ex.: do próprio Cade). Mas por diversas circunstâncias políticas, não foi isso que aconteceu.

A autoridade acabou sendo, na verdade, política e jurídica. Houve toda aquela discussão de que havia uma inconstitucionalidade formal na versão final aprovada com a relatoria do Deputado Orlando Silva, [a versão] foi vetada pelo então presidente Michel Temer, e foi recriada por meio de uma medida provisória.

Mas, nessa sua recriação, ela não foi recriada como uma autarquia, mas, sim, como um órgão dentro da Presidência da República. E isso traz vários problemas, especialmente por ser um órgão vinculado hierarquicamente à própria Presidência, e que, portanto, não traz a independência que todos nós esperamos e que consta nos documentos internacionais relacionados à proteção de dados.

Então, nós sabemos que tanto a OCDE quanto o próprio Conselho da Europa, o GDPR, todos esses textos e diretrizes mais importantes, sempre trouxeram a relevância de termos uma autoridade independente de proteção de dados, e nessa área criminal acho que isso fica mais evidente porque a gente pode ter interesses do governo em determinadas investigações criminais e isso poderia vir a gerar conflitos de interesse com a área de proteção de dados. Então, a discussão da independência, da autonomia, é muito relevante. Eu diria, na proteção de dados de uma forma geral, mas nesta área tão sensível como a investigação criminal, [a discussão] é ainda mais relevante, e acho que isso foi um ponto que foi muito discutido e foi levado em conta pela comissão de juristas.

Outro ponto também, que a ministra Maria Thereza trouxe com muita precisão, foi exatamente a discussão sobre a ideia de se constituir uma lei, uma estrutura normativa e institucional, e se isso também diz respeito à possibilidade de que o Brasil possa trocar dados com outros países, para que a gente possa ter de fato um fluxo de dados, uma cooperação maior. E, de novo, também nesse ponto, uma autoridade não independente poderia trazer problemas para o reconhecimento de uma adequação ou para uma cooperação mais robusta que pudesse vir a ser feita entre o Brasil e outros países, como por exemplo Eurojust, Interpol, etc.

Talvez o terceiro e último motivo que vale a pena também mencionar, que foi trazido em especial pelos Ministérios Públi-

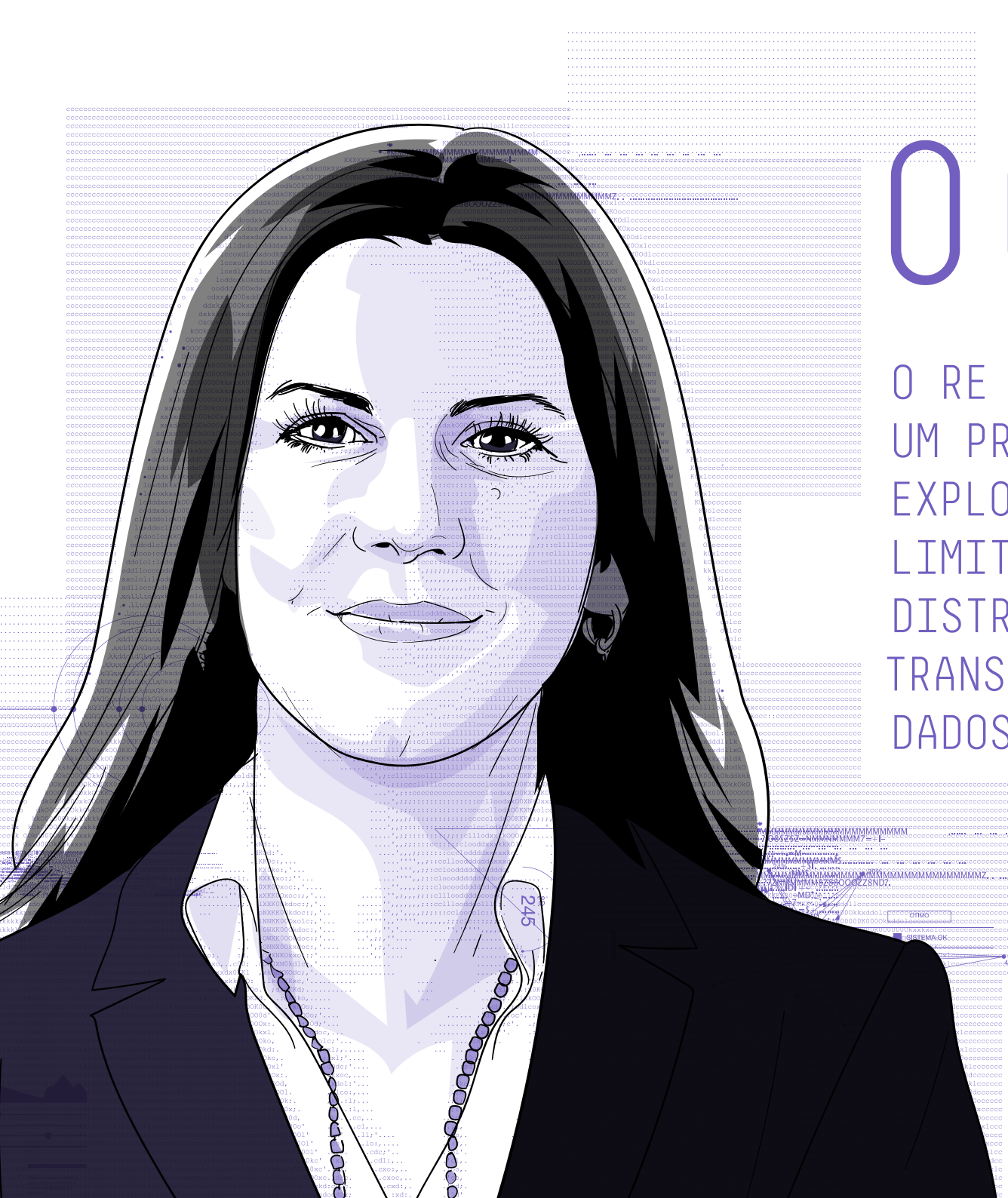
cos, Federal e Estadual, foi um certo incômodo de se submeter a uma autoridade do [Poder] Executivo, mais uma vez tocando na questão da independência [dos poderes], e o fato d[a Autoridade] ser um órgão [de outro Poder] também foi trazido à tona.

Por todos esses motivos, apesar de sabermos que não era a solução mais óbvia e certamente era muito desafiadora, encontramos no CNJ uma instituição plural, composta por muitos membros de diferentes setores e poderes. Além disso, temos o fato de que o CNJ não está subordinado a nenhum outro órgão, então essa independência também nos chamou muito a atenção, e foi por todos esses motivos que [ele] foi colocado [como órgão competente à atuação como autoridade reguladora].

Já chegando ao fim da minha fala, entendo que a ideia foi trazer uma discussão inicial e trazer a público um texto que pudesse ser discutido, criticado e analisado. Inclusive, entendo que quando [o anteprojeto] vier a ser proposto, isso vai merecer uma discussão formal, eventualmente com o próprio CNJ, para reavaliarmos a decisão na posição legislativa. Esse é um ponto importante.

Acho que não tem absolutamente nenhuma decisão [sobre o anteprojeto] que esteja firmada. Muito pelo contrário, foi de fato uma proposta que foi colocada para o público e para todos, em especial ao próprio CNJ, para que pudesse ser debatida e discutida a sua viabilidade. O que vejo hoje na fala de alguns diretores da Autoridade Nacional de Proteção de Dados é que essa discussão sobre a autonomia tem sido feita no âmbito da própria ANPD, e que poderia inclusive vir a ser feita também um projeto de lei para tornar a ANPD autônoma no formato de uma autarquia.

Acho que isso também poderia trazer uma maior tranquilidade para revermos nossos caminhos. Então, há uma série de questões a serem consideradas, inclusive essa. Mas eu queria saudar novamente esse debate, que acho muito importante, e acima de tudo queria que esses eventos e debates pudessem viabilizar uma proposição formal de um projeto de lei de proteção de dados na área criminal que pudesse sanar essas lacunas das quais tanto falamos. Muito obrigada por poder participar dessa discussão, Artur, e agradeço ao InternetLab, à ministra e à generosidade de todos os comentários, e também ao Doutor Renato, certamente a gente pode ter um debate muito interessante aqui ainda. Muito obrigada.



06.

O RE 1.055.941: UM PRETEXTO PARA EXPLORAR ALGUNS LIMITES À TRANSMISSÃO, DISTRIBUIÇÃO, COMUNICAÇÃO, TRANSFERÊNCIA E DIFUSÃO DE DADOS PESSOAIS PELO COAF[1]

Heloisa Estellita

1. Texto previamente publicado na Revista de Direito Público, Volume 18. Dossiê - Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal. n. 100, 606-636, out./dez. 2021

I INTRODUÇÃO: A MATÉRIA DISCUTIDA NO STF NO RE 1.055.941

Em dezembro de 2019, o Supremo Tribunal Federal (STF), ao decidir, com repercussão geral, as controvérsias a ele submetidas no Recurso Extraordinário 1.055.941, estabeleceu (1) ser "constitucional o compartilhamento dos relatórios de inteligência financeira da UIF (...) com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional"; e (2) que o "compartilhamento pela UIF (...) 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".[2]

O ponto central era saber se a revelação de informações sigilosas (financeiras) pelo Conselho de Controle de Atividades Financeiras (doravante, COAF) às autoridades de persecução penal por meio dos relatórios de inteligência financeira (RIFS) necessitaria ou não de autorização judicial prévia.[3] A resposta foi negativa, pois haveria permissão legal para isso (art. 15, Lei 9.613/98 [Lei de Lavagem de Dinheiro, adiante LLD]).

O tribunal também apreciou as modalidades de relatórios de inteligência financeira: espontâneos (de ofício ou de disseminação espontânea) ou "por encomenda" (disseminação a pedido), muito embora não tenha se formado maioria para que pudesse cravar uma posição sobre a admissibilidade deste último (Borges, 2021, p. 85),[4] tendo os Ministros ao menos concordado quanto à "proibição da realização pelo COAF de investigações criminais prospectivas (e.g. *fishing expeditions*)" (Borges, 2021, p. 90).

A discussão envolvia, essencialmente, dois diplomas legais: a LLD e a Lei Complementar 105/2001 (adiante LC 105). Lembremos que, em dezembro de 2019, quando a decisão foi proferida, nem a Lei 13.709/2018 (Lei Geral de Proteção de Dados, LGPD) estava em vigor, nem mesmo o STF tinha julgado as ADIS ns. 6.387 MC-Ref/DF, 6.388 MC-Ref/DF, 6.389 MC-Ref/DF, 6.390 MC-Ref/DF e 6.393 MC-Ref/D, nas quais veio a reconhecer, em maio de 2020, que "o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos".[5] Tampouco a PEC 17/2019, que inclui a proteção de dados pessoais no rol dos direitos fundamentais, tinha sido aprovada.

Isso ajuda a explicar a razão pela qual na discussão a Corte não se fez uso, de forma geral,[6] da gramática da proteção de dados pessoais, que viria a ser incorporada com mais força em seu discurso a partir de 2020. Uma outra explicação se deve, evidentemente, à exclusão, do âmbito de regência da LGPD, do tratamento de dados pessoais "realizado para fins exclusivos de (...) segurança pública" ou de "atividades de investigação e repressão de infrações penais" (art. 4º, III, LGPD).

Fixado esse contexto, pretendo analisar de uma forma um pouco mais ampla a questão empregando a dogmática dos direitos fundamentais – especialmente do direito fundamental à proteção de dados pessoais – cujos elementos

2. Ementa do acórdão proferido pelo STF no RE 1.055.941, Tribunal Pleno, Rel. Min. Dias Toffoli, julgado em 04/12/2019, DJe 06/10/2020. O tema não era objeto de discussão na formulação originária do RE (cf. fl. 2699).

3. STF, RE 1.055.941, fl. 2706.

4. Neste artigo, o autor faz um exame exaustivo das questões debatidas no julgamento do RE.

5. STF, ADI 6.387 MC-Ref, Tribunal Pleno, Min. Rosa Weber, DJe 12/11/2020 (julgado em 07/05/2020). Um exame detalhado em Souto, Rosal, 2021.

6. A exceção fica por conta do voto do Min. Gilmar Mendes que contém tópico dedicado ao direito fundamental à privacidade e o sigilo de dados bancários e fiscais (fls. 3043 e ss.).

centrais são a imposição de um dever de abstenção do Estado frente a direitos fundamentais e a exigência de que as intervenções sejam veiculadas por lei autorizativa proporcional.

A intenção não é fazer uma crítica *ex post facto* – o que seria injusto –-, mas ampliar o olhar, examinando o rendimento da aplicação dessa dogmática à matéria examinada[7]. Essa ampliação é necessária na medida em que o COAF não trata apenas dados pessoais *sigilosos*, como os financeiros, mas também (muitos) dados pessoais não protegidos por sigilo, como, por exemplo, os dados pessoais relativos a transações com joias, imóveis etc.[8] O assento constitucional dessa gramática e sua aplicação *específica* à proteção de dados na esfera penal foi desenvolvida entre nós, recentemente, por Greco (2019) e por Gleizer, Montenegro e Viana (2021), de cujas premissas partirei.

O trabalho se divide em duas grandes partes: premissas e consequências. Na primeira, serão abordadas as ferramentas normativas e dogmáticas necessárias para enfrentar a questão das comunicações feitas pelo COAF. Na segunda, essas ferramentas serão empregadas para abordar especificamente as comunicações do COAF para autoridades competentes.

II AS PREMISSAS

As atividades desempenhadas pelo COAF no tratamento de dados pessoais intervêm em direitos fundamentais e têm a finalidade de convocar o aparato penal contra pessoas suspeitas da prática de infrações penais, que poderão dar ensejo a uma segunda intervenção em direitos fundamentais da mais alta gravidade. Por estas razões, o ponto de partida da análise deve ser o da teoria dos direitos fundamentais (Greco, 2019, p. 30 ss.) ou da dogmática constitucional da proteção de dados (Gleizer, Montenegro, Viana, 2021, p. 11 ss.; Greco, Gleizer, 2019, p. 1485-1488).

1 PROTEÇÃO DE DIREITOS FUNDAMENTAIS: LEGALIDADE E PROPORCIONALIDADE

A) DEVER DE ABSTENÇÃO E EXIGÊNCIA DE NORMAS AUTORIZATIVAS

Direitos fundamentais são, em primeiro lugar, direitos de defesa dirigidos contra o Estado: a um direito fundamental corresponde um dever do Estado de se abster de intervir em seu âmbito de proteção.[9] Sendo a regra a abstenção e a exceção a intervenção, toda intervenção em direito fundamental tem de ser justificada. Essa justificação se assenta em três pressupostos: um formal e dois materiais. A intervenção tem de ser veiculada em lei em sentido formal, ou seja, uma autorização democrática dada pelo legislador por meio de uma norma autorizativa como exige, entre nós, o artigo 5º, II, CF;[10] "não pode atingir o núcleo dos direitos fundamentais" (Greco, Gleizer, 2019, p. 1487), e, finalmente, tem de ser proporcional, ou seja, idônea, necessária, adequada e proporcional em sentido estrito para a promoção de um fim legítimo.[11]

Dentre esses pressupostos, chamo a atenção para o primeiro, pois, segundo adverte Greco, "até hoje não descobrimos todo o potencial desse dispositivo [o art. 5º, II, CF] (...) [um] verdadeiro gigante adormecido" (2019, p. 36).[12] A exigência

7. Já em 1991, ou seja, há 30 anos (!), *Rogall* identificava o efeito que o direito constitucional e o direito de proteção de dados passaram a ter no fortalecimento dos direitos fundamentais dos afetados por investigações e ações penais (Rogall, 1991, p. 907).

8. Serão considerados dados inanceiros sigilosos aqueles disciplinados na LC 105. Muitas das pessoas obrigadas a comunicar operações em espécie e suspeitas ao COAF (art. 9º, LLD) não estão abarcadas pelo espectro de proteção do sigilo financeiro estabelecido pelo art. 1º da LC 105, cujo critério de proteção não é a natureza dos dados, mas quem os trata: as instituições financeiras.

9. Greco, 2019, p. 35; Gleizer; Montenegro; Viana, 2021, p. 103, 118–123; Dimoulis, Martins, 2021, p. 179 ss.

10. CF, art. 5º, II: "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".

11. Greco, 2019, p. 36; Gleizer, Montenegro, Viana, 2021, p. 49 ss.;

de reserva legal "significa que, sem lei específica que preveja de forma relativamente clara a intervenção e lhe imponha limites materiais e procedimentais, não será lícito intervir no direito fundamental" (Greco, 2019, p. 37).[13] Exige-se, assim, que a intervenção seja autorizada em lei em sentido formal que a veicule de forma precisa, sendo vedada sua extensão a hipóteses nela não previstas.[14]

12. No mesmo sentido, Gleizer, Montenegro, Viana, 2021, p. 41.

13. Também Silva, 2021, p. 119–120.

14. Greco, Gleizer, 2019, p. 1487. Sobre intervenções bagatelares e autorizações veiculadas por meio de cláusulas gerais, cf. Greco, 2019, p. 39-40; Gleizer, Montenegro, Viana, 2021, p. 48, 85-86, 97-99, com ulteriores referências.

B) NORMAS AUTORIZATIVAS E NORMAS DE COMPETÊNCIA (ATRIBUIÇÃO)

E é neste ponto que a distinção entre normas *autorizativas* e normas de *competência*[15] mostra toda sua importância. Nesse sentido, quando fixa competências, "o Estado simplesmente distribui entre os seus o que incumbe a quem. Parece claro, contudo, que uma distribuição interna de tarefas não dá a ninguém um direito de adentrar na esfera de um terceiro", o que exige, como visto, autorização clara e taxativa. Do que decorre que não se pode "derivar da existência de uma competência uma autorização" (Greco, 2019, p. 37-38).

Greco assim exemplifica essa diferença: "incumbe ao Ministério Público proceder à investigação preliminar tão logo existam pontos de apoio fáticos no sentido do possível cometimento de um delito", essas "normas de competência não dão ao ministério público, contudo, o direito de intervir na esfera jurídica de quem quer que seja", se for necessária uma interceptação telefônica ou uma busca "terá de atender aos pressupostos dos dispositivos específicos que fundamentam cada uma dessas medidas, isto é, às normas autorizativas específicas" (Greco, 2019, p. 38).[16] Ajustando o exemplo ao direito positivo brasileiro, o fato de o Ministério Público ter competência para "promover, privativamente, a ação penal pública, na forma da lei" e, para isso, "requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais" (art. 129, I e VIII, CF), não autoriza seus membros a entrarem em domicílios, apreenderem objetos, interceptarem comunicações, acessarem comunicações privadas armazenadas, compartilharem dados pessoais sem autorização legal, terem acesso a dados pessoais financeiros protegidos por sigilo etc.[17] Seguindo nessa linha, o fato de "o constituinte atribuir às polícias militares a competência para exercer policiamento ostensivo e preservação da ordem pública (art. 144, § 5º, CF) não implica, automaticamente, autorização para entrada no domicílio dos cidadãos, mesmo que isso seja necessário para o exercício de tais competências" (Gleizer, Montenegro, Viana, 2021, p. 42),[18] o mesmo valendo para as atribuições que o art. 6º do Código de Processo Penal (CPP) endereça à autoridade policial quando tiver conhecimento da prática de infração penal: apreender objetos, colher provas, ouvir pessoas etc.[19]

15. Usarei o termo competência no decorrer do texto para ser fiel à escolha linguística feita por Greco, que não o limita à competência jurisdicional, mas abrange também normas que determinam as tarefas, funções e atribuições de órgãos e agentes estatais, muito embora talvez o termo atribuição fosse mais adequado ao ambiente jurídico brasileiro.

16. E acrescenta: "Isso significa que, como regra, a norma tem de prever a concreta medida interventiva, e isso não apenas por meio de uma conceituação 'funcional' (obter informações, descobrir, esclarecer etc.), que é a linguagem das normas determinadoras de tarefas ou de competências, e sim com termos mais 'naturalísticos', que descrevam o concreto meio de que as instâncias de persecução se valerão para cumprir a função que lhes é legalmente atribuída" (2019, p. 39).

17. Em sentido similar, reportando-se ao § 161 I S. 1 StPO (Código de Processo Penal alemão), que garante ao ministério público o poder de realizar diligências investigativas diante da suspeita da prática de crime ou de fazê-lo por meio da polícia, afirma Rogall que tal norma não autoriza a intervenção em direitos fundamentais, que só podem ser feitas pelo ministério público diante de normas legais de autorização veiculadas de forma clara (Rogall, 1985, p. 6-7).

18. Essa mesma dicotomia se vê no direito de polícia alemão (Greco, 2019, p. 40-41).

A força dessa verdadeira *decorrência lógica* do regime constitucional de proteção de direitos fundamentais fica clara quando pensamos que seria muito fácil atraiçoar a garantia dos direitos fundamentais do artigo 5º da CF (cláusulas pétreas) se, logo à frente, o Constituinte, por meio de meras regras de competência, negasse todo o catálogo de direitos fundamentais antes consagrados. Mais concretamente: se se entendesse que normas (ainda que constitucionais) de competência consubstanciassem uma "carta branca" aos agentes estatais para que, a pretexto de "bem" cumpri-las, por exemplo, aplicassem uma sanção penal sem o devido processo legal (art. 5º, LIV, CF) ou privassem o cidadão de parte de seu patrimônio (art. 5º, *caput* e XXII, CF), o sistema constitucional de proteção de direitos fundamentais ruiria duas ou três páginas à frente de sua consagração, pois as regras de competência se sobreporiam às normas garantidoras de direitos fundamentais. A CF traria já em seu âmago uma contradição evidente, uma espécie de *back door* para a negação dos direitos que acabara de garantir. Também o disposto no art. 60, § 4º, CF, se tornaria letra morta, inútil. Daí que, se levarmos a sério o que dispõem o art. 5º (especialmente seu inciso II[20]) e o 60, § 4º, IV, CF, a afirmação de que *de uma regra de competência (atribuição) não decorre uma norma autorizativa* é uma decorrência lógica (também) de nosso direito (constitucional) positivo.[21]

19. Manifestação clara dessa confusão no parecer oferecido pela PGR no ARE 1.042.075, em 08/10/2021, e que trata do acesso ao conteúdo de smartphone apreendido pela polícia. Ali se toma a norma de competência/atribuição do art. 6º do CPP como se fosse uma norma autorizadora de intervenção em direitos fundamentais.

20. Cf. Greco, 2019, p. 40.

21. Cf. Gleizer, Montenegro, Viana, 2021, p. 41-43, com ulteriores referências, e também Greco, 2019, p. 36-37.

C) PROTEÇÃO DE DADOS PESSOAIS

Essas ideias se aplicarão à proteção de dados pessoais, seja ela entendida como um (novo) direito fundamental, seja como uma nova forma de proteção dos direitos gerais de personalidade.[22]

Seu reconhecimento tem como marco histórico decisões tomadas pela Corte Constitucional Federal alemã,[23] que reconheceram que o livre desenvolvimento da personalidade depende do estabelecimento de limitações à obtenção, armazenamento, utilização e transferência de dados pessoais no contexto da capacidade atual de processamento, especialmente automatizado, de dados.[24] Como direito fundamental, também está sujeito a intervenções (restrições[25]), mas que devem estar previstas em lei e serem proporcionais.

É importante ter em mente que cada forma ou fase do tratamento de dados – a obtenção, o armazenamento, a utilização, a transferência etc.[26] — configura uma intervenção *autônoma* no direito à autodeterminação informacional, um direito que garante ao seu titular o controle sobre cada uso (tratamento) que é feito de seus dados. Por isso, cada forma de tratamento tem de ser objeto de autorização legal autônoma: "uma norma que autoriza a obtenção de um dado não autoriza já automaticamente a utilização ou o armazenamento, muito menos a transferência" (Greco, 2019, p. 44).[27] Ademais, esse direito dá a seu titular o poder de saber para qual *finalidade* seus dados são coletados. Como "uma *alteração de finalidade* é um ato interventivo autônomo", que necessita de expressa autorização legal (Gleizer, Montenegro, Viana, 2021, p. 50), tanto a coleta de um dado para fins de inteligência ou

22. Gleizer, Montenegro, Viana, 2021, p. 37-39, entendem que são vários os direitos conformando a proteção de dados pessoais; em sentido similar, Rogall, 1991, 926-927.

23. Sobre a origem e desenvolvimento conceitual deste direito, além das obras já citadas, cf., ilustrativamente, entre nós, Mendes, 2020. Questionamentos acerca do acerto dessa decisão ao invocar um novo direito subjetivo em Rogall, 1985, p. 11-12, e 1991, p. 919-924.

24. GRECO, 2019, p. 43.

25. Interessante o ponto de vista de Rogall no sentido de que esse direito não deve ser entendido como um domínio sobre dados, mas um direito limitado de disposição sobre informações pessoais, que pode variar de acordo com os riscos para os interesses pessoais (Rogall, 1985, p. 11-12).

26. Cf. LGPD, art. 5º, X.

segurança pública (uma finalidade), como, por exemplo, a sua transmissão e utilização para fins de persecução penal (outra finalidade) têm de estar autorizadas em lei.

D) SEPARAÇÃO INFORMACIONAL

O vínculo entre *finalidade* e *autorização* de tratamento de dados mostra toda sua força por meio da ideia de *separação informacional*. No que nos interessa, da separação entre atividades de inteligência, prevenção e persecução penais: "os dados de inteligência não podem ser usados pela polícia preventiva, os da polícia preventiva não podem ser usados repressivamente, e vice-versa, sem expressa previsão legal" (Greco, 2019, p. 45). Como a alteração de finalidade é uma nova intervenção, tem de estar prevista em lei.

Seria uma ousadia tentar, nesta oportunidade, delimitar os conceitos de *inteligência*, *segurança pública* e *persecução penal* em um ambiente normativo que não só não definiu (ou não o fez de forma clara) esses conceitos,[28] como no qual não há uma separação clara quanto às atividades por eles abarcadas,[29] e no qual há muitos resquícios normativos de nossa herança ditatorial.[30] Se a ausência de lineamentos normativos é, de um lado, perniciosa, de outro, confere certa liberdade para carregar as expressões com conteúdo semântico ligado às suas finalidades, pois finalidades diversas fundamentam amplitudes diversas de tratamento de dados, especialmente no que diz respeito à coleta.

As atividades de *inteligência* "têm como função a coleta e a análise de informações necessárias para antecipar-se a perigos ou formular políticas de segurança interna ou externa" (Gleizer, Montenegro, Viana, 2021, p. 54). Estão voltadas à precaução, razão pela qual não é necessário um ensejo (um incidente de segurança, uma prática criminosa etc.) para suas atividades. Por isso, há uma ampla margem de coleta, já que a missão aqui é, justamente, a reunião de informações, num estágio prévio à atividade policial.[31] Para que essa amplitude não se torne uma ameaça aos direitos fundamentais em um Estado Democrático,[32] os órgãos de inteligência não podem agir, mas devem transmitir as informações aos órgãos de investigação/persecução penal para que estes atuem.[33] As atividades de *segurança pública* têm finalidade de proteção contra perigos, um olhar prospectivo e *preventivo* e são condicionadas por um interesse em proteger bens jurídicos contra perigos (Gleizer, Montenegro, Viana, 2021, p. 52-53).[34] A *persecução penal*, por fim, está voltada para a confirmação de uma suspeita, tem um olhar retrospectivo e condicionado por um interesse repressivo.[35]

27. Em sentido diverso, diferenciando as formas de tratamento, sustenta Rogall que a coleta (Erhebung) e o armazenamento (Speicherung) são sempre intervenções em direitos fundamentais; a utilização ou a análise (Nutzung oder Auswertung) de dados coletados licitamente não são intervenções e a transmissão (Übermittlung) é uma intervenção, a não ser quando isso é feito dentro da mesma agência ou órgão que a coletou e desde que não haja mudança de finalidade (1991, p. 929-930).

28. Estellita, Gleizer, Montenegro, 2020.

29. O Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal reflete essa insegurança quando inclui serviços de inteligência tanto no conceito de segurança pública como no de persecução penal (art. 5º, XXI e XXII), no que certamente precisa de aprimoramento, todavia a inclusão foi feita justamente em virtude da indefinição quanto a essas atividades para que não se alegasse, à frente, que os serviços de inteligência operariam ao largo de uma lei geral de proteção de dados em matéria penal.

30. Lima, Bueno, Mingardi, 2016, p. 50.

31. Greco, 2019, p. 52.

32. Muito bem percebida pelo Min. Édson Fachin no "Caso ABIN" (STF, MC na ADI 6.529, Tribunal Pleno, Relatora Min. Cármen Lúcia, DJe 15/10/2020), p. 58.

33. A finalidade da inteligência aqui tratada é diversa daquela regulada pela Lei 9.883/1999, que criou o Sistema Brasileiro de Inteligência, e que, apesar de refletir essa mesma ideia de coleta e disseminação de informações, parece liminar a inteligência àquela destinada à segurança do Estado (cf. art. 1º, § 1º). Daí que Abreu, ao analisar as expressões do art. 4º, III, da LGPD, conecte as ações de inteligência justamente ao âmbito da alínea "c", "segurança do Estado" (Abreu, 2021, p. 594). Para um apanhado histórico da regulação dos serviços de inteligência entre nós, cf. Mota, Herkenhoff, Lira, 2018. Uma crítica minuciosa à indeterminação das normas de compartilhamento de dados no âmbito da Lei 9.833/1999 pode ser encontrada no voto do Min. Gilmar Mendes no "Caso ABIN" (STF, MC na ADI 6.529, Plenário, Relatora Min. Cármen Lúcia, DJe 15/10/2020), p. 88.

Essas diferentes finalidades dão azo a diferentes autorizações de intervenção. As "normas autorizativas ou de faculdades autorizam ou facultam aos serviços de inteligência em primeira linha intervenções no direito à autodeterminação informacional" e, por isso, as transferências de informações de um "órgão de inteligência a um órgão de polícia é regulada por lei e limitada em vários sentidos" (Greco, 2019, p. 54-55). Na relação entre segurança pública e persecução penal, por exemplo, a polícia pode utilizar câmeras para monitorar manifestantes em uma passeata, utilizando, assim, seu efeito inibidor para evitar lesões ao patrimônio (prevenção de perigos), mas, terminada a manifestação, não pode armazenar essas imagens, a não ser que exista uma norma legal autorizando a manutenção das imagens caso algum crime tenha sido cometido e os dados sejam necessários para a persecução penal (interesse repressivo).[36]

34. Os autores dedicam todo um capítulo ao tema das intervenções informacionais para fins de segurança pública (p. 77 e ss.) e para o qual remeto o leitor. Cf. também Greco, 2019, p. 51-52; e Abreu, 2021, p. 595.

35. Gleizer, Montenegro, Viana, 2021, p. 52.53. No mesmo sentido, Abreu, 2021, p. 595.

36. O exemplo é de Gleizer, Montenegro, Viana, 2021, p. 53-54.

E) PROTEÇÃO DE DADOS NO BRASIL

Recapitulando: o instrumental normativo até aqui reunido e que também se encontra em vigor entre nós compõe-se dos seguintes elementos: *dever de abstenção* frente a direitos fundamentais; *intervenções apenas quando autorizadas por lei proporcional*, do que decorre que *normas de competência (atribuição) não veiculam autorizações*; direito fundamental à proteção de dados pessoais/autodeterminação informacional que se insere nessa mesma gramática, exigindo *autorização em lei para cada forma de tratamento* com estrito atendimento à *finalidade legalmente prevista* para o tratamento, do que também decorre a exigência de *separação informacional*. Esse instrumental, é bom dizer, *independe* de uma lei federal de proteção de dados para o âmbito penal, muito embora uma tal lei seja desejável.[37]

Foi nessa estrutura normativa constitucional de proteção de direitos fundamentais, em vigor desde 1988, que o STF assentou o reconhecimento da proteção de dados pessoais[38] e o fez reconhecendo-o como um direito fundamental no qual só se pode intervir mediante autorização prevista em lei que observe os pressupostos de proporcionalidade da intervenção (devido processo legal material, nas palavras da Corte). Isso aconteceu no julgamento das ADIS 6.387 MC-Ref/DF, ADI n. 6.388 MC-Ref/DF, ADI n. 6.389 MC-Ref/DF, ADI n. 6.390 MC-Ref/DF e ADI n. 6.393 MC-Ref/DF,[39] sob relatoria da Min. Rosa Weber, e no qual se discutia acerca da legalidade do compartilhamento de dados pessoais não anonimizados de usuários de empresas de telecomunicação com o IBGE (MP 954/2020).[40] O ônus argumentativo que pesou sobre a Corte será bem mais leve a partir da promulgação da PEC 17/2019, aprovada pelo Senado em 20/10/2021, que inclui a proteção de dados pessoais no rol dos direitos fundamentais (art. 5º, CF).

37. Especialmente para regular de forma geral, expressa e detalhada alguns aspectos dessa proteção específicos desse âmbito como, por exemplo, prazos de eliminação, exercício direto e indireto dos direitos dos titulares, autoridade nacional de proteção de dados etc. No mesmo sentido, Abreu, 2021, p. 599. Esses aspectos foram tratados pelo Anteprojeto de Lei de Proteção de Dados para a segurança pública e a persecução penal, cf. Comissão de Juristas da Câmara dos Deputados, 2020.

38. Rogall chama a atenção para essa mesma situação na Alemanha quando proferida a famosa "Decisão do Censo" (1983) pela Corte Constitucional, a qual, segundo ele, nada mais fez que estender ao âmbito das relações informacionais os princípios já reconhecidos no âmbito da proteção de direitos fundamentais frente a intervenções informacionais estatais (Rogall, 1991, p. 930).

39. Mas também no "Caso ABIN", STF, MC na ADI 6.529, Tribunal Pleno, Relatora Min. Cármen Lúcia, DJE 15/10/2020. Cf. especialmente o voto do Min. Édson Fachin, p. 57, e do Min. Gilmar Mendes, p. 77 e ss.

40. Um relato detalhado em Souto, Rosal, 2021.

2 PRIVACIDADE E PROTEÇÃO DE DADOS NO TRATAMENTO PARA AS MEDIDAS DE CONTROLE E PREVENÇÃO DA LAVAGEM DE CAPITAIS

A) DIREITO À PRIVACIDADE, DIREITO À PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMACIONAL

Independentemente da discussão acerca da autonomia do direito à proteção de dados[41], há consenso quanto ao fato de que esse direito vai além da ideia clássica de privacidade como direito de estar só, de se afastar da multidão – baseada numa dicotomia entre o público e o privado[42]– , para manifestar um direito de controle[43] do titular sobre os próprios dados ("pessoa-informação-circulação-controle", Bioni, 2020, p. 94). Nesse âmbito, dados compartilhados com o público, que não gerariam por si questões atinentes à privacidade no sentido clássico, podem, "quando agregados a outros fatos (dados), revelar detalhes precisos sobre a personalidade de um indivíduo" (Bioni, 2020, p. 95). Os direitos de acesso e retificação que tem o titular de dados pessoais mesmo quando "transitam na esfera pública" (Bioni, 2020, p. 95) são um exemplo claro de que essa tutela não se confunde com a da privacidade entendida no seu sentido originário de "afastamento da multidão" (Doneda, 2020, p. 181-182).[44] Passamos, assim, da lógica segundo a qual "dados que não são 'sigilosos'... não são protegidos" (Abreu, 2021, p. 588), para uma de proteção ampla de dados pessoais contra todas as formas de tratamento. Essas considerações são importantes no âmbito do tratamento de dados para fins de controle e prevenção da lavagem de capitais, especialmente no tratamento dado pelo COAF, objeto da decisão do STF.

41. Sobre essa discussão, cf., entre nós, o trabalho pioneiro de Doneda, 2020, passim. Silva registra que talvez "não haja outro direito que tenha passado por transformações tão profundas e tão rápidas em seu significado nas últimas décadas como o direito à privacidade" (Silva, 2021, p. 203). Para Bioni, 2020, p. 95, trata-se de um "novo direito da personalidade". Cf. Para Gleizer, Montenegro, Viana, 2021, é uma decorrência dos direitos fundamentais que conformam a garantia ao livre desenvolvimento da personalidade p. 38-39. A LGPD optou por assentar a proteção de dados pessoais tanto no respeito à privacidade, como na autodeterminação informativa e na inviolabilidade da intimidade, da honra e da imagem (art. 2º, incs. I, II e IV, respectivamente).

42. Bioni, 2020, p. 91-94.

43. Mas não de domínio ou propriedade como sustenta Rogall, 1985, p. 11-12.

44. Também Abreu, 2021, p. 584.

B) DADOS PESSOAIS, DADOS PESSOAIS SENSÍVEIS E DADOS PESSOAIS SIGILOSOS

Os dados pessoais podem ser divididos em categorias segundo certas restrições impostas a seu tratamento.

A LGPD define dado pessoal como a "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, inc. I), e dado pessoal sensível como aquele "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, inc. II). O tratamento destes últimos está sujeito a uma série de restrições como, por exemplo, um consentimento qualificado do titular (arts. 11 a 13, LGPD).

No âmbito das medidas de prevenção à lavagem (adiante, PLD), há tratamento de grande quantidade de dados pessoais e de dados pessoais sensíveis. No cumprimento de suas obrigações de PLD (arts. 10, I, II, 11, I e II, LLD), as pessoas obrigadas (art. 9º, LLD) devem proceder a várias operações de tratamento de dados pessoais em quantidades nada desprezíveis. Usando a linguagem do art. 5º, X,

45. Para que se tenha uma ideia da quantidade e amplitude dos dados tratados, basta consultar a Resolução COAF n. 36, de 10 de março de 2021, que se aplica apenas às pessoas obrigadas sujeitas à supervisão do COAF, arts. 7º a 12.Um apanhado geral da regulação no âmbito de competência regulatória do BACEN e da CVM em Oliveira, 2020. A CVM acaba de atualizar sua regulação setorial de PLD, cf. Resolução CVM n. 50, de 31 de agosto de 2021. A amplitude dos dados tratados é objeto de preocupação no ambiente europeu há algum tempo, cf. ilustrativamente, Autoridade Europeia para Proteção de Dados, 2017; Preziosi, 2017; Malish, 2018; Khan, 2016; Peña Zafra, 2016.

da LGPD, elas devem, *pelo menos*, coletar, produzir, recepcionar, classificar, utilizar, acessar, reproduzir, transmitir, distribuir, processar, arquivar, armazenar, avaliar, controlar, modificar, comunicar, transferir e difundir dados pessoais.[45]

Dentre os dados pessoais tratados pelo COAF, haverá também dados *sensíveis* e *sigilosos*.

Dados pessoais *sensíveis* serão objeto de tratamento quando relativos a "presidentes e tesoureiros nacionais, ou equivalentes, de partidos políticos", pois considerados pessoas politicamente expostas (art. 1º, § 1º, VI, Resolução COAF n. 29, de 7 de dezembro de 2017) e relativos, portanto, à filiação a organização de caráter político (art. 5º, II, LGPD). Nesse caso, as pessoas obrigadas devem adotar providências especiais para o acompanhamento de operações ou propostas de operações com pessoas expostas politicamente (art. 1º, caput, Resolução COAF n. 29). Elas devem "dedicar especial atenção às operações ou propostas de operações envolvendo pessoa exposta politicamente, bem como com seus familiares, estreitos colaboradores e ou pessoas jurídicas de que participem, observando, nos casos de maior risco" (art. 2º, *caput*, Resolução COAF n. 29).

Além dessas atividades de coleta de dados pessoais feitas no âmbito do *know your customer* (KYC) ou *customer due diligence* (CDD), uma das obrigações mais relevantes para a prevenção e repressão à lavagem é a de *comunicação* de operações em espécie (COE) e de operações suspeitas (COS) ao COAF. Os dados transmitidos (para usar a linguagem da LGPD, art. 5º, X) pelas pessoas obrigadas ao cumprirem seus deveres de comunicação de operações em espécie (art. 11, II, a, LLD) e suspeitas (que possam "constituir-se em sérios indícios dos crimes previstos nesta Lei, ou com eles relacionar-se", art. 11, II, b, LLD), envolverá, por definição, dados pessoais. Isso é assim porque virão, necessariamente, acompanhadas de informações relacionadas às pessoas naturais envolvidas nas transações[46], pois apenas elas[47] estão sujeitas à responsabilidade penal e são, portanto, os alvos finais de toda a legislação de controle, prevenção e repressão à lavagem de capitais e ao financiamento ao terrorismo.[48]

Além de dados pessoais sensíveis, é da essência da atividade do COAF o tratamento de dados sujeitos a *sigilo*: um dever imposto, por lei ou ato privado, ao recipiente do dado ou informação de não revelá-lo a outras pessoas, senão àquelas expressamente autorizadas pelo titular, pelo ato privado ou pela lei.[49] O sigilo, de forma geral, restringe certas formas de tratamento que impliquem *revelação* a terceiros não autorizados do conteúdo da informação sigilosa, ou seja, na linguagem do art. 5º, X, da LGPD, a *transmissão, a distribuição, a comunicação, a transferência, a difusão*.

Há vários sigilos, médico, profissional, comercial, financeiro etc., instituídos sobre diversos fundamentos jurídicos[50], e sua violação (leia-se, a revelação da informação protegida) é conduta criminalizada, entre nós, de forma geral, pelos arts. 154 e 325 do CP.[51] Especificamente no que diz respeito ao

46. Cf. Nota Técnica 40.241 do COAF referida no voto do Min. Gilmar Mendes no RE 1.055.941, fl. 3073-3074: "O primeiro tipo de comunicação reporta operações individuais, sem a necessidade de maiores detalhamentos. A COE informa o valor da operação, a identificação do titular da conta, a pessoa que efetuou a operação, o proprietário do dinheiro e dados cadastrais bancários, tais como conta, agência, banco e cidade"; o "segundo tipo de comunicação (COS) assim se define segundo critérios emanados da lei e de regulamentos aplicáveis". O detalhamento dos dados que devem compor as duas espécies de comunicação é feito por cada regulação setorial. No caso dos bancos, por exemplo, cf. BACEN, Circular n. 3.978, de 23 de janeiro de 2020, arts. 48 a 55.

47. Exceção feita às pessoas jurídicas no âmbito dos crimes ambientais, Lei 9.605/98.

48. Greenleaf, Tyree, 2017, p. 45.

49. A LGPD não define o que sejam dados sigilosos, mas indica as limitações em seu tratamento e as medidas de segurança para evitar revelação que devem ser aplicadas, cf. arts. 46 a 49.

50. Sobre os diversos fundamentos do sigilo no âmbito do § 53 do STPO (Código de Processo Penal alemão), cf. Rogall, 2018, especialmente números marginais 10 e seguintes. Sobre o sigilo médico e sua orientação à proteção de interesse individual do paciente, cf., Soares, 2020.

51. Os dois tipos penais indicam como conduta incriminada a de revelar segredo ou fato que deva permanecer em segredo.

sigilo *financeiro*, segundo opinião majoritária, serve à preservação do direito à privacidade,[52] recebendo tutela penal específica, atualmente, no âmbito da LC 105,[53] que incrimina a "quebra de sigilo, fora das hipóteses autorizadas" na lei punindo-a com pena de reclusão, de um a quatro anos, e multa (art. 10).[54]

3 O TRATAMENTO DE DADOS PESSOAIS PELO COAF

É tempo de examinar as possíveis consequências das ideias até aqui apresentadas para o tratamento de dados pessoais pelo COAF, exame que deve ser feito em conformidade com as premissas até aqui estabelecidas e que recapitulo brevemente: (a) as competências e tarefas atribuídas ao COAF não são autorizações para intervenção em direitos fundamentais, do que decorre (b) a necessidade de que todo tratamento de dados realizado por esse órgão tenha de estar previamente autorizado por lei proporcional,[55] que é aquela (c) que estabelece de forma clara tanto a modalidade de tratamento autorizada como a finalidade da intervenção (sendo cada nova forma de tratamento uma intervenção autônoma), e que (d) no caso de dados pessoais protegidos por sigilo financeiro, ademais, formas de tratamento que impliquem revelação[56]

52. Cf. Baltazar Júnior, 2005, p. 60; Salomão Neto, 2020, p. 678; Belloque, 2003, p. 73; Abreu, 2021, p. 584-585. Ferraz Júnior, por sua vez, parece assentar o sigilo bancário no disposto no art. 5º, XII, CF (2020, p. 170, nota 6). No próprio RE 1.055.941, o Min. Gilmar Mendes, por exemplo, assenta-o no art. 5º, X, CF (fl. 3043). Como a LC 105 institui o sigilo em função das operações e dos detentores dos dados (instituições financeiras), ela não o limita às pessoas naturais, mas alcança também pessoas jurídicas. Isto poderia colocar em xeque o entendimento segundo o qual o fundamento desse sigilo é a privacidade caso se reconheça que as pessoas jurídicas não têm um direito fundamental à privacidade. Isso indicaria a correção do entendimento que vê neste sigilo uma espécie de sigilo profissional fundado na liberdade geral de ação, como se faz na Alemanha (Kalkbrenner, Koch, 2019, número marginal 3; que alertam para o fato de que a proteção do sigilo bancário é mais ampla quanto aos sujeitos protegidos do que a da proteção de dados pessoais, nm. 7).

53. Quanto à relação entre o art. 10 da LC 105/2001 e o art. 18 da Lei 7.492/1986, entende-se que os dois estão em vigor e têm abrangência distinta em função do âmbito de sujeitos abrangidos pela LC 105 e pela Lei 7.492/86, cf. Baltazar, 2005, p. 172-173.

/ ESSE ACÚMULO DE ATRIBUIÇÕES [...] TORNA DIFÍCIL ALOCAR O ÓRGÃO SOB ESTE OU AQUELE PILAR E, CONSEQUENTEMENTE, PODE GERAR RISCOS /

/ HÁ MUITO A FAZER [...] NUM AMBIENTE CUJO TRATAMENTO DE DADOS É TÃO AMPLO E INTENSO COMO O DO COAF /

(transmissão, distribuição, comunicação, transferência, difusão) devem cumprir rigorosamente o que dispõe a LC 105.

A) COMPETÊNCIAS E TAREFAS ATRIBUÍDAS AO COAF

A LLD criou, em 1998, o COAF com a "a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta Lei, sem prejuízo das competências de outros órgãos e entidades" (art. 14, caput).[57] O órgão tem como atribuições, ainda, "coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores" (art. 14, § 2º). Para isso, tem autorização ("poderá") para "requerer aos órgãos da Administração Pública as informações cadastrais bancárias e financeiras de pessoas envolvidas em atividades suspeitas" (§ 3º). Por fim, o órgão "comunicará às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito" (art. 15).

A par dessas normas, em 7 de janeiro de 2020, foi promulgada a Lei n. 13.974, que, além de vincular o órgão ao Banco Central do Brasil (art. 2º), estabelece sua estru-

54. Outras violações graves ao regime de proteção de dados pessoais ainda carecem de tutela penal entre nós, mas já foram contempladas, por exemplo, em Portugal, na Lei n. 59/2019, arts. 53 a 60; na Itália, no Decreto Legislativo n. 51, de 18 de maio de 2018, arts. 43 a 45; na Alemanha, na Bundesdatenschutzgesetz – BDSG (Lei Federal de Proteção de Dados), par. 42; na Suíça, no StGB (Código Penal), arts. 143, 143-bis, 179-novies); e na Espanha nos arts. 197 e 198 do Código Penal.

55. Em virtude dessa exigência, é que o Decreto 9.663, de 1º de janeiro de 2019, que aprova o Estatuto do COAF, não oferece fundamento legal para tratamento de dados, razão pela qual não será objeto de exame nesta oportunidade.

56. A LC 105 fala em "conservar sigilo" (art. 1º), "violação de sigilo" (art. 1º, § 3º), "revelação de informações sigilosas" (art. 1º, § 3º, V), "quebra de sigilo" (art. 1º, § 4º), "dever de sigilo extensivo" (art. 2º), "preservação do sigilo mediante acesso restrito às partes" (art. 3º), "levantamento do sigilo" (art. 7º), "quebra de sigilo" (art. 10, que define a conduta a partir de uma metáfora).

57 . Uso a redação em vigor em 20/09/2021.

tura organizacional e atribuições, dentre elas as de "produzir e gerir informações de inteligência financeira para a prevenção e o combate à lavagem de dinheiro" e a de "promover a interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades" (art. 3º, I e II). Esse diploma legal, porém, não veicula autorizações legais para a intervenção em direitos fundamentais, mas trata da estrutura interna e funcionamento do órgão (norma de *competência*, portanto, no sentido acima empregado III, 1, b). Sob este ponto de vista, por exemplo, a "produção e gestão de informações de inteligência financeira" que envolvam dados pessoais (art. 3º, I, acima) poderá ser feita desde que haja uma autorização legal, seja na LLD, seja em outra lei federal. Inexistindo autorização, a produção e a gestão não poderão envolver dados pessoais, mas, sim, por exemplo, dados anonimizados para fins estatísticos, de construção de tipologias etc. Isso vale também para a interlocução institucional com órgãos nacionais e estrangeiros (cf. infra IV, 3).

As tarefas atribuídas ao COAF parecem misturar elementos de *inteligência*, de *segurança pública* e de *persecução penal*. O órgão coleta e analisa informações necessárias para formular políticas de prevenção de lavagem (*inteligência*), fiscaliza o cumprimento das medidas de controle e prevenção da lavagem pelas pessoas obrigadas para, assim, prevenir

58. O supervisor de proteção de dados europeu vem alertando para os perigos dessa falta de clareza e determinação quanto à natureza das funções das unidades de inteligência financeira desde, pelo menos, 2017: cf. European Data Protection Supervisor, 2017, parágrafo 52; e mais recentemente, European Data Protection Supervisor, 2020, parágrafos 35 e 36.

59. "Art. 11. As pessoas referidas no art. 9º: (...) II - deverão comunicar ao Coaf, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização: a) de todas as transações referidas no inciso II do art. 10, acompanhadas da identificação de que trata o inciso I do mencionado artigo; e b) das operações referidas no inciso I".

60. Neste sentido, cf. o § 28 da Geldwäschegesetz (adiante, GwG) que detalha, em 13 incisos, todas as atividades da UIF alemã, seguido do § 29, que disciplina o tratamento de dados pessoais pela UIF.

perigos contra bens jurídicos (*segurança pública*) e, finalmente, se volta para o passado, ao apurar operações suspeitas de lavagem e as comunicar aos órgãos de persecução penal (*persecução penal*). Esta última faceta poderá ser ainda mais acentuada se se admitir a elaboração de RIFs a pedido (cf. infra IV, 2). Esse acúmulo de atribuições com finalidades diversas, que veicula uma coleta de dados de amplitude singular em nosso sistema jurídico, torna difícil alocar o órgão sob este ou aquele pilar e, consequentemente, pode gerar riscos para a proteção de dados pessoais, especialmente sob o ponto de vista da separação informacional.[58]

61. "Art. 14. Fica criado, no âmbito do Ministério da Economia, o Conselho de Controle de Atividades Financeiras - Coaf, com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta Lei, sem prejuízo das competências de outros órgãos e entidades" (Redação dada pela Medida Provisória nº 886, de 2019).

B) DADOS PESSOAIS

Sob o ponto de vista do tratamento de dados pessoais, os artigos 11, 14 e 15 da LLD sugerem o seguinte regime:

< I > o art. 11 veicula a norma autorizativa que autoriza as pessoas obrigadas (do art. 9º) a transmitirem ao COAF dados pessoais não sujeitos a sigilo financeiro;[59]

< II > o artigo 14, *caput*, lido com benevolência (já que a linguagem se aproxima mais da de uma norma de competência do que de uma norma de autorização[60]), autoriza o COAF ao tratamento ("receber, examinar e identificar") interno de dados pessoais recebidos das pessoas obrigadas exclusivamente para a finalidade de apuração da ocorrência de suspeita de prática de lavagem de dinheiro e financiamento ao terrorismo ("as ocorrências suspeitas

de atividades ilícitas previstas nesta Lei"), vedado o tratamento para qualquer outra finalidade;[61]

< III > uma especial forma de tratamento, a comunicação (também chamada de "disseminação"), só pode ser realizada *pelo* COAF *para* as "autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito" (art. 15);

< IV > o dever imposto ao órgão de "coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores" (art. 14, § 2º),[62] não parece veicular norma autorizativa para compartilhamento de dados pessoais (sigilosos ou não) com pessoas que não as indicadas no art. 15, pois o que a lei autoriza é que o órgão *coordene* e *proponha*, mas não que *troque* informações, ou seja, que as transmita, distribua, comunique, transfira, difunda ou dissemine.

C) DADOS PESSOAIS FINANCEIROS SIGILOSOS

Além de dados pessoais comuns e sensíveis, o COAF recebe e trata também dados pessoais financeiros *sigilosos*, submetidos, até 2001, ao regime do art. 38 da Lei 4.595/1964, e, a partir de 2001, ao regime da LC 105. A regra é que as operações ativas e passivas e os serviços prestados pelas instituições financeiras indicadas no art. 1º, § 1º, da LC 105, sejam sigilosas, no sentido de que as informações a elas relativas *não possam ser reveladas* (transmitidas, distribuídas, comunicadas, transferidas, difundidas ou disseminadas) a terceiros.

62. Art. 15: "§ 2º O COAF deverá, ainda, coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores".

A relação entre a LLD (e suas alterações) e a LC 105 habita o problemático ambiente das relações entre leis ordinárias e lei complementares. A partir de 1988, o art. 192, *caput*, da CF passou a determinar que o sistema financeiro nacional fosse regulado por lei complementar. Por essa razão, a Lei nº 4.595, de 31 de dezembro de 1964, que tratava da matéria, foi recepcionada pela nova ordem constitucional como lei complementar.[63] E era seu art. 38 que, até 2001, instituía o sigilo financeiro. Em 2001, como dito, sobreveio nova lei complementar disciplinando de forma mais detalhada o sigilo financeiro, a LC 105.

Muito embora o STF tenha reconhecido, por maioria, que não existe, em regra, hierarquia entre uma lei ordinária e uma lei complementar, há uma certa distribuição constitucional material (*ratione materiae*) entre as espécies legislativas:[64] uma reserva constitucional de lei complementar limitada a certas matérias. Assim, uma lei ordinária poderia dispor em sentido contrário do disposto em uma lei complementar e, assim, revogar seus dispositivos, *desde que* não trate de matéria privativa desta.[65] *A contrario sensu*, uma lei complementar que trate de matéria a ela não reservada pela CF vale como lei ordinária[66].

E por que isso importa?

Porque tendo sido o sigilo financeiro estabelecido em lei complementar, se houver, para essa matéria, reserva constitucional de lei complementar,[67] as normas da LLD não revogariam nem as da Lei 4.595/1964 (até 2001), nem as da LC 105 (após 2001), que regeriam, soberanas, as

63. BALTAZAR, 2005, p. 73.

64. STF, RE 377.457, Tribunal Pleno, rel. Min. Gilmar Mendes, DJe 18/11/2008.

65. STF, RE 377.457, Tribunal Pleno, rel. Min. Gilmar Mendes, DJe 18/11/2008, fl. 1819.

66. STF, RE 377.457, Tribunal Pleno, rel. Min. Gilmar Mendes, DJe 18/11/2008, fl. 1834. A complexidade dessa discussão se mostra com toda sua força na discussão travada no plenário por ocasião deste julgamento e que não pode ser captada nesta oportunidade.

67. Um tema que merece estudo mais aprofundado, inviável aqui.

autorizações para a revelação de dados financeiros sigilosos. Em outras palavras: a revelação de dados financeiros sigilosos *para* o COAF e *pelo* COAF dependeriam das autorizações expressas da LC 105. Neste caso, tanto as comunicações de operações (em espécie e suspeitas) feitas pelas pessoas obrigadas *para* o COAF contendo dados financeiros sigilosos, como *do* COAF para as autoridades competentes para a persecução penal (por meio de RIFs no sentido do art. 15, LLD) dependeriam de norma autorizativa na LC 105. Sob esse entendimento, teríamos o seguinte quadro à luz da LC 105:

68. O art. 10, II, e o art. 11, II, que distingue, em suas alíneas "a" e "b", entre operações em espécie (que geram as comunicações denominadas COE) e as suspeitas (que geram comunicações denominadas COS).

69. Cf. LC 105/2001, art. 1º, § 3º, VI, c.c., especialmente, com o art. 9º.

< I > haveria uma autorização para "a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa" (art. 1º, § 3º, IV, LC 105), aplicável a quaisquer pessoas submetidas à LC 105, dentre elas parte das pessoas obrigadas do art. 9º da LLD. Essa seria a norma que veicularia autorização legal para a comunicação de operações suspeitas (COS) pelas pessoas obrigadas sujeitas à LC 105 ao COAF;

< II > haveria autorização para que o BACEN e a CVM, no exercício de suas atribuições e quando verificassem "a ocorrência de crime definido em lei como de ação pública, ou indícios da prática de tais crimes", informassem o Ministério Público sobre tais fatos juntando à comunicação os documentos necessários à apuração ou comprovação dos fatos (art. 9º, caput, LC 105); ou seja, haveria uma autorização para comunicação não ao COAF, mas ao MP, sobre eventual suspeita de prática de crime;

< III > haveria autorização para que o BACEN e a CVM e demais órgãos de fiscalização (mas não as instituições financeiras), nas áreas de suas atribuições, fornecessem ao COAF "as informações cadastrais e de movimento de valores relativos às operações previstas no inciso I do art. 11 da referida Lei", que são as que "possam constituir-se em sérios indícios dos crimes previstos nesta Lei, com eles relacionar-se" (art. 11, I, LLD). O dispositivo, portanto, só alcança operações suspeitas (art. 2º, § 6º, LC 105);

< IV > quanto às comunicações de operações em espécie, disciplinadas em dois dispositivos da LLD,[68] a LC 105 não teria veiculado autorização para que as pessoas obrigadas pela LLD, mas submetidas ao sigilo financeiro, fizessem tais comunicações, a não ser que se entenda que toda operação em espécie é suspeita, em um sentido mais amplo deste termo, diverso do sentido que lhe é dado pela LLD;

< V > por fim, a LC 105 instituiu o sigilo de dados financeiros, mas não tratou da comunicação do COAF *para* as "autoridades competentes" (art. 15, LLD) que contenham dados protegidos por sigilo financeiro, como fez, expressamente, quanto ao BACEN, à CVM e à Receita Federal.[69] Esse pernicioso silêncio pode dar azo a disputas quanto à possibilidade de o COAF incluir dados cobertos por sigilo finan-

ceiro em seus relatórios para autoridades de persecução penal.[70]

A questão ficou ainda mais complexa com o advento da mudança do COAF para âmbito do BACEN por força da Lei 13.974, de 7 de janeiro de 2020. Se se entender que, a partir de então, o órgão e seus agentes fazem parte do BACEN, a eles se estende o dever de sigilo (art. 2º, § 5º, LC 105) e também a autorização para a comunicação prevista no art. 9º, o que tornaria inquestionável a possibilidade de que os RIFs contivessem dados protegidos por sigilo financeiro. A complexidade criada pelo art. 2º da Lei 13.974, que "vinculou administrativamente" o COAF ao BACEN, mas manteve sua "autonomia técnica e operacional", está a merecer melhor exame, especialmente sob o viés da separação informacional.

Se, porém, se entender que a matéria do sigilo financeiro, apesar de veiculada em lei complementar, não está a ela reservada, então tanto as normas Lei 4.595/1964 como as da sua sucessora, a LC 105, valeriam como lei ordinária e as normas da LLD teriam o condão de regular a matéria, criando permissões de revelação desses dados não contempladas na LC 105. Neste caso, o art. 11 da LLD, na redação recebida por força da Lei 12.683/2012, seria a base legal que autorizaria todas as pessoas obrigadas – dentre elas também aquelas sujeitas à LC 105, que é anterior à Lei 12.683/2012 – a comunicar dados pessoais financeiros sigilosos ao COAF; e o art. 15 da LLD autorizaria este órgão a comunicá-los, nos RIFs, às autoridades competentes.

Até aqui, a bem ver, tratamos de revelação de dados pessoais *financeiros sigilosos* limitados a certas operações (suspeitas, em espécie, indicativas da prática de crime), do que decorre uma delimitação clara dos dados que podem ser revelados em termos de tempo, espaço, pessoas envolvidas, montantes, espécie de operação ou serviços, pois a *finalidade* é clara. Embora, como dito, configurem intervenções no direito à proteção de dados pessoais e na privacidade, a severidade dessa intervenções, em si mesmas, é mais limitada do que a revelação de dados financeiros não conectados a certas operações, mas, sim, a lapsos temporais. Neste último caso, trata-se de revelar aspectos amplos não só da privacidade da pessoa afetada, mas de sua intimidade, além de dados de terceiros insuspeitos.[71] Enquanto a comunicação de uma prática criminosa está limitada (finalidade) apenas às informações necessárias para a comprovação da suspeita, por exemplo, o recebimento de certa quantia, em certa data, envolvendo certas pessoas etc.; o que conhecemos por "quebra" do sigilo bancário por ordem judicial ou de comissões parlamentares de inquérito implica em revelação indiscriminada da privacidade e da intimidade tanto da pessoa que é alvo da "quebra" como de terceiros insuspeitos dentro do espectro temporal coberto pela determinação. Trata-se, assim, de uma intervenção muito mais severa no âmbito do direito fundamental à privacidade e é por esta razão que, nestes casos, a LC 105 não veicula uma autorização direta para que agentes públicos os acessem, mas exige uma autorização judicial individualizada (*reserva de jurisdição*, art. 1º, § 4º) ou a aprovação por órgão colegiado no âmbito das comissões parlamentares de inquérito (art. 4º, § 2º), e, ademais, determina que o caráter sigiloso seja mantido mediante "acesso restrito às partes, que delas não poderão servir-se para fins estranhos à lide" (art. 3º, *caput*, LC 105).[72]

70. Essa incerteza não é um privilégio do Brasil como registra Maillart em tom crítico, quanto aos cinco países analisados em abrangente estudo comparativo sobre a regulação da lavagem de capitais concluído em 2020 (Vogel, Maillart, 2020, p. 848).

71. Cf. Estellita, Gleizer, 2020.

72. Este é só um dentre os inumeráveis fundamentos que evidenciam a ilegalidade da determinação feita pela PGR, em meados de 2020, às Forças-Tarefa da Operação Lava-Jato no Rio de Janeiro, São Paulo e Curitiba para que lhe entregassem "todas as bases da dados estruturados e não-estruturados utilizadas e obtidas em suas investigações, por meio de sua remessa atual, e para dados pretéritos e futuros, à Secretaria de Perícia, Pesquisa e Análise do gabinete do procurador-geral da República" (https://g1.globo.com/politica/noticia/2020/08/03/fachin-revoga-decisao-de-toffoli-que-permitia-compartilhamento-de-dados-entre-pgr-e-forcas-tarefa-lava-jato.ghtml; acesso em 11/09/2021), seguida da Portaria Conjunta PGR/MPF - CMPF n. 1, de 7 de janeiro de 2021. Outras considerações em Luz, 2021. A determinação é objeto de disputa no STF, na RCL 42.050, que tramita sob sigilo.

III CONSEQUÊNCIAS

Estabelecidas todas essas premissas, cumpre delas extrair as consequências para aquela que é a questão central examinada neste texto: os limites da transmissão, distribuição, comunicação, transferência e difusão (ou disseminação, no jargão do COAF) de dados pessoais *pelo* COAF.

1 RIFS DE OFÍCIO ("DISSEMINAÇÃO ESPONTÂNEA")

Como visto, tanto a LLD como a LC 105 contêm autorizações[73] para que o COAF receba, classifique, utilize, processe, arquive, armazene, avalie e controle dados pessoais, sigilosos ou não. Quanto às operações de transmissão, distribuição, comunicação, transferência e difusão (que evidentemente incluem a "disseminação"), norma autorizativa para essas formas de tratamento é o art. 15 da LLD, que as limita à comunicação às autoridades competentes, quando o próprio órgão concluir pela existência ou fundados indícios da prática de crimes previstos na LLD, ou qualquer outro ilícito.[74] Nada mais é dito sobre a forma e o conteúdo dessas comunicações.[75]

2 RIFS A PEDIDO ("DISSEMINAÇÃO A PEDIDO")

Os dois diplomas legais que regulam a atividade do COAF não parecem lhe impor um dever de compartilhar dados pessoais *a pedido de autoridades públicas*.[76]

73. Muito embora com linguagem fraca em termos da clareza e da determinação que se deve exigir das normas autorizativas de intervenções em direitos fundamentais (cf. acima II, 1, a e b).

74. A referência a "qualquer outro ilícito", prevista no final do art. 15, caput, LLD, merece reparo, pois poderia levar a transformar o órgão de combate e prevenção à lavagem de dinheiro e ao financiamento do terrorismo em agência de inteligência de quaisquer ilícitos, penais ou administrativos, praticados no País. Sobre a importância de rigorosa observância da finalidade do tratamento de dados pelas unidades de inteligência financeira, cf. European Data Protection Supervisor, 2020, parágrafos 8 a 10.

75. O dispositivo é lacônico, beirando o descumprimento do princípio da clareza e determinação e merece atenção do legislador. Nesse sentido, vale conferir o detalhado § 32, 5, GwG.

Com relação a eventuais pedidos de representantes do Ministério Público, muito embora seja sua "função institucional" "promover, privativamente, a ação penal pública, na forma da lei" e "requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais" (art. 129, I e VIII, CF),[77] dessas atribuições não derivam autorizações para intervenção em direitos fundamentais, as quais, como dito e repetido, têm de ser autorizadas por lei (art. 5º, II, CF).[78]

O Ministério Público tem, assim, competência para fazer essas requisições, mas o atendimento que implique tratamento de dados pessoais só pode ser efetuado se houver autorização legal proporcional. Um entendimento que autorizasse aos membros do MP a obtenção direta, junto às instituições financeiras ou ao COAF, de informações cobertas por sigilo financeiro permitiria que, como dito, pela porta dos fundos (*back door*), fosse corroído o regime constitucional (e infraconstitucional) de proteção de direitos fundamentais. Isso implicaria, ademais, em verdadeira *fusão informacional* entre os dois órgãos,[79] pois, por essa via, o Ministério Público obteria acesso a um imenso conjunto de dados que o legislador outorgou *apenas* ao COAF.[80] Esses mesmos limites valem, logicamente, para as autoridades policiais.

76. Em sentido similar, BOTTINI, 2021. Sobre a situação nos cinco países objeto da pesquisa coordenada por Vogel e Maillart, cf. Vogel, Maillart, 2020, p. 848-849.

77. A Lei Complementar n. 75/1993 repete essa regra de competência (art. 6º, V) e contém outra regra de competência no art.

78. A teoria dos poderes implícitos discutida no STF quando chamado a decidir se membros do Ministério Público poderiam investigar não é incompatível com o que aqui se afirma, pois seus poderes de investigar só podem ser exercidos desde que respeitados os direitos e garantias fundamentais (cf. STF, RE 593.727, Tribunal Pleno, rel. Min. Cezar Peluso, DJ 08/09/2015).

79. Em sentido similar, Greco, Leite, 2019.

80. Badaró chama a atenção para esse ponto considerando equivocada a decisão do STF no RE por não separar adequadamente "quem detém a informação" de "quem detém o poder de persecução penal" (Badaró, 2021). Em sentido diverso, aparentemente, BOTTINI, 2021.

Conforme explicações fornecidas pelo COAF ao STF no RE aqui analisado, o Sistema SEI-C, além de ser utilizado para as comunicações do COAF para as autoridades competentes, também é utilizado como um canal de comunicação na via oposta: das autoridades competentes para o COAF. Nele, essas autoridades registram dados sobre pessoas investigadas, os crimes dos quais são suspeitas e a descrição do modo como os teriam praticado. Essas novas informações, incorporadas ao acervo informacional que o COAF já tem,[81] podem ser objeto de análise, com a conclusão da existência de operações suspeitas de lavagem. Neste caso, o COAF pode, naturalmente, gerar um RIF e comunicar as operações suspeitas individualizadas às autoridades competentes, nos exatos termos da autorização que lhe é dada pelo art. 15 da LLD. Esta foi, inclusive, a posição do relator do RE 1.055.941 (cf. fl. 2738 do acórdão) no STF e que parece acertada, pois aqui, na verdade, não se trata de um RIF ou "disseminação" a pedido", mas de RIF de ofício ("disseminação espontânea").[82]

81. Questão que está a merecer atenção diz respeito à necessidade de maior transparência quanto às fontes de dados. Sobre isso, cf. Bialski, Vento, Messina, Wiegerinck, 2021.

82. Razão pela qual seria recomendável não o denominar de "RIF decorrente de intercâmbio", expressão que sugere um RIF produzido por provocação de autoridades públicas, tratamento de dados que, como visto, não está autorizada pela LLD.

83. COAF - CONSELHO CONTROLE DE ATIVIDADES FINANCEIRAS. Inteligência Financeira: Aspectos Práticos do Intercâmbio Internacional via Rede Egmont. [s.l.: s.n., s.d.]. Disponível em: <https://www.youtube.com/watch?v=i5N_LqLmewI>. Acesso em: 8 ago. 2021.

3 INTERCÂMBIO INTERNACIONAL ENTRE UIFS

A questão é bem mais delicada quando se trata do intercâmbio de dados pessoais (dentre eles também financeiros sigilosos) com unidades de inteligência financeira de outros países, como no âmbito do chamado Grupo Egmont. Segundo informações públicas do próprio COAF,[83] a cooperação com as UIFs estrangeiras dá-se no âmbito do próprio SEI-C, onde podem ser transmitidos e transferidos (e também obtidos) dados como comunicações de operações suspeitas, comunicações de operações em espécie, identificação de pessoas naturais e jurídicas (suspeitas e relacionadas a suspeitas), identificação de beneficiários finais, de sócios e representantes de empresas, participações societárias, lista de bens móveis e imóveis, histórico criminal etc.

Como dito, nem o dever imposto ao órgão de "coordenar e propor mecanismos de cooperação e de troca de informações" (art. 14, § 2º), nem mesmo sua competência para, "em todo território nacional", "promover a interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades" (art. 3º, II, Lei n. 13.974/2020) lhe franqueiam autorização legal para compartilhar dados pessoais (sigilosos ou não) com pessoas que não as do art. 15 da LLD. A cooperação e a troca de informações, assim, não poderia envolver dados pessoais (sigilosos ou não), a não ser que houvesse diploma legal (reserva de lei) autorizando o órgão a fazê-lo,[84] como poderia ser, por exemplo, um tratado internacional incorporado ao nosso direito positivo com hierarquia de lei federal.[85]

84. Segundo Teixeira, Wehrs e Madruga, a "troca de dados entre Unidades de Inteligência Financeira integrantes do Grupo Egmont não é regulada por convenção ou tratado internacional, mas apenas pelas normas e princípios do próprio Grupo" (Teixeira, Wehrs, Madruga, 2019, p. 22). O site do órgão igualmente não indica uma base legal para a cooperação, cf. https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/articulacao-institucional/ariticulacao-internacional-em-pld-ft (acesso em 11/09/2021). As Convenções de Mérida e de Palermo, incentivam a cooperação, mas sempre observada a legislação interna (Convenção de Mérida, art. 14, 1, b; Convenção de Palermo, art. 7, 1, b).

85. Pressuposto ligado à validade da cooperação ativa, mas que não necessariamente habilitaria o Brasil a receber dados de Estados estrangeiros dada a inexistência de infraestrutura legal de proteção de dados pessoais nesse âmbito. Nesse sentido, cf. ARAS, 2020, p. 14–31, p. 26 e ss. Um panorama do direito positivo brasileiro, do ambiente legal da União Europeia e da Convenção de Budapeste em Domingos, Abreu e Silva, Oliveira, 2020, p.140-162. Sobre as exigências de adequação ao standard de proteção europeu, cf. Morán Martínez, 2020, p. 163–196 e European Data Protection Board, 2021.

Poder-se-ia, talvez, deduzir essa permissão do próprio art. 15, que não teria limitado o rol de autoridades competentes às domésticas, a par de estar em conformidade com as recomendações do GAFI. Esse entendimento, porém, é questionável por algumas razões.

De um lado, o GAFI é um órgão intergovernamental, um fórum, que emite orientações e diretrizes para o combate à lavagem de capitais e financiamento do terrorismo. Suas recomendações não têm impacto vinculante em nosso direito positivo ("soft law"). De outro, dentro do regime de proteção de direitos, também as transferências internacionais devem ser veiculadas por norma legal proporcional, pois se trata de intervenção especialmente severa envolvendo alvos que estarão privados da tutela jurisdicional prestada pelo Poder Judiciário brasileiro,[86] feita sem exigência de que o receptor tenha um nível adequado de proteção de dados pessoais.[87] Além disso, "autoridades competentes para a instauração dos procedimentos cabíveis" têm sido compreendidas como autoridades competentes para a investigação e persecução penal de infrações penais,[88] algo que nem todas UIFs são, como serve de exemplo o próprio COAF. Quanto aos dados pessoais financeiros sigilosos, a LC 105, além de dever ser interpretada de forma restritiva,[89] não autorizou o COAF a transmitir esses dados para autoridades estrangeiras. Por fim, uma eventual invocação de atos normativos inferiores à lei (decretos, convênios, acordos de cooperação etc.) não supriria o que determina o art. 5º, II, da CF, pois "não há autorização constitucional a agentes não-parlamentares para que decidam, à margem do processo democrático, impor restrições a direitos de defesa que valem, principalmente, contra eles".[90]

Em um mundo no qual já se reconhece que não há dados irrelevantes, no qual a proteção de dados pessoais é um direito fundamental, no qual os diplomas legais nacionais e regionais que regulam a proteção de dados impõem uma série de requisitos para o intercâmbio internacional de dados e criam diversos mecanismos de proteção dos titulares afetados,[91] uma tal interpretação do art. 15 merece ser revista, por obsoleta e incompatível com essa nova realidade.[92]

Essas objeções não impedem, evidentemente, que uma autorização legal expressa e proporcional venha a ser veiculada pelo Poder Legislativo. Até lá, porém, a prática, nos limites das parcas informações acessíveis publicamente, não parece ser admissível.

IV À GUISA DE CONCLUSÃO

Ao fim deste exercício, fica patente que há muito a fazer em termos observância do princípio da legalidade e do respeito à proteção de dados pessoais num am-

86. No mesmo sentido, Teixeira, Wehrs, Madruga, 2019, p. 24. Os autores lembram, ilustrativamente, as autorizações expressas e detalhadas dadas pela lei alemã de lavagem de dinheiro, bem como pela portuguesa.

87. Como é feito, por exemplo, no âmbito da União Europeia, onde se exige uma decisão de adequação prévia da Comissão Europeia (art. 36, Diretiva UE 680/2018). Cf. European Data Protection Board, 2021. Ainda que se leve em conta o disposto no art. 33 da LGPD, o inciso VII, que poderia amparar a transferência, não faz tal exigência ao destinatário dos dados. De outro lado, o inciso III não se aplica à hipótese ora analisada, pois o Grupo Egmont não é um órgão público e nem sequer há um acordo de cooperação internacional que permita a invocação do inc. VI.

88. Cf. RE 1.055.941, voto Min. Gilmar Mendes, fl. 3073, 3075.

89. Cf. STF, RE 1.055.941, voto Min. Gilmar Mendes, fl. 3049, 3072

90. Gleizer, Montenegro, Viana, 2021, 44. Como dito, o Decreto 9.663, de 1º de janeiro de 2019, que aprova o Estatuto do COAF, não oferece fundamento legal para a transmissão, a distribuição, a comunicação, a transferência, a difusão ou disseminação de dados pessoais, sigilosos ou não, devendo a troca limitar-se a tipologias, dados estatísticos anonimizados etc. (cf. art. 16).

91. Apenas ilustrativamente, cf. LGPD, arts. 33 a 36; Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), arts. 41 a 45; Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016, arts. 35 a 40. O já mencionado Anteprojeto também sugeriu disciplina para a matéria em seus arts. 53 a 58.

92. Incompatibilidade que, a rigor, afeta, como um todo, o ambiente brasileiro relativo à prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. O Brasil, neste momento, não reúne condições mínimas para conseguir uma decisão de adequação para ser recipiente de dados oriundos do ambiente europeu (cf. o guia para adequação preparado pela autoridade europeia de proteção de dados, European Data Protection Board, 2021).

biente cujo tratamento de dados é tão amplo e intenso como o do COAF e feito para fins que podem conduzir à privação da liberdade de seus alvos.

Para que esse labor possa ser feito sem causar prejuízos irreparáveis às atividades de inteligência, de segurança pública e de persecução penal, poderíamos muito bem nos aproveitar daquilo que os alemães chamam de bônus de transição,[93] e nós chamamos de modulação de efeitos,[94] concedendo um prazo razoável para a adaptação da legislação às exigências da proteção de dados pessoais.

Enquanto essa legislação não vem e no atual ambiente, no qual apenas se aguarda a promulgação da PEC 17/2019, no qual a LGPD já está em vigor e, por fim, no qual o STF já tomou importantes decisões em prol da proteção de dados pessoais, é de se esperar que a Corte adote uma abordagem mais rigorosa tanto no que diz respeito tanto à exigência de autorização legal como no que tange à estrita observância dos limites legais para o tratamento de dados pessoais nos âmbitos da inteligência, da segurança pública e da persecução penal. No que interessa a este artigo, não admitindo RIFs a pedido, nem o intercâmbio internacional entre UIFs sem respaldo legal e sem garantia de infraestrutura normativa de proteção de dados pessoais pelo recipiente e reexaminando os limites do compartilhamento de dados financeiros sigilosos à luz desse novo cenário normativo.

93. Trata-se da concessão de um prazo ao legislador para que implemente as exigências relativas à proteção de dados. Cf. Greco, Leite, 2019; Greco, 2019, p. 47; Wolter, 2019, p. 167.

94. O Anteprojeto contém uma cláusula temporal de adequação no prazo da vacatio ali sugerida, que é de 365 dias (arts. 67 e 68). Talvez esse prazo deva ser ampliado dado o trabalho que deverá ser feito por juristas e parlamentares para adequar a legislação às exigências constitucionais no trato com dados pessoais.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; *et al* (Orgs.). *Tratado de proteção de dados pessoais*. São Paulo: Forense, 2021, p. 583–603.

ARAS, Vladimir Barros. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. In: DE MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; ARAS, VLADIMIR BARROS, Augusto; et al (Orgs.). Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020, p. 14–31.

AUTORIDADE EUROPEIA PARA PROTEÇÃO DE DADOS. Síntese do Parecer da Autoridade Europeia para a Proteção de Dados relativo à proposta da Comissão que altera a Diretiva (UE) 2015/849 e a Diretiva 2009/101/CE - Acesso a informações sobre os beneficiários efetivos e implicações para a proteção de dados, 2017.

BADARÓ, Gustavo. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: Direitos fundamentais e processo penal na era digital [livro eletrônico] / [editores] Francisco Brito Cruz, Bárbara Simão. São Paulo : InternetLab, 2021, sem paginação.

BALTAZAR JUNIOR, José Paulo. Sigilo bancário e privacidade. Porto Alegre: Livraria do Advogado, 2005.

BELLOQUE, Juliana Garcia. Sigilo bancário: análise crítica da LC 105/2001. São Paulo: Revista dos Tribunais, 2003.

BIALSKI, André, VENTO, Antonio, MESSINA, Eduardo, WIEGERINCK, Oliver. Transparência no tratamento de dados por UIFs: em busca de um benchmark. São Paulo, FGV-Data Privacy Brasil, 2021, no prelo.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. Revista Brasileira de Ciências Criminais, São Paulo, v. 176, p. 69–105, 2021.

BOTTINI, Pierpaolo Cruz. Os limites da atuação do COAF. Consultor Jurídico, 29/03/2021. Disponível em: <https://www.conjur.com.br/2021-mar-29/direito-defesa-limites-atuacao-coaf>. Acesso em: 08/08/2021.

COAF - CONSELHO CONTROLE DE ATIVIDADES FINANCEIRAS. Inteligência Financeira: Aspectos Práticos do Intercâmbio Internacional via Rede Egmont. [s.l.: s.n., s.d.]. Disponível em: <https://www.youtube.com/watch?v=i5N_LqLmewI>. Acesso em: 08/08/2021.

COMISSÃO DE JURISTAS DA CÂMARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, 2020.

DIMOULIS, Dimitri; MARTINS, Leonardo. Teoria geral dos direitos fundamentais. 8. ed., São Paulo: Revista dos Tribunais, 2021.

DOMINGOS, Fernanda Teixeira Souza; ABREU E SILVA, Melissa Garcia Blagitz; OLIVEIRA, Neide M. Cavalcanti Cardoso de. Transferência internacional de dados pessoais para fins de investigações criminais à luz das leis de proteção de dados pessoais. In: ARAS, Vladimir Barros; DE MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha (Orgs.). Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020, p.140-162.

DONEDA, Danilo. Da privacidade à proteção de dados. 2. ed., São Paulo : Revista dos Tribunais, 2020.

ESTELLITA, Heloisa; GLEIZER, Orlandino. A investigação penal de insuspeitos. Folha de S. Paulo, p. A3, 2020.

ESTELLITA, Heloisa; GLEIZER, Orlandino; MONTENEGRO, Lucas. Por um direito de segurança pública. Estadão, 05/10/2020. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/por-um-direito-de-seguranca-publica/>. Acesso em: 9 set. 2021.

EUROPEAN DATA PROTECTION SUPERVISOR. Opinion 1/2017 - EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications. [s.l.: s.n.], 2017.

_____. *Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing*. [s.l.: s.n.], 2020.

EUROPEAN DATA PROTECTION BOARD. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive - Adopted on 2 February 2021. 2021.

FERRAZ JÚNIOR, Tércio Sampaio. Comunicação de dados e proteção aos sigilo. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Boas (coord.). Lei geral de proteção de dados (Lei n. 13.709/2017): a caminho da efetividade. São Paulo: Thomson Reuters Brasil, 2020, p. 165-176.

GRECO, Luís, O inviolável e o intocável no direito processual penal: Considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). In: WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Madri; Barcelona; Buenos Aires; São Paulo: Marcial Pons, 2019, p. 21–82.

GRECO, Luís; GLEIZER, Orlandino, A infiltração online no processo penal - Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal, v. 5, n. 3, p. 1483–1518, 2019.

GRECO, Luís; LEITE, Alaor. Discussão do Supremo sobre caso Coaf joga luz em lacuna legislativa. Folha de S. Paulo, 19/11/2019. Disponível em: <https://www1.folha.uol.com.br/

poder/2019/11/discussao-do-supremo-sobre-caso-coaf-joga-luz-em-lacuna-legislativa.shtml>. Acesso em: 23 set. 2021.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. São Paulo: Marcial Pons, 2021.

GREENLEAF, Graham; TYREE, Alan, Bankers' Duties and Data Privacy Principles: Global Trends and Asia-Pacific Comparisons. In: BOOYSEN, Sandra; NEO, Dora (Orgs.). Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World. Cambridge: Cambridge University Press, 2017, p. 31–61.

KALKBRENNER, Arndt; KOCH, Christian. Bankgeheimnis und Datenschutz. 4. ed. Wiesbaden: DG Verlag, 2019.

KHAN, Sana. The Fourth AML Directive and the EU ' s Approach to Data Protection: A Precautionary Warning. ACAMS Today. 15/07/2016. Disponível em: <https://www.acamstoday.org/fourth-aml-directive-eus-approach-to-data-protection/>. Acesso em: 23 set. 2021.

LIMA, Renato Sérgio de; BUENO, Samira; MINGARDI, Guaracy. Estado, polícias e segurança pública no Brasil. Revista Direito GV, v. 12, n. 1, p. 49–85, 2016.

LUZ, Yuri. Bancos de dados públicos e o compartilhamento com agências penais. In: Direitos fundamentais e processo penal na era digital [livro eletrônico] / [editores] Francisco Brito Cruz, Bárbara Simão. São Paulo : InternetLab, 2021, sem paginação.

MALISH, Richard. Financial Crime and Compliance Management under GPR (White Paper). [s.l.]: NICE Actimize, 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 13. ed. São Paulo: Saraiva Educação, 2018, livro eletrônico.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar - Revista de Ciências Jurídicas, v. 25, n. 04, p. 1–18, 2020.

MORÁN MARTÍNEZ, Rosa Ana. Garantías requeridas en la UE para la transferencia internacional de datos a terceros países en la cooperación judicial penal. In: ARAS, Vladimir Barros; DE MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha (Orgs.). Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020, p. 163–196.

MOTA, Gibran Ayupe; HERKENHOFF, Henrique Geaquinto; LIRA, Pablo; et al. Constitucionalização da Atividade de Inteligência - Perspectivas e Desafios Brasileiros. Revista Brasileira de Segurança Pública, v. 12, n. 1, p. 134–150, 2018.

OLIVEIRA, Nina Ribeiro Nery. As novas resoluções do Banco Central e da Comissão de Valores Mobiliários e o sigilo dos dados compartilhados na forma da Lei 9.613/98. Revista de Direito Penal Econômico e Compliance, v. 4, p. 162–193, 2020.

PEÑA ZAFRA, Manuel. Vinculación entre protección de datos de carácter personal y prevención de blanqueo de capitales. *In*: *Estudios sobre controle del fraude fiscal y prevención del blanqueo de capitales*. Navarra: Thomson Reuters Aranzadi, 2016, p. 227–239.

PREZIOSI, Camilleri. Finding the balance between data protection and AML requirements. Lexology. Disponível em: <https://www.lexology.com/library/detail.aspx?g=8aabfbf8-33c1-456d-869b-ef1f56ec0e08>. Acesso em: 29 set. 2021.

ROGALL, Klaus, Moderne Fahndungsmethoden im Lichte gewandelten Grundrechtsverständnisses. Goltdammer's Archiv für Strafrecht, v. 1985, p. 1–27.

_____. Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht. Zeitschrift für die gesamte Strafrechtswissenschaft, v. 103, n. 4, 1991.

_____. § 53. In: WOLTER, Jürgen (Org.). Kommentar SK-StPO. [s.l.]: Carl Heymanns, 2018.

SALOMÃO NETO, Eduardo. Direito Bancário. 3ª ed., São Paulo: Trevisan, 2020.

SILVA, Virgílio Afonso da. Direito constitucional brasileiro. São Paulo: Editora Universidade de São Paulo, 2021.

SOARES, Hugo. Estupro, dever de comunicação às autoridades e titularidade da ação penal: reflexões derivadas da Resolução do Cremerj n. 296/2019, que estabelece a notificação de estupros aos órgãos competentes investigativos em casos atendidos por médicos no Estado do Rio de Janeiro. In: ESTELLITA, Heloisa; SIQUEIRA, Flávia (Orgs.). Direito Penal da Medicina. São Paulo: Marcial Pons, 2020, p. 347–356.

SOUTO, Gabriel; ROSAL, Isabela. *O direito à proteção de dados pessoais à luz da jurisprudência do STF*. LAPIN, 31/03/2021. Disponível em: <https://lapin.org.br/2021/03/31/o-direito-fundamental-a-protecao-de-dados-pessoais-a-luz-da-jurisprudencia-do-supremo-tribunal-federal/>. Acesso em: 8 ago. 2021.

SUPREMO TRIBUNAL FEDERAL. RE 377.457, Tribunal Pleno, rel. Min. Gilmar Mendes, DJe 18/11/2008.

_____. RE 593.727, Tribunal Pleno, Rel. Min. Cezar Peluso, DJ 08/09/2015.

_____. RE 1.055.941, Tribunal Pleno, Rel. Min. Dias Toffoli, julgado em 04/12/2019, DJe 06/10/2020.

_____. MC na ADI 6.529, Tribunal Pleno, Rel. Min. Cármen Lúcia, DJe 15/10/2020.

_____. ADI 6.387 MC-Ref, Tribunal Pleno, Rel. Min. Rosa Weber, DJe 12/11/2020.

TEIXEIRA, Adriano; WEHRS, Carlos; MADRUGA, Antenor. O valor processual das informações de inteligência financeira obtidas por meio do Grupo Egmont. *JCC*, v. 2, n. 2, p. 21–30, 2019.

VOGEL, Benjamin; MAILLART, Jean-Baptiste (ed.). National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection. Cambridge, Antwerp, Chicago: Intersentia, 2020.

WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2019.

07.

CASO COAF: CRITÉRIOS DE CLASSIFICAÇÃO E TRANSPARÊNCIA

Luiz Fernando Bugiga Rebellato

Honra-me o convite para uma reflexão acerca do "caso COAF" - Conselho de Controle de Atividades Financeiras, e seus precedentes para proteção de dados e investigações criminais, formulado pelo *InternetLab*, instituto de notório respeito pelo primor científico de seus trabalhos publicados e pelo elevado nível dos Congressos realizados, fruto da competência de seus integrantes.

A abordagem proposta perpassa, necessariamente, pela decisão do Supremo Tribunal Federal no Recurso Extraordinário n.º 10.55.941, que reconheceu a constitucionalidade do compartilhamento dos relatórios de inteligência financeira da UIF com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial:

> Repercussão geral. Tema 990. Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem 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 RFB referido no 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.
>
> (STF, Recurso Extraordinário n.º 1.055.941, Relatoria do Ministro Dias Toffoli, Tribunal Pleno, julgado em 4 de dezembro de 2019, DJe-243, divulgado em 5 de outubro de 2020 e publicado em 6 de outubro de 2020)

Entretanto, considerando que o tema foi objeto de extensa e profícua análise pelos demais integrantes do painel que honrosamente compus, proponho uma reflexão distinta, sob a ótica da proteção de dados e sua tratativa e processamento nas entranhas do referido órgão de inteligência, especialmente com relação à matriz de risco e seus critérios de classificação a partir de algoritmos predefinidos.

O ponto de partida para a análise se relaciona ao reconhecimento de um direito autônomo e individual de proteção aos dados pessoais, enquanto inerente à própria personalidade de seus titulares.

A proteção aos dados pessoais vem sendo objeto de recorrente preocupação normativa, à exemplo da Convenção n.º 108/1981 do Conselho da Europa, para proteção de pessoas a respeito do tratamento automatizado de dados pessoais; das Diretivas n.º 95/46/CE e 2002/58/CE, ambas do Parlamento Europeu e do Conselho Europeu, relacionadas respectivamente à proteção das pessoas singulares no tratamento de dados pessoais e da livre circulação desses dados; bem como da Decisão-Quadro 2008/977/JAI, do Conselho da União Europeia, que regulamentou a proteção de dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, posteriormente revogada e substituída pelo Regulamento

Geral de Proteção de Dados na União Europeia (*General Data Protection Regulation*), conforme Diretiva (UE) 2016/680.

De igual sorte, a Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, reconheceu em seu artigo 8º a proteção aos dados de caráter pessoal, bem como o Comitê de Direitos Humanos da Organização das Nações Unidas, em sua Recomendação n.º 16, disciplinou que os Estados deverão assegurar, sinteticamente, que informações a respeito da vida privada não estejam ao alcance de pessoas que não são autorizadas para recebê-las, processá-las ou utilizá-las.

Em cenário nacional, merece destaque a menção expressa pela Lei Geral de Proteção de Dados (artigo 2º, inciso II, da Lei n.º 13.709/2018) ao conceito de "autodeterminação informativa"[1], erigindo à condição de "fundamento" do referido diploma normativo.

Trata-se de noção extraída a partir da garantia da inviolabilidade do sigilo de dados, da intimidade e da vida privada (artigo 5º, incisos X e XII, da CF), bem como do princípio da dignidade da pessoa humana (artigo 1º, inciso III, da CF), sendo reconhecido como direito fundamental autônomo[2] conferido a cada cidadão [o direito] de ter, sob seu controle, as próprias informações; de determinar sobre a exibição e o uso de seus dados pessoais, delimitando-se o alcance do seu direito à privacidade; bem como de ter conhecimento sobre quem sabe e o que sabe sobre si, quando e em qual ocasião.

1. As primeiras noções de "autodeterminação informativa" foram trazidas a partir do célebre julgamento, pelo Tribunal Constitucional Alemão, do caso BVerfGE 65, 1, "Recenseamento" (Volkszählung), versando sobre a Lei do Censo Alemã de 1983. Na ocasião, a Corte alemã reconheceu reconhecida a capacidade do indivíduo de autodeterminar seus dados pessoais enquanto parcela fundamental do direito de desenvolver sua privacidade, embora tenha destacado que o direito à autodeterminação informativa não é absoluto (MARTINS, Leonardo (org.) Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 233-234). Sobre o tema, recomenda-se também: DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª ed. São Paulo: Editora RT, 2019, p. 165-172.

Ademais, a proteção aos dados recebeu substanciosa reccepção legislativa, deixando de ser um elemento vinculado à tutela de outros direitos (privacidade, intimidade, etc.) para ser reconhecido constitucionalmente como direito autônomo, inclusive em meios digitais (artigo 5º, inciso LXXIX, da Constituição Federal).[3]

Nesta perspectiva, é inegável que qualquer intervenção a este direito exige a observância de uma série de requisitos que o tornam legítimos: a observância à legalidade (a partir de leis, regulamentações e atos normativos que estabeleçam as hipóteses de tratamento dos dados), bem como do órgão legalmente autorizado para tanto, que deverá fazê-lo para uma finalidade específica; a fixação de critérios para o fluxo informacional entre os órgãos estatais de inteligência e de persecução penal; a obediência a um regular procedimento para coleta, utilização, compartilhamento e armazenamento destes dados.

Estabelecidos estes parâmetros, é necessário se avançar para a análise quanto à regularidade do tratamento de dados pessoais pelo COAF, especialmente diante de sua natureza enquanto órgão de inteligência.

Inicialmente, com relação à legalidade, não há dificuldades em se reconhecer que o COAF foi criado pelo artigo 14 da Lei n.º 9.613/1998 e sofreu sucessivas regulamentações (portarias, instruções normativas e resoluções próprias), que estabeleceram ao COAF a atribuição de produzir e gerir informações de inteligência financeira para a prevenção e o combate à lavagem de dinheiro, assim como o dever de promover a interlocução

2. Para Laura Mendes, o "(...) reconhecimento desse direito fundamental não é apenas uma possibilidade; trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado democrático de direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal (...)" (MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. p. 202).

3. Incluído pela Emenda Constitucional n.º 115 de 2022.

institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades (artigo 3º, incisos I e II, da Lei n.º 13.974/2020).

O COAF, enquanto órgão de atividade de inteligência financeira, é peça chave na gestão preditiva de crimes que rompem fronteiras [nacionais] e estão inseridos em uma proposta de governança internacional cooperativa (*v.g.*, terrorismo, corrupção, lavagem de capitais, etc.), especialmente a partir de um novo modelo de cooperação e compartilhamento de deveres entre o Estado e os demais setores da sociedade, a quem são impostas obrigações para pronta identificação e prevenção de atividades suspeitas que possam ser caracterizadoras da lavagem de dinheiro.[4]

4. A Exposição de Motivos da Lei nº 9.613/1998 estabelece, nos itens 81 a 86, a intenção de compartilhar a responsabilidade pelo combate da lavagem de capitais entre o Estado e os demais setores da sociedade.

Assim, nesta engrenagem participativa, e impulsionada por políticas de "*compliance*" e de "*know your costumer*", impostas às pessoas físicas e jurídicas de setores sensíveis – a quem são incumbidos os deveres de adotarem medidas preventivas para impedir que suas estruturas sejam utilizadas para a perpetração de lavagem de capitais e outros crimes[5] –, o COAF passou a ser um dos principais órgãos responsáveis pela recepção das informações atípicas e daquelas tidas por "suspeitas" (artigo 11 da Lei n.º 9.613/1998), processando os dados dentro de critérios e procedimentos internos que podem culminar com a geração de relatórios de inteligência financeira ("RIFs"), a serem posteriormente remetidos às autoridades competentes na persecução criminal.

5. BARROS, Marco Antonio de. Lavagem de capitais e obrigações civis correlatas: com comentários, artigo por artigo, à Lei 9.613/98. 3. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2012. p. 308-309.

Ainda em relação à finalidade no tratamento dos dados, é imprescindível que estes não possam ser tratados para fins diversos daqueles estabelecidos na prevenção e combate à lavagem de capitais, terrorismo e outros delitos graves. De igual sorte, a base de dados do COAF não poderá servir para finalidades desproporcionais ou distintas daquelas que ensejaram a criação do órgão, tais como para se instruir procedimentos de natureza cível (TJSP: Agravo de Instrumento n.º 2132188-88.2021.8.26.0000, 8ª Câmara de Direito Privado, Rel. Des. Pedro de Alcântara da Silva Leme Filho, julgado em 26 de junho de 2021).

Por se tratar de um órgão dotado de elevado grau de concentração de dados pessoais, os cuidados com a sua preservação e o tratamento dentro das finalidades legais exige o estabelecimento de bases procedimentais para seu processamento, com critérios transparentes e sindicáveis, dentro da própria unidade de inteligência.

Conforme se verá a seguir, desde a recepção dos dados até a oportuna elaboração dos relatórios de inteligência financeira ("RIF"), o processamento dos dados segue uma série de etapas perante o próprio COAF, conforme previsão estabelecida no próprio *site* oficial do Governo Federal.[6]

A primeira etapa a ser observada corresponde às comunicações recebidas pelo COAF, a partir dos "setores obrigados" que detêm a obrigação legal de fornecer as informações ao referido órgão de inteligência.

Enquanto detentoras de dados pessoais (que lhe foram confiados por clientes e usuários), as entidades têm o dever de zelar por sua integridade e resguardá-los de compartilhamento com terceiros sem prévia autorização ou obrigação legal. Portanto, a fim de se evitar que o tratamento[7] dos dados ocorra de forma discricionária, foram estabelecidas duas

6. https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/analise-de-informacoes.

7. Valendo-se do conceito de tratamento como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (artigo 5º, inciso X, da LGPD).

formas específicas de compartilhamento de dados entre os "setores obrigados" e o COAF: a) *Comunicação de Operação em Espécie (COE);* b) *Comunicação de Operação Suspeita (COS)*.

Na primeira espécie, as comunicações são realizadas automaticamente pelos "setores obrigados" ao COAF, especialmente diante da realização de transações em espécie acima de determinado valor (artigo 10, inciso II e artigo 11, inciso II, alínea b, ambos da Lei n.º 9.613/1998). Neste caso, independentemente de qualquer análise interna corporis pelos referidos setores indicados no artigo 9º da Lei n.º 9.613/1998, a transação atípica[8] – o que não configura, necessariamente, uma atividade suspeita – é informada ao COAF, o qual não disporá de detalhamento relacionado ao extrato bancário do responsável pela realização da transação atípica. Com efeito, a comunicação se limita ao valor da operação, a identificação do titular da conta, a pessoa que efetuou a operação, o proprietário do dinheiro e dados cadastrais bancários, (tais como conta, agência, banco e cidade).

8. *V.g.*, o artigo 4º, inciso I, da Resolução n.º 25, de 16 de janeiro de 2013, estabelece o dever de ser comunicado ao COAF, independentemente de análise ou qualquer outra consideração, qualquer operação ou conjunto de operações de um mesmo cliente no período de seis meses que envolva o pagamento ou recebimento de valor igual ou superior a R$ 30.000,00 (trinta mil reais) ou equivalente em outra moeda, em espécie.

Como se vê, atingido um critério objetivo e previamente fixado pelas autoridades competentes, a partir de instruções infralegais expedidas, a transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ou qualquer ativo passível de ser convertido em dinheiro (artigo 11, inciso II, da Lei n.º 9.613/1998) é considerada atípica e, portanto, deve ser comunicada, sem qualquer exigência de se perquirir a existência de "sérios indícios" de crimes previstos na Lei de Lavagem de Capitais, ou que com ele guardem relação.

/ O COAF PASSOU A SER UM DOS PRINCIPAIS ÓRGÃOS RESPONSÁVEIS PELA RECEPÇÃO DAS INFORMAÇÕES ATÍPICAS E AQUELAS TIDAS POR "SUSPEITAS /

/ AS ENTIDADES TÊM O DEVER DE ZELAR POR SUA INTEGRIDADE E RESGUARDÁ-LOS DE COMPARTILHAMENTO COM TERCEIROS /

Por sua vez, a *Comunicação de Operação Suspeita (COS)* é realizada pelos setores obrigados quando estes perceberem a ocorrência, nas transações realizadas por clientes, de "sérios indícios" de lavagem de capitais, financiamento do terrorismo e outros ilícitos. Nesta etapa, a "suspeita" que motiva a comunicação é construída a partir de critérios legais e regulamentares, dentro de políticas de controle e procedimentos (*due diligence* e *know your costumer)* para avaliação de riscos e escrutínio contínuo das transações realizadas. Trata-se da previsão normativa contida no artigo 11, inciso I, da Lei n.º 9.613/1998.

Ainda, a comunicação ao COAF poderá partir de autoridades competentes, inclusive de órgãos de persecução penal, que comunicam ao COAF [detalhes sobre] as investigações em curso sobre determinados suspeitos. A hipótese, que vem ao encontro do dever de interlocução institucional do COAF com órgãos e entidades nacionais (artigo 3º, inciso II, da Lei n.º 13.974/2020), está relacionado à necessidade de uma atuação cooperada e de troca de informações, em ações rápidas e eficientes, no combate à ocultação ou dissimulação de bens, direitos e valores.

A partir da comunicação realizada pelos setores obrigados, através da plataforma SISCOAF (Sistema de Controle de Atividades Financeiras), os dados são objeto de três etapas de processamento.

A primeira consiste na avaliação do risco da operação e das partes envolvidas, por intermédio de regras de seleção previamente definidas.[9]

Ato contínuo, uma segunda etapa consiste na análise dos dados através de um "modelo preditivo", que promove a seleção das comunicações e permite uma análise individualizada, a partir da probabilidade de a comunicação conter elementos de risco.

9. https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/analise-de-informacoes.

Se a comunicação for selecionada pelo "modelo preditivo", a comunicação é remetida a um dos analistas do COAF, em distribuição aleatória realizada próprio SISCOAF (o que impediria a seleção específica de uma comunicação por parte dos analistas), assegurando-se a impessoalidade na análise dos dados comunicados.

Finalmente, cabe ao analista registrar as informações em uma "matriz de risco", que "*estabelece automaticamente o nível de risco da comunicação, somando os pontos calculados de cada fator de risco identificado. Esses fatores podem ser referentes à forma de movimentação comunicada, às partes envolvidas, às regiões geográficas apontadas, à existência de investigações em curso, dentre outros. A análise individualizada é, portanto, uma terceira etapa de verificação*".[10]

10. Idem.

A matriz de risco é estabelecida por uma sequência de mecanismos de filtragem que promovem pontuações aos riscos, de modo que, caso atingida a referida pontuação, o registro e as demais bases de dados armazenadas no COAF passam a integrar um processo eletrônico, registrado em uma Central de Gerenciamento de Risco e Prioridades (CGRP), o qual será distribuído a outro analista para uma análise aprofundada, em uma pasta eletrônica virtual chamada "*caso*".

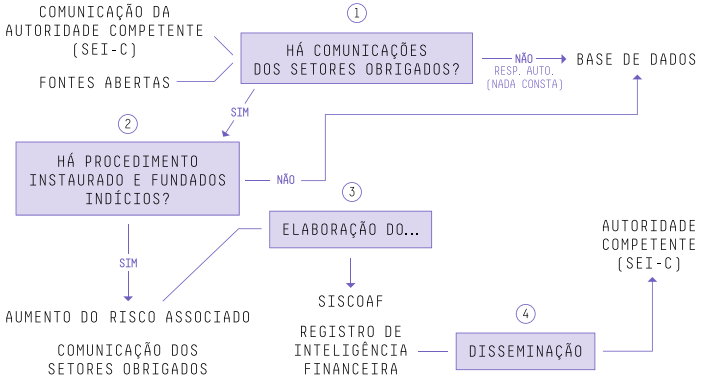
Nesta última etapa de análise conjunta dos dados com as informações contidas no SISCOAF sobre o investigado, é aferido se o procedimento de investigação é válido e atende aos critérios de realização de análise.

As informações deverão ser analisadas em cotejo com outros bancos de dados existentes sobre a pessoa investigada, composto por fontes abertas (v.g., pesquisa no Google) e outras "restritas" (*Rede Infoseg*), Cadastro de Pessoas Físicas (CPF), Cadastro Nacional de Pessoas Jurídicas (CNPJ), Declaração de Operações Imobiliárias (DOI), Cadastro Nacional de Informações Sociais (CNIS), Cadastro de Pessoas Expostas Politicamente (Cadastro de PEPS), Prestação de Contas Eleitorais do TSE, Cadastro Nacional de Empresas (CNE), Base de Grandes Devedores da União, Bases do Tribunal Superior Eleitoral, Declaração de Porte de Valores (e-DPV).

Uma vez constatados indícios de lavagem de capitais, financiamento ao terrorismo ou outros delitos conexos e igualmente graves, o COAF elaborará um Relatório de Inteligência Financeira ("RIF"), com posterior distribuição às autoridades competentes (artigo 15 da Lei n.º 9.613/1998).

A dinâmica do processamento dos dados pode ser representada pelo esquema gráfico abaixo, extraído do Relatório de Inteligência do COAF de 2021[11]:

11. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf



Conforme se extrai do roteiro de análise de informações publicado no *site* do Governo Federal, há um procedimento específico, delimitado e segmentado em três etapas, que disciplinam a análise e processamento dos dados, desde sua comunicação até a eventual elaboração do Relatório de Inteligência Financeira ("RIF"), privilegiando-se uma tratativa

automatizada dos dados e a observância de critérios que assegurem a impessoalidade na análise e nas conclusões.

No acórdão que fixou a possibilidade de compartilhamento do Relatório de Inteligência Financeira (RIF) do COAF com os órgãos persecutórios (conforme prevista contida no artigo 15 da Lei n.º 9.613/1998), o Ministro Dias Toffoli reconheceu que *"(...) o sistema de UIF adotado pelo Brasil está de acordo com os padrões internacionais. A relação entre a UIF e o sistema financeiro deve ser tão aberta quanto tem sido, e não vejo sua forma de proceder como uma afronta à garantia constitucional do sigilo financeiro (...)"* (STF, RE 1055941, julgado em 04/12/2019, p. 37 do voto).

Entretanto, o acórdão paradigma da Corte Suprema deixou de avançar sobre um aspecto essencial no tocante ao tratamento dos dados perante o COAF, especialmente com relação à composição dos algoritmos e elementos que permitam a aferição e valoração dos critérios de risco, a partir da matriz desenvolvida para sua constatação.

Nesta senda, embora o procedimento observe a legalidade e critérios aparentemente objetivos para tratamento e processamento dos dados, alguns pontos merecem uma reflexão, no que chegamos ao ponto nevrálgico de nossa análise.

Com efeito, nas comunicações realizadas automaticamente, é certo que estas são submetidas a uma análise sistêmica, realizada eletronicamente pelo SISCOAF, com regras de seleção previamente definidas a partir da identificação de fatos e fenômenos específicos que, em princípio, não apresentam riscos potenciais de lavagem de dinheiro, terrorismo, proliferação de armas de destruição em massa e outros ilícitos.

Essas regras, chamadas de *regras de diferimento automático*, são acionadas nas hipóteses de baixíssimo risco associado ou a comunicações suspeitas sem detalhamentos mínimos de atipicidade constatada, o que torna a comunicação "diferida", sendo registrada apenas na base de dados para consulta.

Nesta etapa, já floresce uma primeira questão relacionada aos elementos integrativos das referidas *regras de diferimento automático,* que serão fundamentais para a separação entre as informações representativas do risco e aquelas que apenas integrarão uma crescente base de dados.

Em verdade, a menção à automatização do sistema de aferição de risco não afasta a necessidade de se verificar quais os algoritmos programados para a análise eletrônica do conteúdo dos dados, especialmente para aferir-se a legitimidade, legalidade e a adoção de padrões efetivamente impessoais na coleta, análise e determinação do grau do risco aferido.

Em outras palavras, a mera referência à utilização de critérios objetivos para processamento dos dados dentro da matriz de risco nos parece insuficiente para aferir a regularidade no tratamento, especialmente se considerarmos que o algoritmo utilizado para a fixação de padrões de risco e sua classificação constitui verdadeiro produto de ação humana, produto de uma série de interações, conflito de valores, interesses e programação tecnológica.[12]

A falta de transparência quanto aos critérios utilizados pelo COAF para tratamento dos dados é constatada, também, na composição dos elementos que integram a "matriz de risco", que estabeleceria automaticamente o nível de risco da comunicação.

Trata-se de fator de especial relevância, à medida que os "filtros" utilizados nesta matriz permitirão definir se o risco é "baixo", "médio" ou "alto" - sendo que, nestas duas últimas hipóteses, haverá a análise destes dados em conjunto com outros integrantes da base de dados do COAF, para a composição de um processo eletrônico chamado "*ca-*

12. PERON, Alcides; ALVAREZ, Marcos César. O sistema detecta em São Paulo e o papel do vigilantismo nas práticas de segurança da cidade. In: BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos fundamentais e processo penal na era digital. São Paulo: InternetLab, 2020, v. 3. p. 160.

13. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf.

so", que será registrado na Central de Gerenciamento de Risco e Prioridades (CGRP).[13]

Portanto, a "matriz de risco" exige o aclaramento dos os índices e elementos de filtragem que a compõem, para permitir o tratamento dos dados e sua submissão automatizada - assim como é necessário na elaboração dos critérios de pontuação para constatação do risco em "baixo", "médio" ou "alto", especialmente considerando que o seu resultado trará diferentes consequências. Pode haver, inclusive, consequências de cunho persecutório com a subsequente elaboração e compartilhamento do Relatório de Inteligência Financeira ("RIF").

Ao mesmo tempo, não se pode fechar os olhos para a necessidade de um órgão de inteligência financeira resguardar um certo sigilo nos elementos que compõem sua matriz de risco, uma vez que sua revelação, de forma absolutamente aberta e transparente, pode comprometer e inviabilizar o próprio exercício da atividade de inteligência financeira.

Em verdade, o aclaramento absoluto permitiria que os criminosos soubessem quais os critérios utilizados e, por conseguinte, buscassem meios para evitar serem flagrados nos "filtros" e algoritmos que compõem a referida "matriz de risco".

Finalmente, com relação à comunicação do Relatório de Inteligência Financeira (RIF) com os órgãos persecutórios, chega-se à hipótese de interlocução entre o produto do exercício das atividades de inteligência (financeira, policial, etc.) e a atividade persecutória criminal, cuja atuação compartilhada já foi admitida.

De início, impende destacar que o Relatório de Inteligência Financeira (RIF) não deve ser considerado como meio probante, mas apenas elemento que possa subsidiar uma investigação, à medida que sequer é acompanhado de dados relacionados ao sigilo fiscal ou extratos bancários, já que o próprio COAF não dispõe de acesso a estes elementos.[14]

O compartilhamento de informações poderá se dar através da chamada "*disseminação espontânea*", ocasião em que o órgão de inteligência deverá ser capaz de reportar as informações e resultados de suas análises para as autoridades competentes, quando houver suspeita de lavagem de dinheiro, crimes antecedentes ou financiamento do terrorismo.

Entretanto, o caminho inverso também é admitido, de modo que o COAF poderá promover a *"disseminação a pedido"*, respondendo a pedidos de informações de autoridades competentes de acordo com a Recomendação 31 do GAFI.

Porém, há de se destacar que este compartilhamento não pode subverter a natureza do COAF, enquanto órgão de inteligência financeira e, portanto, não dotado de capacidade investigativa. Assim, o COAF não pode realizar atividades investigativas e engendrar esforços, junto aos setores obrigados, para obtenção de informações das quais não dispunha previamente em seu banco de dados, especialmente nos casos de operações "suspeitas" (STJ, AgRg no RHC n.º 125.643/RJ, 5ª Turma, Rel. Min. Felix Fischer, julgado em 16 de março de 2021, DJe 08/04/2021). Do contrário, a atividade de inteligência se transmudaria em atividade persecutória e a atuação do órgão flertaria com o "*fishing expedition*",[15] que consiste na utilização de meios probatórios legais para a obtenção de toda e qualquer evidência em face de uma pessoa, tenha ou não relação com o caso concreto, o que se desenvolve como uma investigação especulativa e demasiadamente ampla.[16]

Outrossim, deve ser reafirmada a autonomia técnica e operacional do COAF (conforme artigo 2º da Lei n.º 13.974/2020) no tocante ao fornecimento das informa-

14. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf.

15. A utilização da *fishing expedition*, também chamada de "efeito hidra" (SCHÜNEMANN, Bernd. La Reforma del Proceso Penal. Madrid: Dykinson, 2005, p. 33), é medida ilegal, conforme jurisprudência da Corte Suprema: STF, HC n.º 163.461/PR, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 5 de fevereiro de 2019, DJe 03/08/2020; STF, RE n.º 1.055.941, Rel. Min. Dias Toffoli, julgado em 4 de dezembro de 2019, DJe 06/10/2020; STF, Inq n.º 4.831/DF, decisão do Min. Celso de Mello, 5 de maio de 2020

ções solicitadas, de modo que os órgãos de investigação não poderão requisitar ou obrigar o COAF a fornecer as informações que possua em seu banco de dados.[17] Assim, não há relação de subordinação entre os órgãos persecutórios e os de inteligência, mas apenas um dever de cooperação entre todos, especialmente na prevenção e combate a crimes de especial gravidade.

Ademais, as comunicações devem ser realizadas a partir de um sistema próprio, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios – *Sistema Eletrônico de Intercâmbio (SEI-C)*.

Assim, conclui-se que o acórdão do Supremo Tribunal Federal (STF), ao analisar o compartilhamento de informações do COAF com os órgãos persecutórios, deixou de se atentar para um conjunto de temas relacionados à proteção de dados pessoais, especialmente com relação aos critérios utilizados para processamento e definição do grau de risco da comunicação, quando de sua análise dentro da própria estrutura do COAF.

Não parece suficiente a alegação de que a impessoalidade e objetividade se contente com a existência de um arcabouço metodológico que abrange regras definidas por especialistas da área, a análise de dados por dois analistas distintos, modelos de *machine learning* e avaliação individualizada orientada por critérios objetivos.[18]

A automatização, conquanto salutar e indicativa de impessoalidade, é orientada por critérios algoritmos preestabelecidos, os quais não são conhecidos nem bem esclarecidos, inviabilizando que se saiba como as informações são tratadas, classificadas e individualizadas.

16. SILVA, Viviane Ghizoni da; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. Fishing Expedition e Encontro Fortuito na Busca e Apreensão. Florianópolis: Editora Emais, 2019, p. 41.

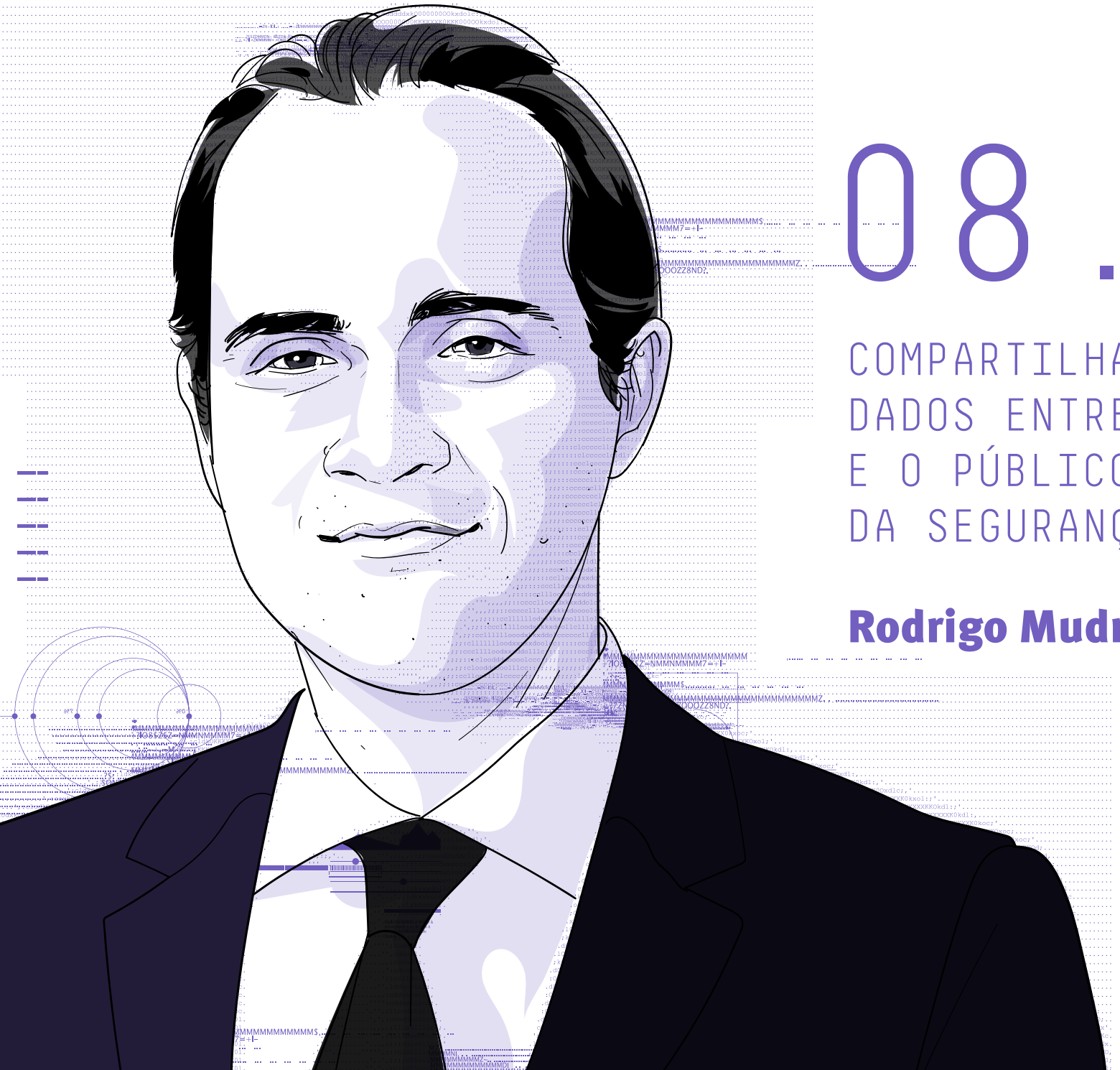
17. No mesmo sentido é a Recomendação n.º 29 do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF).

18. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf.

O sigilo da "matriz de risco", conquanto essencial para o exercício da atividade financeira, não pode ser absoluto, de modo que deve ser trilhado um caminho intermediário, que não se direcione para a revelação irrestrita dos critérios utilizados na "matriz de risco" mas, ao mesmo tempo, permita sua sindicabilidade e controle, a ponto de se aferir se obedecem a efetivos aspectos objetivos, impessoais e isonômicos.

Portanto, é imperiosa a adoção de medidas para ampliar a transparência nas *regras de diferimento automático*, especialmente na modulação dos critérios para associação do que é "atípico" ou potencialmente suspeito, bem como se trazer maior diafaneidade na formatação dos mecanismos utilizados na marcação da "matriz de risco" e respectiva pontuação, para conclusão sobre "risco baixo", "risco médio" e "risco alto", a motivarem a abertura de casos e geração de relatórios de inteligência financeira.

Somente assim se permitirá que os titulares dos dados saibam que suas informações pessoais, asseguradas constitucionalmente e aliadas ao conceito de autodeterminação informativa, não serão tratadas de forma subjetiva ou arbitrária, em afronta às legislações brasileiras e internacionais que asseguram o tratamento vinculado a uma finalidade legal, específica e proporcional.



08.

COMPARTILHAMENTO DE DADOS ENTRE O PRIVADO E O PÚBLICO NO ÂMBITO DA SEGURANÇA PÚBLICA

Rodrigo Mudrovitsch

Obrigado, Clarice! Quero cumprimentar você e meus colegas de painel, Dra. Carolina e Dra. Bárbara. É uma alegria e uma honra enorme poder participar dessa discussão tão importante e tão bem ladeada. Espero também contribuir de alguma forma com o debate e estou totalmente aberto a qualquer questionamento que eventualmente venha a ser feito.

O tema da nossa conversa é o compartilhamento de dados entre privado e público, no âmbito da segurança pública. Tem-se ouvido muito falar o termo que coloca - eu acho que é um termo importante - que nós vivemos hoje num "capitalismo de vigilância", que é marcado por uma assimetria de poder enorme entre cidadãos e Estado. O fato é que nós temos uma Lei Geral de Proteção de Dados (LGPD) que regulamenta as questões sob a perspectiva do direito civil. Quando olhamos para a seara penal - a temática do nosso encontro, no âmbito da segurança pública - temos um vácuo legislativo. Levando em consideração a vigilância extrema em que se vive e essa assimetria de poder entre cidadão e Estado, o vácuo legislativo leva a uma tentativa de regulamentação do tema através de uma interpretação a partir de uma ponte constitucional. Ou seja, tentar, a partir das garantias funcionais e penais existentes no texto constitucional, feitas em outro contexto e que são lacônicas com relação ao tema, buscar as melhores soluções para os problemas que existem na prática, e que, como as colegas que me antecederam muito bem colocaram, não são poucos. É a partir do vácuo legislativo que nos sobra examinar as questões a partir dos dispositivos previstos no artigo 5º da Constituição, notadamente os incisos X e XII.

É importante colocar, já numa fase inicial da minha fala, que nós temos uma iminência de aprovação da PEC 17/2019, já aprovada em dois turnos, a última no dia 31 de agosto de 2021, inserindo uma disciplina mais precisa no inciso XII.[1] Dessa forma, a leitura do texto terá um acréscimo. Ao que já existia, "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal", será acrescido: "bem como é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais". E essa inclusão da proteção, especificamente, no rol do artigo 5º da Constituição, além da maior estatura, impulsiona um debate sobre implementação de acessos de fluxo de dados pessoais e tende a ser uma forma de contenção de um avanço do Estado dentro de um capitalismo de vigilância com uma assimetria de poder significativa.

Algumas questões têm aparecido nessa discussão e são relevantes para que nós pensemos a problemática. Na perspectiva da segurança pública, nós perguntamos, por exemplo, quando temos a discussão relacionada ao direito à privacidade sob a perspectiva de garantia da segurança pública. Nós temos a possibilidade de que o Estado utilize justificativas cíveis e penais? Por exemplo, se nós tivermos uma situação de catástrofe ou de calamidade pública, como recentemente, o Estado pode acessar os dados do cidadão para garantir a segurança de determinada região? No ápice da pandemia, chegamos a ter propostas sobre acesso a geolocalização dos indivíduos para controle sobre a disseminação do vírus. O reconhecimento facial disseminado, tal como está ocorrendo, é um cenário de hipervigilância, sob a perspectiva de garantir a segurança pública. Como o reconhecimento facial em aeroportos, em transportes públicos e em eventos. Isso torna a segurança um pouco mais eficaz ou eventualmente pode fazer com que, a pretexto de segurança

1. Agora a Emenda Constitucional Nº 115, de 10 de fevereiro de 2022, que altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

pública, se tenha um controle estatal privado de dados individuais? E como vão manusear essas informações? Como vai ser feita a utilização e o descarte disso?

Outro problema que também é relevante com relação à privacidade é o da criptografia de ponta a ponta. Porque, muitas vezes, o que se discute é: quando você a tem de uma forma que garanta integralmente a privacidade das conversas do cidadão, você por outro lado também priva o Estado de qualquer tipo de acesso preventivo ou repressivo. E isso coloca os Estados, talvez, numa posição de vulnerabilidade. É justificado, então, eventualmente reduzir a privacidade, de forma a garantir que o Estado tenha mais acesso a esse tipo de informação? Veja que eu coloquei três pilares, mas poderia colocar outros.

Quanto à intimidade, nós também temos outros questionamentos. Nós temos aqui no Brasil um elevado fluxo de vazamento de dados. Isso está longe de ser uma exceção. A gente pode chegar até o ponto de dizer que virou uma regra, especialmente vazamentos de operações policiais, muitas vezes sigilosas, ou mesmo o vazamento de bases extensas de dados. O que temos, muitas vezes, é o acesso indevido e falta de segurança nos órgãos públicos, a falta de estrutura de cibersegurança e, muitas vezes, vazamento de dados que estão sob o poder do Estado. O que acontece é que, muitas vezes, a transferência dessas informações também pode levar a um problema, porque a custódia, muitas vezes, não é feita, ou por falta de aparelhamento, ou falta de regra ou por falta de cuidado. E isso tem se agravado pelo fato de que grande parte das informações são provenientes do setor privado. Logo, é possível que se estabeleça uma forma de transmissão dessas informações? Ou seja, das informações sobre indivíduos que se concentram em redes sociais ou documentos armazenados em telefones, em nuvens, em bancos, enfim.

Uma série de questões que nós temos hoje, como os lugares em que se armazenam esses dados, como fazer uma estrutura segura e parâmetros de controle para que ocorra a transmissão dessas informações, e como isso pode ser feito a partir de uma justificativa legítima de acesso, com uma legítima finalidade pública? E como vai ser feito depois o descarte disso?

São questões que, quando olhamos para esse vácuo legislativo que eu apontava no começo (e que começa a ser suprido a partir da perspectiva constitucional), na perspectiva penal ainda têm um vácuo legislativo posto, a interpretação passa a ser muito difícil. Então, o retrato atual, hoje, é o de trabalhar esse tipo de situação a partir de regras gerais. Como mencionei inicialmente, nós temos uma interpretação de porte constitucional e nós temos algumas regras gerais de quebra de sigilo. Então, a ordem judicial como regra, a partir da interpretação da Lei de Interceptação Telefônica (Lei nº 9296/96), especialmente a partir da lei 12.850/13, é de que há alguns dados pessoais, como dados cadastrais e dados de geolocalização - dados que muitas vezes as pessoas fornecem sem nem saber que estão fornecendo -, para os quais o acesso pelo Estado não dependeria da necessidade de uma ordem judicial prévia, especialmente quando se discute crime de organização criminosa e lavagem de ativos. Esse tema está em julgamento ainda pelo Supremo, é uma lei que tem impugnação. O julgamento se iniciou mas ainda não terminou, teve um pedido de vista do ministro Nunes Marques. Mas é uma discussão que permite que, na prática, tenha-se a possibilidade de acesso a tipos de dados (dados cadastrais e dados de geolocalização), que muitas vezes as pessoas nem sabem que estão fornecendo ao Estado sem ordem judicial prévia. Então, esse seria um estado geral do compartilhamento no que toca às regras gerais de quebra de sigilo.

E o que nós temos, também, é um intuito cada vez mais forte das autoridades - isso é importante que seja colocado - de realizar interceptações entre as pessoas investigadas, através de acesso às plataformas digitais e aos aplicativos de comunicação. Há uma resistência cada vez mais forte por parte do poder estatal, dentro desse capitalismo de vigilância, dentro de uma assimetria de poder, que deve ser levado em consideração, para que se cumpram ordens judiciais de interceptação, mesmo existindo a criptografia de ponta a ponta. Ou seja, há uma resistência com relação a isso. Não é longe da nossa história, os bloqueios que o WhatsApp sofreu, quando deixou de cumprir algumas ordens judiciais que, muitas vezes, atentaram contra [os direitos de privacidade], sob a perspectiva de uma posição de garante do Estado e que exigiria que, para esse tipo de informação, fosse facultado o acesso.

Ainda nessa parte do estado geral da questão, temos as técnicas de reconhecimento facial, que muitas vezes são utilizadas pelos governos de forma indiscriminada. E que são utilizadas na perspectiva, não de controle, mas de se chegar ao que nós chamamos de "monitoramento por arrastão". Capturam-se dados biométricos, que são dados sensíveis, de determinados indivíduos, em prol de uma persecução penal que, não raramente, é sequer bem delimitada. Nós temos, nesse caso, uma assimetria de poder informacional entre cidadãos e o Estado, sendo realizada quase como uma *fishing expedition*[2] - que nós conhecemos em outro contexto, mas é o que se tem quando tem no monitoramento por arrastão.

2. Uma phishing expedition (em português, uma expedição de pesca) é um termo informal e pejorativo para uma busca não específica de informação, especialmente informação incriminatória. É mais frequentemente organizada pelas autoridades de policiamento.

Neste caso, não no que toca à perspectiva do indivíduo afetado, mas da pluralidade de indivíduos afetados com relação a isso, o problema que se coloca é que nós não temos *accountabi-*

/ É UM INTUITO CADA VEZ MAIS FORTE [...] DE REALIZAR INTERCEPTAÇÕES ENTRE AS PESSOAS INVESTIGADAS /

/ O REFLEXO DESSE ANTEPROJETO É, ESSENCIALMENTE, ASSEGURAR O PRINCÍPIO DA PRESUNÇÃO DE INOCÊNCIA, *IN DUBIO PRO REO*, DA NÃO INCRIMINAÇÃO /

lity[3] por parte dos órgãos investigadores que permita, pelo menos, que se tenha algum tipo de controle - ainda que não prévio, mas posterior - no que toca aos indivíduos que estão sendo investigados. A posição de vulnerabilidade existe, ela se agrava nesse tipo de situação, em que se tem as quebras de sigilo "por arrastão". E isso é agravado no contexto em que a interpretação vigente, a partir da Lei de 12.850 de 2013,[4] uma interpretação que dispensa a ordem judicial prévia desse tipo de controle, o qual muitas vezes permite um acesso indiscriminado do Estado a dados críticos, como a geolocalização, e em que muitas vezes os indivíduos não sabem que estão fornecendo essas informações.

Para além disso, há algumas dúvidas que os tribunais ainda estão tentando solucionar. A primeira delas é a possibilidade da autoridade policial ter acesso a um celular apreendido sem consulta prévia ao magistrado. Porque nós sabemos que, numa operação de busca apreensão, por exemplo, essencialmente, as autoridades querem ter acesso ao aparelho celular do indivíduo. O Supremo ainda não tem uma jurisprudência pacificada sobre isso. Muito embora já exista, dentro do Supremo, o entendimento quanto à existência de um direito autônomo à proteção de dados pessoais (isso foi estabelecido já no conhecido julgamento das Ações Diretas de Inconstitucionalidade, da relatoria da ministra Rosa Weber, ADIS 6.389, 6.390, 6.393, 6.388 e 6.387), não há ainda uma participação da jurisprudência no âmbito do Supremo.

Já no âmbito do Superior Tribunal de Justiça, o que se entende, então, é uma interpretação extensiva protetiva dos cidadãos, o que eu acho que é importante, porque face à vulnerabilidade e à assimetria, é necessário que o Poder Judiciário olhe numa forma mais hiperbólica das garantias individuais.

3. N/E: Termo inglês, em tradução livre, correspondente à ideia de "responsabilização" ou "prestação de contas".

4. N/E: A Lei de Organizações Criminosas.

Há, portanto, [no STJ], o entendimento de que deve existir sim a autorização judicial específica para que se possa ter essa quebra de sigilo que, muitas vezes, é mais gravosa do que a própria quebra de intimidade que se pretendeu autorizar a partir da ordem de busca apreensão. É o julgamento, já também famoso do STJ, do Habeas Corpus 51.531. Vou ler aqui só um curto trecho, que eu acho importante, onde onde foi colocado: "atualmente, o acesso ao aparelho de telefonia celular de pessoa presa em flagrante possibilita à autoridade policial o acesso a inúmeros aplicativos de comunicação em tempo real, todos eles com as mesmas funcionalidades de envio e recebimento de mensagens, fotos, vídeos e documentos em tempo real. Após baixados automaticamente, ficam armazenados na memória do telefone, cabendo ressaltar que a maioria das empresas que disponibilizam tais serviços, não guardam os referidos arquivos em seus servidores". Isso o ministro Rogério Schietti disse à época. O ministro Nefi Cordeiro colocou que o celular "deixou de ser um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso a múltiplas funções, o que mostra a necessidade de uma proteção jurídica mais sólida e mais detalhada". E aqui há um vácuo legislativo, que exige que a navegação por parte dos magistrados seja uma navegação complexa, muitas vezes através de interpretação de normas genéricas e vagas.

A outra questão que também chegou aos tribunais superiores, ainda no contexto do estado geral das interceptações, é a questão da ilicitude da prova obtida via *print* do WhatsApp Web. Essa é uma questão também que é extremamente interessante porque permite uma intervenção direta da autoridade na prova. Tanto que eventual exclusão de mensagem enviada ou recebida não deixa vestígio. Então não se tem uma garantia de cadeia de custódia precisa. Isso foi julgado pelo STJ, no Recurso em Habeas Corpus 1.33.430/PE. O relator, também o ministro Nefi Cordeiro, mostrou a importância de ter uma precaução com relação à utilização desse tipo de quebra por parte do Estado. Mas vejam que o Judiciário vem em um caso. Quantos casos talvez possam ter ocorrido e que isso nunca tenha chegado a julgamento? Ou eventualmente, também, que outras formas de se exercer a vigilância mais expansiva não existem? Dado o fato de que - voltando ao meu ponto inicial - há um vácuo legislativo que precisa ser ocupado. Por isso, então, vemos a importância do anteprojeto da LGPD Penal.

O então ministro do Superior Tribunal de Justiça, que precocemente se aposentou, mas que fez um trabalho magnífico pelo STJ, fez um trabalho magnífico também como presidente de uma comissão de juristas criada pela Câmara dos Deputados de anteprojeto de uma LGPD Penal. Esse anteprojeto foi entregue ao então presidente da Câmara no final do ano passado e foi regulamentado a partir de uma comissão de juristas que desejava regulamentar o disposto no artigo 4º da LGPD. Isso é muito importante, porque nós temos uma regulamentação jurídica muito bem feita, desde a Lei da Interceptação Telefônica, mas que não resolve os problemas que temos atualmente. E lembrem bem que na jurisprudência pré-1996, a interceptação telefônica, à míngua de uma legislação, era ilícita. Mas ela existia, então ela provocou a existência da lei.

Fato é que o arcabouço normativo que nós temos hoje, feito por quem tem competência para isso, que é o Congresso Nacional, não resolve todos os problemas atinentes ao compartilhamento, ao uso, ao armazenamento, ao descarte [de dados pessoais], enfim, a todas as questões que eu coloquei, que existem e que cada vez se proliferam mais, porque a expectativa é que esse capitalismo de vigilância somente aumente. Ou seja, as quebras por arrastamento [devem crescer], enquanto o espectro da intimidade e da privacidade que os indivíduos poderão resguardar do Estado vai ser, naturalmente, cada

vez menor. Portanto, é importante que se tenha, por exemplo, para lidar com todo o arrastamento no reconhecimento facial, os dados massivos de localização. Ou seja, hoje nós temos um Estado capaz de saber, sem ordem judicial, onde eu estou a cada momento, via monitoramento por câmeras, enfim, uma série de coisas que deixa a nossa vida completamente exposta ao Estado. A perspectiva da segurança pública obviamente não deixa de ser um valor importante, mas isso pode levar a abusos, pode levar a exageros.

Então, essencialmente, olhamos para o anteprojeto, um trabalho muito bem feito, por juristas muito qualificados, e segue em debate no Congresso. A ideia básica do anteprojeto foi harmonizar a segurança jurídica para os órgãos de persecução penal com os direitos fundamentais dos cidadãos expostos a essas medidas. E hoje, o fato é que todos são, porque nós já vemos ocorrer quebras de sigilo por arrastão, a quebra de intimidade por arrastão, muitas vezes, tendo em vista o arcabouço normativo que nós temos hoje, [conforme mencionado] a Lei nº 12.850 de 2013, feito à míngua de ordem judicial.

De maneira geral, o que nós temos no anteprojeto é um detalhamento melhor dos princípios constitucionais da autodeterminação informativa, da reserva legal, porque isso já vem do texto constitucional. Mas também desde a interpretação que se fez da Lei nº 9.296/96, e também da presunção de inocência, que deve existir e que se irradia sob a perspectiva de como o Estado deve atuar no que toca aos dados dos cidadãos, ainda que seja na perspectiva de controle da segurança pública. Então a lei trata especificamente, também, do compartilhamento de dados entre [entes] privados e públicos em matéria de segurança pública, e faz isso de forma bem detalhada e bem cuidadosa. Estabelece uma autoridade controladora, o que também é algo que é muito importante.

Enfim, eu tinha feito algumas anotações aqui sobre a lei, mas eu tenho um pouco de preocupação com o meu tempo também não quero não quero me alongar demais, até para que haja tempo para perguntas. Mas, então, o anteprojeto vem na perspectiva de suprir um vácuo legislativo muito importante. Um outro ponto muito importante é a possibilidade de haver auditorias, ainda que não haja, no contexto, decisões tomadas de forma automatizada, que haja auditorias sobre o processo decisório. O direito à revisão por pessoa natural. A possibilidade de que isso ocorra sem discriminação, acho que isso é muito importante. Colocar o papel do CNJ como órgão supervisor, que também é significativo. E colocar requisitos mínimos para cada tipo de tecnologia de monitoramento. Então, eu acho que é uma preocupação que sempre tem que se colocar.

Acho que um ponto - que eu acho que meus colegas também já colocaram um pouco - é a preocupação também de lidar com aquilo que é relevante para a investigação, mas que ainda que seja relevante para a investigação, é altamente relevante tambémpara os indivíduos. Tanto que a gente fala que quando há algum tipo de vazamento, aquilo que constrange, muitas vezes, não é o ilícito, é o lícito, mas que é levado na perspectiva de constrangimento e de execração. Então, trabalha-se muito com uma lógica de adequação, necessidade e também de finalidade.

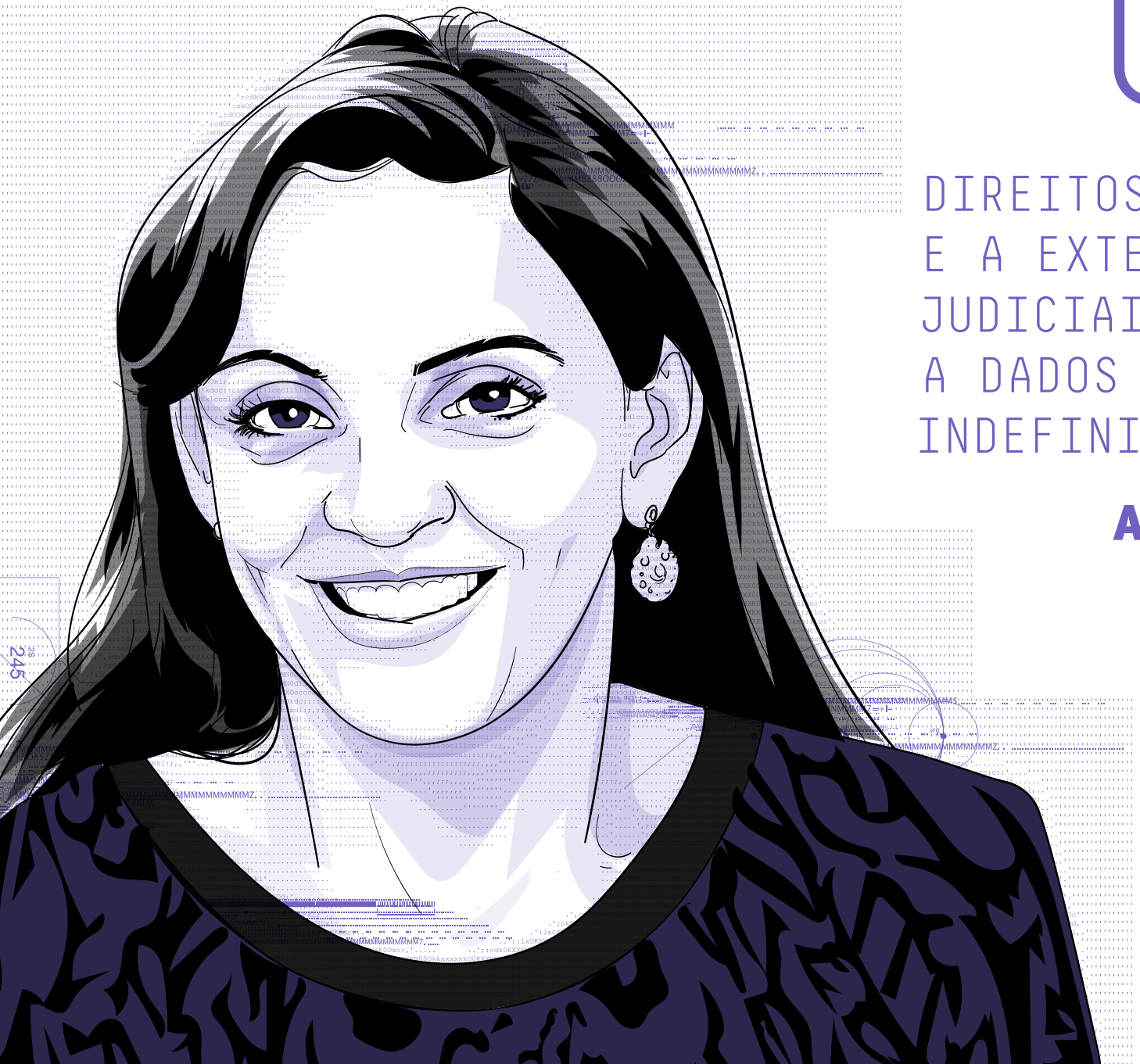
Eu diria que o reflexo desse anteprojeto é, essencialmente, assegurar o princípio da presunção de inocência, *in dubio pro reo*, da não incriminação, que são tão ameaçados quando nós olhamos - voltando ao que eu falei inicialmente desse capitalismo de vigilância - o perigo que é uma lacuna legal e o perigo que é deixar isso ao cuidado exclusivo dos magistrados, que muitas vezes ainda que imbuídos das melhores intenções, muitas vezes, não vão ter o arcabouço normativo para navegar com segurança, e, muitas vezes, também, tem que se levar em

consideração que os maiores atingidos por essas quebras são justamente aqueles que talvez tenham o menor poder de ir ao Judiciário e se defender e se estabelecer. Então acho que isso é muito importante.

Outra questão do anteprojeto é a consagração da proporcionalidade, dentro da perspectiva de uma máxima para interpretação das colisões entre direitos fundamentais, e que muitas vezes é utilizada de forma muito simplista por parte dos tribunais. Então, a ideia essencial do anteprojeto é, ao mesmo tempo em que não quer inviabilizar o tratamento dos dados nas atividades policiais, é criar uma tal forma regrada de controle que permita a relação de confiança, porque isso não vai ser acessado indevidamente, vai-se ter uma justa proporcionalidade entre o que se atinge o que se busca e vai ter um trato adequado disso na sequência. Um dos membros da comissão, o desembargador federal e professor Ney Bello, diz que é necessário que se tenha algum tipo de baliza para se achar a melhor forma proporcional de intromissão do Estado na esfera dos indivíduos, na esfera de privacidade e intimidade dos indivíduos. E esse cuidado, esse detalhamento, eu acredito que foi muito bem feito no anteprojeto que hoje está em discussão no Congresso.

Então, a ideia é que o instrumento de investigação utilizado e, naturalmente, o nível de intromissão do Estado em certas garantias como intimidade e privacidade devem ter direta proporcionalidade com a gravidade do crime que se busca e, obviamente, com respeito aos regramentos, que caso aprovados vão cumprir um vácuo legislativo existente. E mais do que isso também, outra coisa que acho muito importante na LGPD [Penal] é um respeito à busca pela utilidade da investigação. Ou seja, se tem uma cadeia de custódia definida, se ter um marco temporal delimitado, uma forma regrada de guarda de dados, um possível resgate de toda essa discussão no âmbito do Processo Penal para que se possa ter, a partir dos indivíduos, algum tipo de rastreabilidade, algum tipo de possibilidade de que se tenha essas discussões depois.

Enfim, acho que eu passei um pouquinho aqui do tempo que tinha sido reservado para mim, peço desculpas. O tema é tão fascinante que a gente acaba naturalmente querendo falar. Mas tentei fazer aqui um apanhado do que eu julguei que era pertinente a partir de um tema tão instigante. Agradecendo mais uma vez, Clarice, pelo convite e cumprimentando, mais uma vez também, minhas colegas de painel, Dra. Bárbara e Dra. Carolina.



09.

DIREITOS FUNDAMENTAIS E A EXTENSÃO DE ORDENS JUDICIAIS DE ACESSO A DADOS DE PESSOAS INDEFINIDAS

Anamara Osório

Obrigada, Francisco. Quero agradecer o convite do InternetLab, na tua pessoa, também na pessoa da Bárbara, da Clarice. E parabenizá-los por esse Congresso, por mais uma edição e pelo trabalho que vocês vêm desenvolvendo há longa data nas questões digitais. Acompanho os relatórios de vocês e vocês estão sempre à frente, como todo estudioso do direito digital tem que estar à frente, às vezes, do que está acontecendo agora, neste exato momento. E, assim, eu trabalho hoje na Secretaria de Cooperação Internacional da Procuradoria Geral da República e eu acabo pegando, acompanho o trabalho dos colegas que são especializados em crimes cibernéticos e a gente acaba acompanhando os grandes casos e também as medidas que são necessárias, inclusive na discussão de cooperação, da necessidade ou não de cooperação internacional a respeito de dados.

Bom, também gostaria de parabenizar a professora Marta Saad, que está sempre junto de vocês no Congresso. Sou muito fã dela. Parabenizar minhas colegas de evento, Dra. Carina Quito e a Dra. Lúcia Helena, também, obrigado por estarem aqui.

E, assim, sou entusiasta da tecnologia. Adoro, tento acompanhar tudo, são tantas coisas que se entrelaçam, tantos direitos fundamentais envolvidos, que às vezes é bem complexo. Mas eu sou entusiasta da tecnologia para o uso em geral. Como estudante - nós somos eternos estudantes do Direito, todos nós, - também sou preocupada e atenta aos direitos fundamentais.

Então, o caso que a Dra. Carina trouxe, que é o caso mais emblemático, da vereadora Marielle Franco. Ele traz essa discussão mesmo a respeito do *"geofencing"*, da geolocalização, do *"fishing expedition"*, que são todos termos usados lá fora, mas que a gente acaba incorporando. É uma investigação, uma pesca, que você tenta ir em busca de algo. Você não tem nada e você vai em busca de algo em um grande emaranhado de dados. Queria salientar porque, às vezes, a gente que trabalha no processo penal fica focado, muito focado, nas questões que envolvem o processo penal. Mas dizer que a par do próprio *"geofencing"* ter nascido como uma estratégia de marketing, da qual todos nós nos valemos. Eu pelo menos gosto quando entro em alguma zona geográfica, uma área geográfica, de ser notificada: "olha o seu restaurante X tem aqui perto, tem um posto de gasolina aqui perto de onde você entrou".

A gente sabe que essa foi a forma como se começou o *"geofencing"*, a notificação de marketing, mas ele é usado hoje para coisas muito importantes, de prevenção também, não só de repressão de delitos. Ele é usado pela nossa floresta. Existem técnicas de georreferenciamento para comunidades tradicionais, comunidades indígenas e monitoramento das florestas, tanto para prevenção de delitos quanto também para controle administrativo.

A tecnologia também é usada para, por exemplo, no direito internacional - que eu gosto bastante - você geolocalizar armas. Para você geolocalizar armas em determinados locais. Também para controle de drogas.

Existe uma série para a saúde pública também.

Então existe aí uma série de benefícios que a tecnologia traz. Brumadinho, desastres, catástrofes ambientais podem ser evitadas também por aí. Não é à toa que a ONU, atenta a isso, ela traz em seus objetivos de desenvolvimento sustentável, na meta 9 alínea c, essa questão do aumento do acesso a tecnologias de informação e de comunicação. Não só por uma questão inclusiva, para gerar um acesso universal à internet, mas também por todos os benefícios que pode trazer.

A pandemia nos mostrou que essa desigualdade social que nós temos é abissal com relação ao acesso à internet.

Então tudo isso para dizer que eu sou entusiasta das tecnologias. Mas, claro, evidentemente, com um olhar atento aos direitos fundamentais.

Aí a gente, de repente, começa se perguntando se essa técnica pode ser usada para prevenção e repressão criminal. Pergunta que talvez se faça. Como eu falei, para a prevenção já vem sendo utilizada, para auxílio de proteção ambiental. A repressão em todos os casos mencionados pela doutora Carina, no caso Marielle e muitos outros: tem casos patrimoniais de roubos de joalherias que também foram julgados pelo STJ . Também tem o homicídio de uma menina de 9 anos. Sequestro e homicídio. Pelo menos no mínimo uns seis, sete casos já julgados pelo STJ já utilizaram a técnica. Então, já está sendo utilizada a técnica para o processo criminal.

Mas aí a gente também se pergunta: "que tipo de dado é esse?" para que se possa tentar começar a destrinchar os conceitos. "Que tipo de dado é esse?". Porque a natureza do dado, ela pode, em um primeiro momento, no meu modo de ver, pode se chegar e dizer: "olha, é como se fosse uma vigilância massiva, então não importa qual seja o dado, porque o que importa é o direito de todas as pessoas todas aqui indeterminadas". Mas talvez a gente falar da natureza do dado importa sim naquele aspecto final da proporcionalidade em sentido estrito que é feito sempre o exame. Então, assim, "que tipo de dado é esses nesses casos que se buscou?".

A nossa legislação fala em dados de conexão e de acesso, que é o artigo 22 mencionado pela doutora Carina. Mas aí trazendo um pouco do direito internacional: o que diz a Convenção de Budapeste?". Ela especifica o que é dado de tráfico. Os dados de tráfico são dados onde você quer realmente a localização, na data, na hora, para você partir de um ponto, uma origem e um destino para você conseguir saber. Então é muito clara a finalidade - é bom falar de finalidade porque a LGPD fala em finalidade, a LGPD de projeto penal também fala em finalidade, então a gente tem que ter em mente. Qualquer que seja o tratamento desse dado, principalmente no processo penal, a gente tem que estar com uma finalidade na mente. Então, a finalidade, de acordo com a Convenção de Budapeste, é a identificação de um suspeito. É exatamente isso, a identificação do suspeito. E por quê? Porque a gente vê que a grande dificuldade de quem lida com os crimes cibernéticos é exatamente essa dificuldade de se identificar a autoria do crime. Você tem nos crimes, sejam eles próprios ou impróprios, cibernéticos, sempre alguém por detrás de um computador, por detrás de um celular, cometendo um crime e você não sabe quem é esse alguém. Então, para você partir de qualquer tipo de diligência - e essas são as agruras de quem trabalha com esse tipo de crime - você precisa saber minimamente quem é a autoria, para você poder fazer qualquer outro tipo de diligência. Às vezes o que você tem é uma mensagem. Você não tem nada mais do que uma mensagem. Você vai atrás daquele IP, daquela mensagem ou daquele perfil no Instagram, por exemplo, e tenta saber quem está ali atrás. Às vezes você não consegue a autoria direta ainda de quem está atrás porque você vai precisar de saber quem é o administrador ou quem registrou aquele aquele IP e aí você vai procurar pelo menos três steps até conseguir ver quem talvez esteja por detrás daquilo.

Essa é uma questão que a gente tem que saber lidar nos dias de hoje. O celular é extensão do corpo hoje né. Tanto que foi assim que o Supremo decidiu com relação ao acesso da polícia e o acesso sem autorização judicial no celular, que o celular contém muito mais do que imagina, ele é a extensão do corpo. E se a gente for pensar o que significa essa identificação de pessoas é quase que como você, trazendo para um mundo real sem tecnologia, é quase como você (...).

Por exemplo, existe um crime cometido dentro de um evento e não se sabe quem foi que cometeu esse crime. Da onde a polícia e o Ministério Público vão partir? Entrada. Quem teve acesso ao evento? Se o evento de qualquer forma possui uma

identificação de entrada já é um começo. Está aí a identificação, né. O que talvez com a tecnologia se quer alcançar. Talvez não, é o que se quer alcançar: a identificação.

Há um tempo atrás se discutiu muito também essa questão de você se identificar nas portarias de um prédio. Isso ofende o meu direito de privacidade ou não? Não quero me identificar, quero entrar no prédio, mas hoje é uma prática disseminada. Não tem prédio, pelo menos em São Paulo, que você entre e não tenha que se identificar na portaria, por questões de segurança também né.

Então, por isso aí essa tensão entre os direitos fundamentais. Quando a gente está falando disso, você não está falando, todo mundo sabe disso, só em privacidade. A gente está falando de segurança, está falando de igualdade, porque a igualdade significa também que você não pode deixar pessoas impunes. Por quê? Porque tem toda - e tomara que seja assim - uma massa de pessoas que não cometem crimes e que sabe que, se cometerem crimes, vão ter uma resposta penal. Então, a igualdade também. O acesso à Justiça. O direito à verdade. Então são vários direitos aí que estão em tensão.

Bom, então, classificando como dados de tráfico, vem o segundo ponto: a intensidade desse direito. Isso vai ser importante para se analisar a proporcionalidade em sentido estrito. E aí a Convenção de Budapeste também diz: "a recolha destes dados é encarada como implicando, em princípio, uma menor intrusão, uma vez que se desconhece o conteúdo da comunicação, o que é visto como sendo o mais delicado". Então não adianta, existe uma separação: dado de tráfico, o que o Marco Civil fala em conexão e acesso, é diferente de dados de conteúdo, muito mais invasivo. E a nossa Constituição mostra isso. O artigo quinto, inciso doze, é para dados de comunicação, onde tem reserva de jurisdição. Dados em geral, outros dados, caem no inciso dez, onde sequer se fala em reserva de jurisdição. Mas

/ A PANDEMIA NOS MOSTROU QUE ESSA DESIGUALDADE SOCIAL QUE NÓS TEMOS É ABISSAL COM RELAÇÃO AO ACESSO À INTERNET /

/ EXISTEM PAÍSES QUE PARA DADOS DE TRÁFEGO, NÃO EXISTE MENOR NECESSIDADE DE AUTORIZAÇÃO JUDICIAL /

o que se convencionou? Então onde a gente poderia colocar no pacote de dados ou de sigilos - algo que interfere na privacidade - onde a gente colocaria os dados de tráfico também? Talvez junto com o sigilo bancário fiscal, que é onde fica no artigo quinto, inciso décimo da Constituição, que é a questão da vida privada e a intimidade. Então é diferente de uma medida relativa ao domicílio, diferente de uma medida relativa à comunicação.

Mas volto dizer: essa análise talvez seja importante, e me parece que foi isso que o STJ fez, para analisar a proporcionalidade em sentido estrito da medida, que quando se vê se o meio utilizado, o alcance dos dados de tráfico, é proporcional e sem sentido estrito a finalidade que se quer alcançar. O STJ entendeu se tratar de um crime gravíssimo contra uma vereadora ativista de direitos humanos que lutava contra as milícias e que assim foi reconhecida inclusive pelo alto comissário. Um crime que deveria ser desvendado.

Mas, dentro da proporcionalidade, tanto o Supremo Tribunal Federal como a Corte Interamericana de Direitos Humanos, já disseram que existe uma outra faceta do princípio da proporcionalidade: que é não apenas evitar intervenções estatais excessivas, que é a proibição do excesso. Qual a outra faceta? É a proibição da proteção deficiente ou insuficiente. Então se entendeu que uma obrigação positiva tem ou um dever de proteção do Estado se deve dar não só a vítima como todas as pessoas com relação à integridade - que no caso era a vida - mas também a obrigação de desvendar crimes e de fato punir crimes graves, como é o caso. Isso está no caso Ximenes Lopes, no caso Herzog, no caso de Fazenda Nova Brasília. Isso é um dogma da Corte Interamericana de Direitos Humanos.

Bom, então, já está sendo usado no processo penal. Na verdade, é uma prática que se usa porque os dados já foram coletados, os dados já foram coletados pelas companhias. Então, talvez, a gente tenha que fazer uma discussão: “deveriam

ser coletados?". O que STJ disse? Disse que - porque a alegação era exatamente isso, dados indiscriminados, genéricos e inespecíficos. Lembrando que o anteprojeto LGPD penal também fala isso. Ele diz expressamente no artigo, me parece. Ele diz expressamente, no artigo 11, parágrafo segundo, que "toda e qualquer requisição administrativa ou judicial indicará o fundamento legal de competência expressa para acesso e a motivação concreta, inclusive sua adequação, necessidade e proporcionalidade, sendo vedado os pedidos genéricos ou inespecíficos". Mas o STJ diz: "não é genérico nem inespecífico - ele está lá, num raio, num dia, em uma determinada hora", como a doutora Carina falou: "às vezes passa mais de um dia, ou quatro dias", como, salvo engano, foi o caso da Marielle. Mas ele não chega a ser, vamos dizer assim, uma pesca predatória.

O grande desafio nosso do *"fishing expedition"* é buscar os precedentes do *"fishing expedition"* do STF. O que o STF, então, já, mais ou menos, decidiu? Mandados genéricos não podem, né. Por que? É domicílio, né. Então é um direito fundamental que requer reserva de jurisdição, etc. Na categoria dos direitos fundamentais, a invasão é bem mais ofensiva. Que foi o caso decidido que o mandado era para ter sido cumprido no lugar x, chegando no lugar X, não se localizou, mas se ficou sabendo, conversando lá, que a pessoa estaria no lugar Y. Ou as provas indicariam um lugar Y. E se fez a diligência sem ter uma autorização judicial específica. Então aí gerou muita discussão também sobre autorização judicial específica, que não está ocorrendo nesses casos. Existe uma autorização judicial. Lembrando até que, para dados de tráfico, o legislador brasileiro optou pela autorização judicial. Mas existem países que, para dados de tráfico, não existe menor necessidade de autorização judicial. O Marco Civil da Internet, artigo 23, fala em autorização judicial. E assim tem sido a prática do Ministério Público nesse sentido para acesso a dados de acesso e conexão. E o STJ entendeu que a motivação também estava justificada e, dentro dos critérios e subcritérios de adequação, necessidade e proporcionalidade em sentido estrito, entendeu que também estavam presentes ali. Esses subcritérios, da mesma forma, estão presentes no anteprojeto da LGPD penal.

E é aí que a gente também percebe que tudo gira muito em torno da proporcionalidade em sentido amplo, com esses subcritérios. Porque é o que tem sido mencionado também pelo Alto Comissariado da ONU, que tem sido mencionado também pela Corte Europeia de Direitos Humanos, tem a decisão do Big Brother Watch vs. UK, que é interessante, pois é um desdobramento do caso Snowden no Reino Unido. São pessoas ativistas que se sentiam que estavam sendo vigiadas, suas comunicações estavam sendo vigiadas, e isso foi levado para a Corte Europeia de Direitos Humanos. E o que decidiu a Corte? Pode se fazer toda uma explicação da legislação que se imperava ali. Vamos dizer assim que se tratava de um poder do secretário de Estado. Não era nem autoridade judicial que estava falando. Era uma medida administrativa, porque a vigilância preventiva a prática de delitos. E o que disse a Corte Europeia de Direitos Humanos? Que o método não está errado. Ao contrário, por conta da margem de apreciação os estados, que a Corte sempre confere, podem, de acordo com a sua margem de apreciação, dizer o que é necessário fazer vigilância ou não. Não está errado. Fala em proporcionalidade. Mas o que entendeu a corte que violava o artigo oitavo da convenção, que é o artigo que fala da intimidade da vida privada, foi porque não havia uma autorização de uma autoridade independente e imparcial. Mesmo que fosse *ex post facto*. Que é o que não está faltando na questão brasileira.

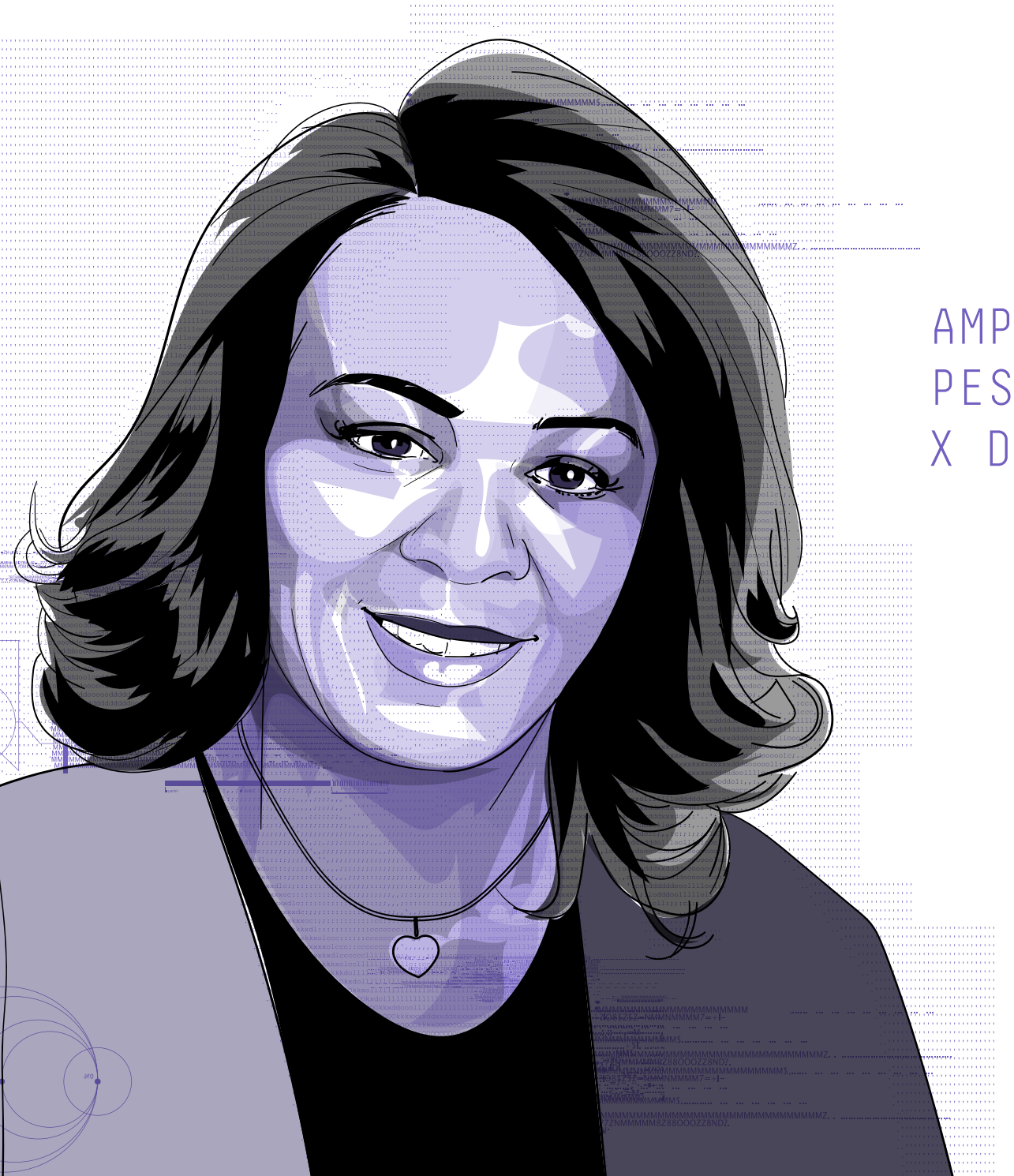
Voltando um pouco até para o *"fishing expedition"*: o que os nossos precedentes trazem? Trazem um alvo muito mais determinado, mas que a prática que se tenta coibir no *"fishing*

expedition" é o objeto né. Você até tem uma finalidade, mas o objeto que é muito amplo. Quando a gente fala aqui do "*geofacing*" a gente fala: "o objeto parece determinado mas essas pessoas são indeterminadas, é uma massa". Então, é o contrário. Mas eu acho que os precedentes valem para isso também. Por exemplo, quando são quebras bancárias de anos que você, por exemplo, recebe uma comunicação suspeita do COAF em que você faz uma devassa nos bancos para tentar identificar. Não, não dá.

Por fim, o que eu gostaria de salientar, ainda dentro dessa questão da vigilância massiva, e além do caso do *Big Brother Watch*, porque talvez aí se identifique com o nosso caso do "*geofacing*", que não é tanto o objeto, a finalidade estão definidas, mas são pessoas indeterminadas e a vigilância ainda, em termos de intrusão e invasão, ainda é pior, porque aqui nesses casos citados no STJ você está diante da prática de um delito. O que diz um relatório deste ano do Alto Comissariado da ONU? O relatório fala sobre manifestações e protestos e a vigilância de manifestantes. Ele traz os pontos positivos de se fazer um monitoramento, por exemplo.

E por isso eu falo que a gente tem que sair um pouco do quadrado do Processo Penal também. Os pontos positivos de fazer o monitoramento é permitir que as forças públicas saibam o volume de manifestantes que estarão lá, para garantir a segurança dos manifestantes. Então faz o cuidado com as redes sociais para poder ver o volume, para projetar um volume e para garantir a segurança. Outro ponto é que consiga conversar junto com os organizadores da manifestação. O Alto Comissariado também fala que esse monitoramento da vigilância também é benéfico para isso. Para você entrar em contato, através das redes sociais. Mas fala tudo o mais, que é péssimo. Inclusive cortar a palavra de manifestantes nas redes sociais. Mas, de novo, qual é o direito que eles salientam? Para a gente ver como existe sempre um feixe muito grande de direitos fundamentais: o direito à reunião pacífica. Uma reunião pacífica, reunião evidentemente que não tenha violência e nem ofensa ao patrimônio ou ofensas em geral. Então, concluindo a minha fala, o que diz o Alto Comissariado nessa questão? Que a gente pode dizer que é um pouco similar, afastando a questão da ordem judicial de tudo, mas um pouco similar com a indeterminação: "que a vigilância dos manifestantes só deveria levar-se a cabo de maneira seletiva e só quando há suspeita razoável de alguém que esteja cometendo ou planejando cometer crimes". Ou seja, você, dentro daquela quantidade de manifestantes, detecta onde poderia estar ocorrendo a prática criminosa, onde está sendo planejada a prática criminosa. De novo, sobre as bases dos princípios da necessidade e da proporcionalidade do controle judicial. Então, acho que são essas as premissas de repente que a gente deveria estabelecer. São dados de tráfico, há necessidade de ordem judicial e sempre tendo em mente a prática de um crime, de um crime grave, e a proporcionalidade, que é extraída da gravidade do delito.

Ficou à disposição para o debate.



10.

AMPLO ACESSO A DADOS PESSOAIS: PRIVACIDADE X DIREITO À INFORMAÇÃO[1]

Lúcia Helena Silva de Barros de Oliveira

1. Este texto tem por base a transcrição da palestra apresentada por Lúcia Helena Silva de Barros Oliveira no painel "Direitos fundamentais e a extensão de ordens judiciais de acesso a dados de pessoas indefinidas", no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab, em 2 de setembro de 2021. A transcrição foi revisada pela autora.

Boa noite a todas e todos. Gostaria de cumprimentá-los e agradecer pela oportunidade oferecida através do convite feito pela InternetLab. Sou grata, em especial, a Francisco, Bárbara e Clarice, pelo honroso convite. É uma excelente oportunidade para que a Defensoria Pública do Estado do Rio de Janeiro possa ocupar um assento tão *valioso*, com a participação num congresso de tamanha importância.

Indiscutivelmente, estamos caminhando para uma modernização do processo penal pátrio. Então, recebam meus parabéns por tal iniciativa, com o Congresso já em sua quinta edição. É realmente muito bom trazer e levar conhecimento a toda a sociedade no que diz respeito ao formato do processo penal e à relação correspondente com os direitos fundamentais — direitos que se revelam tão caros à nossa sociedade.

Gostaria de cumprimentar as colegas que estão aqui comigo neste painel: Dra. Carina Quito e Dra. Anamara Osório. É uma honra para mim estar ao seu lado. Eu não as conhecia pessoalmente e realmente é um prazer ouvi-las. Observo que suas explanações foram maravilhosas, o que resulta em grande responsabilidade ao falar depois de vocês. Acho que não sobrou nada. Mas vamos lá!

Inicialmente, registro a relevância das ponderações feitas pela Dra. Carina, ao resgatar um caso de tão grande importância e que traz, na verdade, o desenho deste painel: o caso Marielle Franco. Há, nele, uma intensa carga subjacente, que envolve o significado de nossos princípios fundamentais, de nossos princípios constitucionais.

A Dra. Anamara, por sua vez, ao trazer reflexão não só sobre o campo da repressão, mas também sobre o campo da prevenção, em relação ao que se deseja com a investigação de dados, também faz um alerta importante: que a sociedade deve observar os reflexos do aspecto da prevenção em tantas áreas, como, por exemplo, a da saúde pública e a do meio ambiente. Esses, sem dúvida, são temas muito caros à nossa sociedade.

Começo com uma reflexão descontraída — sem desmerecer a seriedade do tema — e indago: "Quem quer dados pessoais?". Esse momento de descontração é apenas uma ilustração, e me perdoe pela brincadeira, mas serve exatamente para que possamos refletir sobre a importância do assunto. O objetivo aqui é enxergar com outros olhos a relevância do que estamos falando, do que estamos abordando.

Nossos dados pessoais são algo muito caro, e essa avaliação prescinde de um olhar mais acurado para a Constituição Federal ou para as legislações que cercam o tema. Vamos nos concentrar no resgate da legislação atual, que é a Lei de Proteção de Dados (LGPD), a proteção dos direitos fundamentais de liberdade e a privacidade.

A privacidade, como bem ressaltaram as Dras. Carina e Anamara, apresenta um dilema: um dilema entre a tomada de conhecimento de uma infração penal e a apuração da respectiva autoria. E eu trago aqui os objetivos da LGPD em seu arcabouço: privacidade, inviolabilidade da intimidade, honra, imagem, entre outros, e o enfrentamento [dos limites a esses direitos], que pertence à esfera da proporcionalidade. Entendo que não cabe banalizar a privacidade.

Com frequência, declaramos: "Mas eu não tenho nada a esconder... Então, qual é o problema de investigarem meus dados? De divulgarem meus dados? Pois, de fato, nada tenho a esconder. O Estado pode, sim, ter conhecimento dos meus dados". No entanto, essa questão não é tão simples assim. O fato de não haver nada a esconder não significa que possamos abrir mão de nossa privacidade. Veja, talvez em relação aos e-mails seja mais fácil visualizarmos essa questão. Se ouvirmos de alguém: "Será que posso dar uma olhada no seu e-mail?", talvez

nossa resposta seja: “É claro que sim. Não há segredo algum aqui”. Mas quem se sentiria à vontade, por exemplo, com uma espiada em suas mensagens de WhatsApp e programas afins? Quem se sentiria à vontade com um exame de sua agenda? Então, não se trata de uma pergunta assim tão simples.

Nesse contexto, remeto a uma citação do Edward Snowden: “As Nações Unidas afirmam que privacidade é um direito humano, assim como educação. Por qual motivo você abriria mão disso? Argumentar que você não se importa com o direito à privacidade porque nada tem a esconder não é diferente de dizer que não se importa com o direito à liberdade de expressão porque nada tem a dizer”. É uma ideia que, de fato, merece maior reflexão, ainda que estejamos procedendo a um vasculhamento de dados para encontrar a autoria de um ilícito penal.

Por que digo isso? Digo porque não é apenas uma garantia [de privacidade] prevista no Pacto Internacional dos Direitos Civis, no Pacto de São José da Costa Rica e em nossa Constituição Federal. É mais do que isso. Nosso Código de Processo Penal, se o artigo 3º, B não estivesse suspenso, prevê que caberia ao juiz das garantias “a responsabilidade do controle da legalidade da investigação criminal e salvaguarda dos direitos, e assegurar prontamente, quando se fizer necessário, o direito outorgado ao investigado e ao defensor de seu acesso a todos os elementos informativos e produzidos no âmbito da investigação criminal, salvo no que concerne estritamente às diligências em andamento”. E quais seriam os limites das ordens judiciais para o acesso a dados em relação a pessoas indefinidas? A investigação em massa ofende a privacidade?

Buscando responder a esses questionamentos, eu trouxe aqui algumas opiniões que acabam envolvendo o caso Marielle. Mas, conforme alertou a Dra. Carina, o caso Marielle é bastante emblemático e, de fato, chama a nossa atenção. Mas

/ MAS QUEM SE SENTIRIA À VONTADE, POR EXEMPLO, COM UMA ESPIADA EM SUAS MENSAGENS DE WHATSAPP E PROGRAMAS AFINS? /

/ NO MÍNIMO, DEVERIA HAVER UM ESCLARECIMENTO À POPULAÇÃO SOBRE O QUE ACONTECE NO CAMPO DE SEUS DIREITOS FUNDAMENTAIS /

nós temos uma boa quantidade — mais do que se pensa e mais do que a população tem conhecimento — de decisões judiciais que envolvem acesso a dados. E isso em casos que, conforme já assinalado, abrangem não só infrações graves, mas também infrações menos gravosas.

Neste momento, portanto, é necessário examinar o conceito de *gravidade da infração*. Quando falamos em infração grave, tendemos a pensar logo em homicídio. Ok. Inegavelmente, homicídio é um delito grave. Mas qual seria o conceito exato? O roubo estaria incluído nesse rol? Temos uma decisão que acaba alcançando dados em delitos de roubo. Não se desconhece, obviamente, que estamos falando de um crime praticado com violência ou grave ameaça para obter um patrimônio. Mas será mesmo que, quando falamos de roubo, estamos no mesmo patamar do crime de homicídio?

Nesse cenário, temos um reclamo — melhor dizendo, um clamor — e um questionamento. E eu também questiono as indefinições de nossa legislação que acabam influenciando as decisões judiciais. Nosso arcabouço legal, ainda que acompanhado do Pacto de São José da Costa Rica — que protege a privacidade —, ainda que acompanhado da Convenção de Direitos Humanos, não conta com uma delimitação precisa, determinada, de como ocorreria esse alcance de dados. Parece-me que essa imprecisão caminha na contramão do que se pensa a respeito de legalidade. A mim, parece que temos dificuldade de alcançar também a proporcionalidade.

Cito aqui um caso concreto. Na opinião de Maristela Paz, é inconstitucional, ilegal e desproporcional

> a decisão do STJ para que o Google forneça dados dos seus usuários de forma indiscriminada, sem individualizar os endereços de IP. A decisão não pode ser cumprida pelo Google pela simples razão de que, assim agindo,

> vai violar o direito de privacidade dos usuários e poderá sofrer ações de responsabilidade civil em massa daqueles que se sentirem lesados.

E:

> [...] sem a menor sombra de dúvida, a decisão do STJ gera um estado panóptico que não é desejável em uma espécie de democracia. Pessoas que não são investigadas ou acusadas da prática de algum ato ilícito devem ter a sua privacidade e a sua liberdade preservadas acima de quaisquer outros. No momento em que, para fins sociais, começarmos a abdicar de tais conceitos e interferir na vida de todo e qualquer cidadão, estaremos abdicando do conceito de democracia e do Estado Democrático de Direito.

Qual é o problema? O problema é o alcance, de forma indiscriminada e imprecisa, desses dados. Mas é claro que eu não poderia fazer minha exposição sem trazer a outra face da moeda, porque meu intuito aqui não é fazer defesa de um lado ou de outro, mas tão somente comunicar uma vivência acadêmica e profissional. E levar em consideração que, se, de um lado, as decisões judiciais não são novas, o tema é relativamente recente em nosso cenário jurídico. Não se imaginava, na época do Código de Processo Penal de 1940, que hoje estivéssemos discutindo um assunto dessa natureza.

A outra face da moeda encontra fundamento no artigo 22 do Marco Civil da Internet. Esse artigo 22 é citado pelo STJ. Mas não se limita a isso. Tomei conhecimento de uma decisão num caso de homicídio que teria ocorrido no estado de Pernambuco. Nela, o Juízo da Vara Única da Comarca de Jupi/PE determinou que se alcançassem os dados de algumas pessoas que estivessem próximas ao local do homicídio. Em artigo escrito a esse respeito, da lavra do Desembargador Demócrito Reinaldo Filho, do TJPE, está registrada a posição do Google, mas também os argumentos apontados pelo Judiciário — e um desses argumentos é o artigo 22. No entanto, ele questiona a legitimidade do Google — no sentido de, ao negar acesso a esses dados, estar defendendo direito de privacidade alheio. Acrescenta o autor do artigo um caso ocorrido em Nova York, que teria reconhecido a falta de legitimidade para perseguir a privacidade, para proteger a privacidade de terceiras pessoas que nem sequer estariam reclamando da eventual violação de seus dados. E ele justifica sua decisão de forma política, alertando sobre um monopólio de dados, no sentido de que aquele que tem o monopólio de dados teria também o poder. Se é só você quem tem acesso, se é só você quem tem os dados, isso significa que você detém maior poder. E questiona: "Seria possível dar ciência aos seus usuários dessa ordem judicial?". Ele responde negativamente.

Em minha opinião, contudo, o terceiro deve conhecer aquilo que está sendo tratado sobre seus dados. O terceiro deve ter conhecimento disso — e a informação, a publicização, tudo isso é muito importante. Concordo que sabemos que há sigilo em relação a determinadas provas, mas questiono a afirmação de que não cabe ao terceiro o direito de conhecer, ou seja, de ter ciência de que esses dados estariam sendo fornecidos. E acrescento que ele deve ter ciência prévia disso.

Aqui outros aspectos merecem reflexão: privacidade, responsabilidade civil em massa daqueles que se sentirem lesados, ausência de amparo legal. De fato, o direito à privacidade não é absoluto. Mas não podemos deixar de questionar, além da privacidade, todos os outros elementos que envolvem o tema: legalidade, proporcionalidade e falta de definição do que seria uma infração penal grave. Além disso, como alcan-

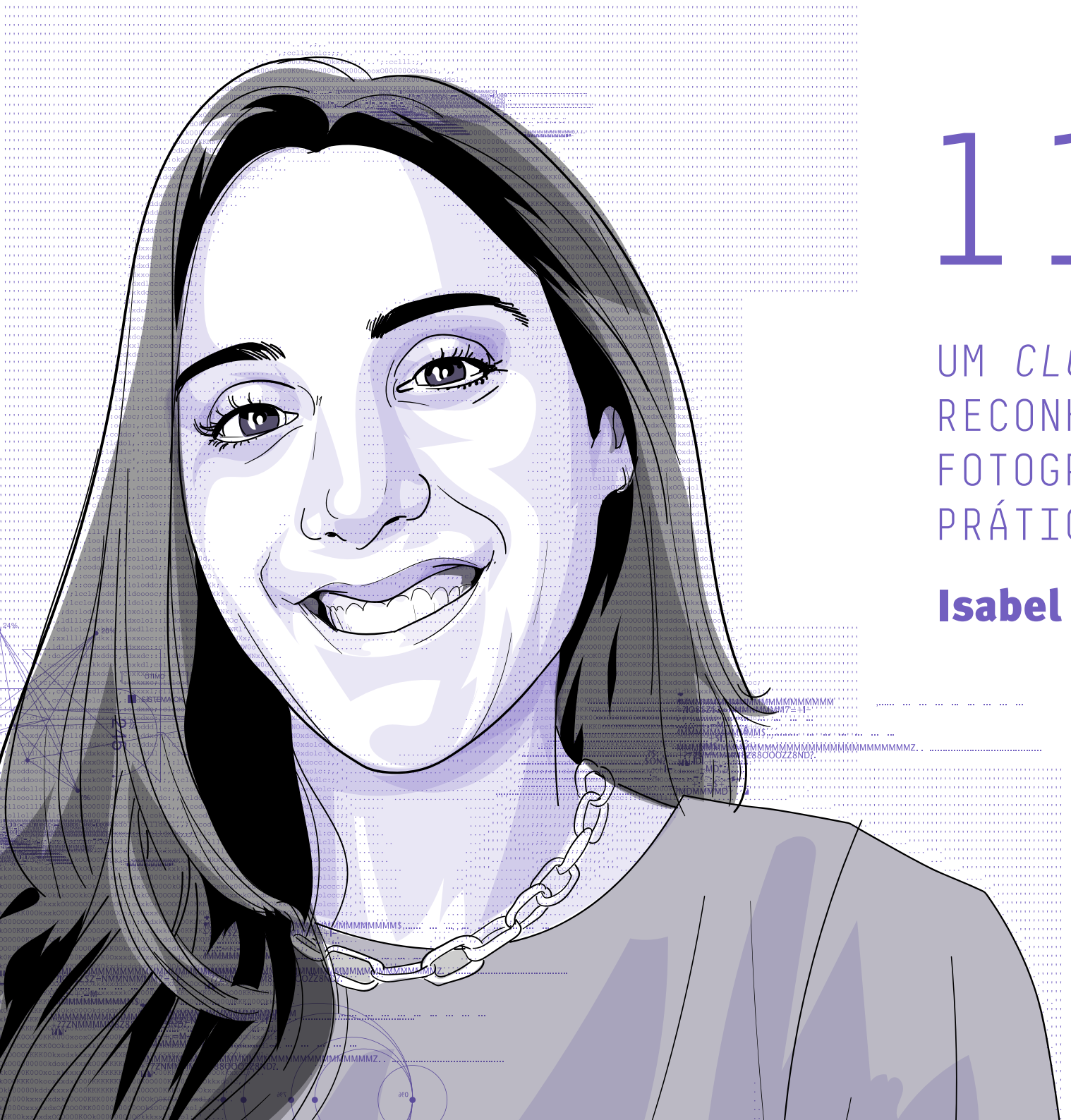
çar todos? Como delimitar os critérios? Insisto que diversas pessoas não têm conhecimento da possibilidade desse alcance, de que decisões judiciais podem acessar seus dados. Então, a mim, parece que, no mínimo, deveria haver um esclarecimento à população sobre o que acontece no campo de seus direitos fundamentais.

Nesse contexto, exponho — inclusive sob a ótica defensiva — uma preocupação que tenho como Defensora Pública: "Como compatibilizar o princípio da ampla defesa com a quebra do sigilo em massa e a proteção de dados de terceiros? Em que momento caberá à defesa se manifestar?". Isso porque, seguindo a lógica de que só constarão do processo os dados da pessoa cuja autoria foi constatada, a defesa não tomaria conhecimento dos dados das demais pessoas. E como, de fato, se apurou aquela autoria? Se ela não tem esse conhecimento, parece que nos encontramos imersos em um dilema: de um lado, o direito à ampla defesa e, de outro, a necessidade de proteger os dados de terceiros. Como compatibilizar essa situação? De minha parte, ainda não encontrei a resposta. Minha veia defensiva, porém, tende para o lado da ampla defesa, mas confesso que não tenho a resposta precisa, determinada. Em verdade, vemo-nos diante da privacidade desses terceiros, mas também da promoção dos direitos humanos — e, inequivocamente, cabe à Defensoria Pública a promoção dos direitos humanos, matéria regida em nossa lei complementar. Cabe-nos buscar algum equilíbrio e firmeza em relação a esse tema.

O momento em que a defesa se manifestará é outra questão para a qual ainda não temos solução. Será que a defesa pode manifestar-se a qualquer tempo no processo na condição de defensora do acusado se essa acusação tiver chegado por meio do acesso aos seus dados? Mas, se a defesa pode manifestar-se a qualquer tempo, em que momento do processo teria acesso a esses dados? É preocupante. Ela poderia ter acesso aos dados e também ao formato da investigação. Essas questões nos preocupam sob o prisma da violação dos dados de terceiros.

Aqui, finalizo com uma frase que serve de reflexão para todos nós. A frase não é minha, mas acho que define bem a importância da privacidade em nossas vidas:

"A privacidade importa, independentemente de quem você é. Precisamos seriamente começar a nos proteger."



11.

UM *CLOSE* NO RECONHECIMENTO FOTOGRÁFICO: DADOS, PRÁTICAS E TESES[1]

Isabel Schprejer

1. Texto que tem por base a transcrição da palestra apresentada por Isabel Schprejer no Painel "Teses: Reconhecimento Fotográfico" no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em 03/09/2021. A transcrição foi revisada pela autora.

Gostaria de parabenizar a InternetLab e todas as pessoas envolvidas na realização deste congresso tão inovador e essencial. Agradeço pelo convite, especialmente ao Pablo Nunes, que me convidou diretamente. Nós tivemos a oportunidade de debater sobre a questão do reconhecimento facial em um evento da Defensoria Pública. É um grande prazer revê-lo! Cumprimento também os demais presentes e o Felipe Freitas, que também compõe o painel. É um prazer conhecê-lo, ainda que virtualmente.

É muito relevante que um painel com essa temática do reconhecimento pessoal e fotográfico tenha sido incluído em um congresso como esse, cujo tema central é o Processo Penal na Era Digital. Isso porque não é possível compreender inteiramente a dimensão do problema do reconhecimento facial, que já é uma realidade muito preocupante no país, sem antes dar um passo atrás e olhar de forma crítica para o reconhecimento pessoal e, principalmente, o fotográfico. Que é algo bastante analógico - por assim dizer -, mas que é enfrentado todos os dias por nós que atuamos na defesa criminal. E algumas das questões relacionadas ao reconhecimento fotográfico vão se estender também ao reconhecimento facial.

O reconhecimento fotográfico tem um enorme potencial de gerar erros judiciais. Isso se dá, principalmente, devido à forma como esse procedimento vem sendo feito na prática, gerando uma possibilidade muito grande de induzimento da pessoa do reconhecedor e de criação de falsas memórias, acarretando em violações de direitos e injustiças. E as injustiças geradas por reconhecimentos fotográficos equivocados, como, aliás, ocorre com as injustiças em geral no Brasil, recaem, principalmente, sobre a população negra, pobre e periférica.

Para retratar melhor esse quadro, eu gostaria de compartilhar alguns dados, que são resultado de duas pesquisas realizadas pela Defensoria Pública do Estado do Rio de Janeiro, através da sua Diretoria de Estudos e Pesquisas de Acesso à Justiça. Os estudos reuniram dados colhidos entre os anos de 2019 e 2020, referentes a processos criminais em que o reconhecimento em sede policial foi realizado através de fotografia e, posteriormente, não foi confirmado em juízo pela vítima do crime, gerando, então, uma sentença absolutória. Ou seja, os estudos reuniram casos de reconhecimento fotográfico realizados em delegacia de polícia que, posteriormente, vieram a se revelar equivocados. A primeira pesquisa[2] coletou e analisou dados somente do estado do Rio de Janeiro, enquanto a segunda,[3] realizada em parceria com o Conselho Nacional das Defensoras e Defensores Públicos-Gerais (CONDEGE), coletou e analisou também dados de outros estados brasileiros. Os dados que serão apresentados a seguir são uma junção dos resultados obtidos em ambas as pesquisas.[4]

Foram reunidos, no total, dados referentes a 75 processos e 90 acusações, em que ocorreram erro no reconhecimento fotográfico, sendo que, dos casos em que havia informação sobre a cor do acusado, em cerca de 81% dos casos, essa cor era negra, incluindo pessoas pretas e pardas, de acordo com a classificação do IBGE, conforme a tabela a seguir:

COR/RAÇA	QUANTIDADE DE RÉUS
BRANCA	14
PARDA	30
PRETA	31
NÃO CONSTA	10
TOTAL	85

2. Disponível em <https://www.defensoria.rj.def.br/uploads/arquivos/33e974efa1004184954cc1b08ac2f253.pdf> . Acesso em 10/04/2022.

3. Disponível em <https://www.defensoria.rj.def.br/uploads/arquivos/54f8edabb6d0456698a068a65053420c.pdf>. Acesso em 10/04/2022.

4. Disponível em <https://www.defensoria.rj.def.br/uploads/arquivos/92d976d0d7b44b338a660ec06af008fa.pdf>. Acesso em 10/04/2022.

Verificou-se, ainda, que, em aproximadamente 77% das acusações analisadas (69 de 90), houve prisão preventiva decretada, sendo que o acusado que ficou mais tempo preso preventivamente, com base unicamente no reconhecimento fotográfico, para, ao final, ser absolvido, permaneceu preso injustamente por, aproximadamente, 3 anos e 21 dias. Veja-se:

MENOR PERÍODO	MAIOR PERÍODO	MÉDIA	MEDIANA
5 DIAS	1.116 DIAS APROX. 3 ANOS/21 DIAS	268 DIAS APROX. 9 MESES	237 DIAS APROX. 8 MESES

Os resultados desses estudos mostram, de maneira flagrante, o viés racial presente nos erros de reconhecimento realizados na modalidade fotográfica.

Nesse sentido, é muito importante que a questão racial seja levantada, e, inclusive, destacada em petições elaboradas no bojo dos processos criminais. É necessário que o debate em torno do reconhecimento fotográfico seja racializado, a questão racial precisa ser colocada para os julgadores – essa é uma das teses possíveis. E é interessante que as pesquisas sobre o tema, que trazem estatísticas e dados concretos, também sejam incluídas nas peças processuais, porque ajudam a entender o tamanho dessa injustiça - vide o caso comentado, de mais de três anos de prisão preventiva, seguida de absolvição.

No Estado do Rio de Janeiro, a modalidade fotográfica do reconhecimento de pessoas é largamente utilizada pelas delegacias de polícia e, muitas vezes, é o único elemento que gera a deflagração de uma ação penal pelo Ministério Público, bem como a decretação da prisão preventiva pelo juízo. Não raro, nos deparamos também com condenações baseadas unicamente no reconhecimento por foto.

Uma prática muito comum é que o reconhecimento por foto em delegacia se dê através de um álbum de suspeitos, que é folheado pela vítima ou por uma testemunha do crime, que podem apontar a foto da pessoa que entendem ser o autor do crime. Porém, não existe qualquer regulamentação desse álbum de suspeitos, ao menos no Estado do Rio de Janeiro. Não existe um álbum unificado da Polícia Civil. Cada delegacia tem o seu próprio álbum, e não há transparência - não há quaisquer informações sobre como e por que as fotografias de algumas pessoas vão parar no álbum de uma delegacia e outras não, havendo, inclusive, uma questão de uso abusivo da imagem. Então, não é possível fiscalizar essa prática, não existe *accountability*[5] em relação ao álbum de suspeitos, dada a falta de regulamentação e a total obscuridade em torno da sua formação. Além disso, folheando o álbum de suspeitos, fica bastante claro o viés racial que foi comentado anteriormente. Então, é de suma importância a extinção ou, ao menos, a devida regulamentação do álbum de suspeitos e transparência com relação à sua formação e utilização.

5. Termo inglês, em tradução livre, correspondente a "responsabilidade".

Uma ação individual que é possível, desde já, é a provocação judicial visando à exclusão da foto de uma pessoa do álbum dos suspeitos de uma delegacia de polícia. Inclusive, nós impetramos recentemente, pela Coordenação de Defesa Criminal da Defensoria, juntamente à Rafaela Garcez, brilhante Defensora que atuou no caso, um mandado de segurança em favor de um rapaz que respondeu por um crime simples de receptação e, por conta disso, teve sua foto incluída no álbum de suspeitos de uma delegacia de polícia e vinha sendo sistematicamente reconhecido por vítimas de roubo. Mesmo depois ter conseguido provar a sua inocência em diversos processos (inclusive no próprio processo por receptação!), [sendo que] não pendia nenhuma condenação definitiva contra si, sua fotografia continuava constando do álbum de suspeitos, sem qualquer justificativa. Então, nós oficiamos a delegacia e, na falta de resposta,

impetramos mandado de segurança.[6] Essa é uma ação individual que pode ser feita.

Porém, na realidade, as ações relativas ao álbum de suspeitos são insuficientes porque, muitas vezes, não são exibidas fotografias desse álbum, mas sim fotos [que constam em] redes sociais, e, nesse ponto, é possível traçar um paralelo com a questão digital. Há, também, uma questão de proteção de dados pessoais, tendo em vista que, por vezes, as redes sociais de um suspeito são vasculhadas, para que as fotografias sejam exibidas para reconhecimento, em seu prejuízo e sem autorização. Então, a própria problemática do álbum de suspeitos vai ficar obsoleta, porque as fotos já estão sendo colhidas através das redes sociais, e, nesse caso, o descontrole e a aleatoriedade são ainda maiores e mais preocupantes.

Muitas vezes, também, é mostrada uma única fotografia para a vítima ou testemunha, o que chamamos de reconhecimento *show-up*, em oposição ao reconhecimento *line-up*, em que são exibidas várias fotos, de pessoas com características físicas semelhantes. Não raro, a vítima, posteriormente, em juízo, informa que, no momento do reconhecimento ou anteriormente, recebeu informações de que aquela pessoa já era suspeita - que já vinha cometendo roubos na região, por exemplo -, e esse fator tem um potencial muito grande de gerar um induzimento da vítima no sentido de que aquela pessoa cometeu o crime. Aliás, o reconhecimento *show-up* é um problema não só do reconhecimento fotográfico, mas também do reconhecimento presencial. Nesse sentido, costumamos dizer que, quando há apenas uma pessoa ou foto, e não um

6. Em 08/09/2021, o Juízo da 1ª Vara Criminal da Comarca de Nilópolis concedeu liminar e, em 28/03/2022, julgou procedente o pedido para conceder a ordem, tornando definitiva a liminar anteriormente concedida, para determinar que o delegado de polícia da 57ª Delegacia exclua a imagem de T.V.G. do cadastro de suspeitos da 57ª Delegacia de Polícia Civil, vedando-se, por consequência lógica, a exibição de sua fotografia em qualquer procedimento referente a qualquer crime em apuração e que tenha ocorrido dentro do limite territorial da Comarca de Nilópolis. Da decisão, o Ministério Público interpôs recurso de apelação. Até a finalização do presente artigo, ainda não tinha ocorrido o trânsito em julgado. Processo nº 0006376-54.2021.8.19.0036.

/ INJUSTIÇAS [...] RECAEM, PRINCIPALMENTE, SOBRE A POPULAÇÃO NEGRA, POBRE E PERIFÉRICA /

/ NO BRASIL, NEM SEQUER CONSEGUIMOS, AINDA, IMPLEMENTAR REGULAMENTAÇÕES E PRÁTICAS MINIMAMENTE JUSTAS /

alinhamento de pessoas ou fotos, isso na realidade não se trata de um reconhecimento, mas de um verdadeiro *apontamento*.

Estamos atuando, na Coordenação de Defesa Criminal da Defensoria do RJ, em um caso absurdo de reconhecimento fotográfico, realizado através da foto 3x4 constante de uma carteira de habilitação, e nós impetramos uma ação constitucional de *habeas corpus* com pedido de revogação da prisão preventiva e também de trancamento da ação penal. Em hipóteses semelhantes, em que a ação penal é deflagrada com base exclusivamente em reconhecimento fotográfico, sem a realização de qualquer outra diligência investigativa, é possível requerer o trancamento da ação penal, por ausência de justa causa.

Muitas vezes, também, são enviadas fotografias, pela polícia, diretamente para o celular das vítimas. Essa prática também tem um enorme potencial de formar falsas memórias, pois pode induzir a vítima ou testemunha a reconhecer aquela pessoa, cuja foto fica armazenada em seu aparelho telefônico e à sua disposição para observá-la a qualquer momento e até mesmo por repetidas vezes.

No Estado do Rio de Janeiro, o documento que é produzido em delegacia por ocasião do reconhecimento de pessoas é um auto de reconhecimento, que é padronizado e que não traz quase nenhuma informação. Seria necessário que fosse feita uma gravação do momento de reconhecimento, para que o procedimento fosse o mais fidedigno possível. Na prática judiciária, observa-se que, em juízo, muitas vítimas afirmam que, na verdade, somente assinaram um documento sem entender seu conteúdo, ou então que reconheceram sem dar qualquer certeza naquele momento, mas o termo não retrata nada disso. Então, a gravação poderia ser uma forma de fiscalização, a fim de garantir a lisura do procedimento de reconhecimento.

Mas fato é que tudo isso carece de regulamentação. A única norma que temos, atualmente, sobre o tema de reconhecimen-

to de pessoas é o artigo 226 do Código de Processo Penal. Esse artigo traz alguns requisitos para o procedimento, que, na realidade, são muito poucos. O primeiro, é que o reconhecedor precisa fazer uma descrição das características físicas da pessoa a ser reconhecida. Depois, a pessoa a ser reconhecida deve ser colocada do lado de dublês, ou seja, de pessoas com quem ela tenha semelhança física, se possível. E, finalmente, é necessário que tudo isso seja registrado em um auto pormenorizado.

Contudo, o artigo 226 do CPP não prevê expressamente a possibilidade de o reconhecimento ocorrer através de fotografia e, por esse motivo, há quem diga que o reconhecimento fotográfico sequer é autorizado pelo direito brasileiro. Essa é uma outra tese que também pode ser ventilada, porém essa linha de pensamento não vem sendo acolhida pelos tribunais. E, mais do que isso, há autores que defendem que o reconhecimento fotográfico, se feito corretamente, pode ser dotado de confiabilidade e, inclusive, pode vir a ser mais justo do que o reconhecimento presencial, por possuir menos potencial de gerar erros.

Assim entendem, por exemplo, Janaina Matida e William Ceconello,[7] que afirmam que o reconhecimento fotográfico deve ser encarado de frente, como uma realidade posta, não havendo "substanciais vantagens epistêmicas na adoção do reconhecimento presencial em detrimento do reconhecimento fotográfico". Aduzem os autores que, na realidade, a modalidade fotográfica pode ser uma boa alternativa às limitações práticas do reconhecimento presencial, já que nem sempre há pessoas com as mesmas características do suspeito disponíveis. Nessa linha, o reconhecimento fotográfico permitiria um alinhamento justo de fotografias de pessoas que não destoassem fisicamente do suspeito.

7. MATIDA, Janaina; CECCONELLO, William W. Reconhecimento fotográfico e presunção de inocência. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 7, n. 1, p. 409-440, jan./abr. 2021. Disponível em <https://doi.org/10.22197/rbdpp.v7i1.506>. Acesso em 14/04/2022.

Os autores apontam, ainda, que devem ser alinhadas fotos de pessoas sabidamente inocentes da prática do delito em questão - os chamados *fillers* -, de forma que um eventual apontamento da pessoa que não é a suspeita não gere um desvio daquela investigação e, com isso, um possível novo erro judiciário. Seriam necessários, ainda, o fornecimento de instruções adequadas ao reconhecedor, bem como a ausência de *feedbacks* a este, com relação ao resultado do reconhecimento, por parte do investigador.

Há diversos outros requisitos apontados pela doutrina, com base nos estudos da psicologia do testemunho, para que o reconhecimento fotográfico tenha validade. Uma das exigências, por exemplo, é que a autoridade policial ou o investigador que conduz o procedimento de reconhecimento não pode saber quem é o suspeito. Isto é, deve haver uma dúvida também por parte do investigador, sobre a pessoa a ser reconhecida, para que ele não induza, ainda que de forma involuntária, o reconhecedor. A esse fator, dá-se o nome de "duplo-cego".[8]

A irrepetibilidade do procedimento de reconhecimento também é um importante preceito apontado pela doutrina, no sentido de que o reconhecimento, enquanto prova penal dependente da memória humana, não pode ser repetido, dada a possibilidade de alteração permanente da memória, que é dotada de maleabilidade, por ocasião de seu processo de recuperação.[9]

Então, fato é que, apesar da falta de previsão legal expressa do reconheci-

8. STEIN, Lilian Milnitsky; ÁVILA, Gustavo Noronha de. Avanços científicos em psicologia do testemunho aplicados ao reconhecimento pessoal e aos depoimentos forenses. Brasília: Secretaria de Assuntos Legislativos, Ministério da Justiça (Série Pensando o Direito, nº 59). Disponível em <PoD_59_Lilian_web-1.pdf (mj.gov.br)>. Acesso em 14/04/2022.

9. CECCONELLO, William Weber; ÁVILA, Gustavo Noronha de; STEIN, Lilian Milnitsky. A (ir)repetibilidade da prova penal dependente da memória: uma discussão com base na psicologia do testemunho. Revista Brasileira de Políticas Públicas, Brasília, v. 8, nº 2, 2018 p. 1057-1073. Disponível em <https://www.publicacoes.uniceub.br/RBPP/article/view/5312/3982>. Acesso em 14/04/2022.

mento fotográfico no direito brasileiro, a tese que possui maior chance de sucesso é no sentido de que o reconhecimento por foto pode, sim, ser realizado, desde que se observe uma série de requisitos que são essenciais à sua lisura, confiabilidade e sua validade.

Nesse ponto, é interessante notar que o artigo 226 do CPP é extremamente vago, não trazendo os requisitos mencionados acima, que são, atualmente, apontados pela doutrina especializada no tema. Então, é essencial a reforma da legislação para que ela traga todos os requisitos exigidos para um reconhecimento justo, a serem observados de forma obrigatória, sob pena de invalidade do procedimento.

Vale observar que, desde o ano de 2020, a jurisprudência dos Tribunais Superiores, principalmente do Superior Tribunal de Justiça, tem sofrido uma reviravolta, inclusive impulsionada pelas pesquisas da Defensoria Pública do Estado do Rio de Janeiro, no que se refere à questão do reconhecimento fotográfico.

Com efeito, anteriormente, entendia-se que as disposições do artigo 226 do Código de Processo Penal configurariam mera recomendação, e não uma exigência, de forma que a sua inobservância não ensejaria a nulidade do reconhecimento - que, inclusive, poderia ser ratificado em juízo e constituir meio idôneo de prova apto a fundamentar condenação.

Em verdadeira virada de chave, no julgamento do paradigmático HC 598.886/SC,[10] o STJ passou a entender que o artigo 226 do CPP traz requisitos de observância obrigatória, sob pena de nulidade do ato. E, mais do que isso, que a nulidade do reconhecimento em delegacia macula eventual reconhecimento pessoal positivo em juízo, de maneira que eventual reconhecimento pessoal positivo em juízo não poderia servir para ratificar um reconhecimento inválido feito em delegacia. Assim, é possível afirmar que o STJ percebeu o potencial sugestionador de um reconhecimento em delegacia realizado sem as formalidades legais mínimas necessárias à sua validade. Essa é uma tese muito forte para ser levada aos tribunais superiores.

Por fim, interessante colocar a seguinte questão para reflexão: como vimos, no Brasil, nem sequer conseguimos, ainda, implementar regulamentações e práticas minimamente justas no que se refere ao reconhecimento feito por pessoas, principalmente, o fotográfico, o que torna ainda mais preocupante a problemática do reconhecimento facial como ferramenta de segurança pública.

Isto porque essa tecnologia confere uma aparente objetividade, e, portanto, uma alegada legitimidade ao procedimento de reconhecimento de pessoas e aos seus resultados, com a suposta exclusão do elemento humano, potencialmente errôneo e falho. Ocorre que, na realidade, sabemos da questão referente à discriminação algorítmica e do grande índice de resultados falsos-positivos obtidos por essas ferramentas, dada a forma como são programadas, treinadas e empregadas, bem como os vieses dos bancos de dados utilizados.

Por esse ângulo, se, como exposto, um olhar mais profundo sobre o reconhecimento fotográfico é capaz de escancarar o viés racial envolvido nessa prática - que é bastante analógica, por assim dizer -, o mesmo ocorre com as modernas e digitais ferramentas de reconhecimento facial, que, apesar de suas aparentes imparcialidades de máquina, apenas fazem reproduzir discriminações estruturais já existentes em nossa sociedade.

Há muito o que falar sobre o tema. Gostaria de agradecer muito pelo convite e pela presença de todas e todos. Obrigada!

10. Superior Tribunal de Justiça, HC nº 598.886/SC, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, por unanimidade, julgado em 27/10/2020, DJe 18/12/2020.

12.

MANDATO POLICIAL, SISTEMA DE JUSTIÇA E PROCESSO PENAL NO BRASIL[1]

Felipe da Silva Freitas

1. Texto que tem por base a transcrição da palestra apresentada por Felipe da Silva Freitas no Painel "Teses: Reconhecimento Pessoal" no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em 03/09/2021. A transcrição foi revisada pelo autor.

Olá. Bom dia! Bom dia a todas e a todos. Para mim é uma alegria muito grande estar aqui tanto pelo papel do InternetLab e da Faculdade de Direito da USP na análise dos temas contemporâneos quanto pela urgência do tema e pelo significado real e concreto que ele tem na vida das pessoas, na vida das comunidades e na forma que essas pessoas experienciam um contato majoritariamente traumático com as forças policiais e com o sistema de justiça criminal.

E pensei em destacar aqui, nessa rápida conversa, quatro pontos que eu considero muito importantes para fortalecer a nossa discussão sobre esse tema e para tentar ampliar uma questão que geralmente aparece no pano de fundo desse debate, que é a da relação entre Polícia e Justiça. Da forma pela qual o sistema de justiça trata a ação policial, o papel das polícias, tanto da Polícia Militar - do policiamento ostensivo -, quanto da polícia investigativa.

DISCRICIONARIEDADE DA AÇÃO POLICIAL

O primeiro aspecto, que me parece muito importante, é de se destacar que não há ação policial sem discricionariedade. Algum nível de discricionariedade é muito próprio das forças policiais, sobretudo do policiamento ostensivo, mas não só. Na ponta da cadeia do Processo Penal, a gente sempre vai ter uma atuação policial, que desenvolve um processo de seleção, que vai resultar ou não na investigação, na prisão ou no processamento de pessoas. Portanto, essa dimensão discricionária é quase que uma etapa inescapável da ação policial.

De modo que, o grande desafio a se fazer é fixar protocolos para que estas escolhas sejam passíveis de controle social e para que se produza previsibilidade de como deve se estabelecer essa interação policial mesmo sabendo que há uma parte desta interação que é eminentemente imprevisível. Mas, ao mesmo tempo, fortalecer as vias de controle dessa atuação, tanto por meio de instâncias internas, que possam ser pressionadas politicamente pelas organizações e pelo conjunto da sociedade, como também pela via do controle externo do Ministério Público e da sociedade, através de suas instâncias políticas de pressão e de controle social.

No mesmo sentido é também importante destacar que tem se falado muito pouco do controle da ação policial pela via judicial, ou seja, discutimos pouco como o estabelecimento de parâmetros, ou reconhecimento dos parâmetros constitucionais - bastante rígidos para a persecução penal - são considerados no processo de tomada de decisão dos juízes e juízas, para que isso seja, também, uma forma de controle da ação policial.

Então, esse é um primeiro aspecto que me parece muito importante e que atravessa essa questão do reconhecimento, em vários níveis: como se produz uma baliza democrática para o exercício da discricionariedade policial? A questão latente a este debate é resolver como se viabiliza, ao mesmo tempo, a flexibilidade necessária para uma atuação policial eficaz, no sentido do oferecimento de respostas sociais, em termos de responsabilização e elucidação dos fatos violentos e que demandam uma resposta estatal. Mas, ao mesmo tempo, se fixam balizas rígidas que deem previsibilidade, por um lado, e que deem transparência, para que isso possa ser objeto de debate público.

É preciso que haja transparência sobre essas formas para que a gente possa acessar, não uma previsão normativa genérica, mas o cotidiano dessas práticas. Que se possa olhar para elas e incidir sobre elas, a partir da política, com a seguinte discussão: qual tipo de parâmetro nós, como sociedade, constituímos para que as forças policiais atuem? Para isso, é fundamental que a gente veja o que a polícia faz e não apenas o que a polícia diz que faz, mas que a gente acesse, objetivamente,

e que possa observar o que a polícia faz. Mas não só ela, todas as instâncias de controle.

Dito de outra forma, me parece que há aqui um desafio central de definir melhor, política e juridicamente, qual é a extensão do mandato policial dentro de uma sociedade democrática.[2] Não só em termos daquilo que nós chamamos de policiamento ostensivo, mas também no curso das investigações policiais. Então acho que é preciso um arcabouço democrático que nos viabilize, não só uma análise mais rigorosa e precisa, mas também uma intervenção que evoque a vida democrática, com essas práticas tão embotadas pelo autoritarismo.

2. Sobre o tema ver: FREITAS, Felipe. Polícia e Racismo: uma discussão sobre mandato policial. Tese de Doutorado, Programa de Pós-Graduação em Direito, Universidade de Brasília, 2020.

A FALTA DE BALIZAS PROCESSUAIS DE VALORAÇÃO DAS PROVAS

Um segundo aspecto dessa questão, me parece ser a constatação de que há, no cotidiano das interações processuais com o trabalho das polícias, uma profunda desídia, um profundo desprezo com a constituição de uma matriz de decisão no âmbito processual. Tanto na sua dimensão legislativa, quanto na sua dimensão jurisprudencial, que ofereça um compasso, que ofereça uma regra, que ofereça um parâmetro decisório, do qual esses agentes não podem se afastar, sob pena de estarem rompendo com a Constituição e com a ordem democrática. Isso é fundamental de ser constituído, porque isso é a condição necessária para que se interrompa um ciclo de práticas abusivas e autoritárias, que a professora Manuela Abath Valença,[3] processualista importante da nossa geração, chama de "soberania

3. VALENÇA, Manuela Abath. Soberania policial no Recife do início do século XX. Tese de Doutorado, Faculdade de Direito, Universidade de Brasília, 2018.

/ TEM SE FALADO MUITO POUCO DO CONTROLE DA AÇÃO POLICIAL PELA VIA JUDICIAL /

policial", ou que a professora Jaqueline Muniz vai chamar de "autonomização predatória das forças policiais".[4]

Ou seja, é preciso que se produza protocolos legislativos, protocolos reconhecidos em lei, um pouco como a Dra. Isabel sublinhou. Mas não apenas para ser uma referência para o que a polícia vai fazer em termos do que hoje está muito sendo discutido (ex.: controle da politização das polícias etc.). Mas para o controle dessa dimensão da politização da ação policial, que é a adoção de práticas completamente alheias ao texto legal. Essa é uma dimensão da politização das forças policiais, no sentido de que, se produz uma normatividade extralegal, que é carimbada pelo Poder Judiciário, pelo Ministério Público, muitas vezes, quase que num processo de renúncia à sua própria atribuição institucional.

Portanto, o que está em jogo ao exigir uma baliza, ao se falar, como fala a professora Janaína Matida,[5] numa baliza processual mais rigorosa para valoração dessas provas, e para o procedimento de produção dessas provas, diz respeito à, no fundo, um resgate do papel decisório do Poder Judiciário, e em alguma medida do Ministério Público, que não é, propriamente, um poder decisório, mas é um papel institucional, no sentido de resgatar o seu próprio significado processual. Porque a mera corroboração da prática informal estabelecida em sede de investigação, sem uma nova valoração a partir dos critérios judiciais, no fundo, é também uma renúncia do Poder Judiciário, não só à sua própria obrigação, mas às suas próprias prerrogativas. Então, no fundo, a prevalência dessas práticas informais representa um desprestígio que o Poder Judiciário produz sobre si mesmo, um rebaixamento que se põe na condição de um mero carimbador de práticas informais, com pouco poder decisório e com pouca capacidade reflexiva sobre o que se lhe apresenta em termos processuais. Por sua própria conduta o Judiciário se coloca muitas vezes como mero homologador acrítico do que fazem as polícias na rua.

4. MUNIZ, Jacqueline de Oliveira. Fé cega, facas amoladas: regime do medo e práticas de exceção. Trincheira Democrática: Boletim do Instituto Baiano de Direito Processual Penal. Ano 2, n. 6, Dezembro 2019, p. 7 – 8.

5. MATIDA, Janaina R.;VIEIRA, Antonio. Para além do BARD: uma crítica à crescente adoção do standard de prova 'para além de toda a dúvida razoável' no processo penal brasileiro. Revista Brasileira de Ciências Criminais, v. 156, p. 221-248, 2019.

OS RISCOS DE CONDENAÇÃO INDEVIDA

Em seguida, eu acho que tem um outro aspecto que é: como, nas franjas - ou nas fronteiras - dessa ação policial, vão aparecendo vários conceitos pouco precisos, como "fundadas suspeitas", das buscas pessoais ou domiciliares sem mandado, e também do reconhecimento fotográfico realizado sem parâmetro, que, no fundo, põem em risco o sentido do processo penal democrático e, na prática, colocam em risco todo o sistema processual. Tanto porque produzem decisões injustas, no sentido de que produzem a condenação de inocentes, ou seja, põem em questão o próprio sentido ético da Justiça, mas, também, o seu sentido democrático de proteção e de garantia. Então essas duas dimensões são postas em risco.

Como vem sendo ressaltado em outros estudos sobre o tema, tanto da academia, tanto da sociedade civil, quanto da imprensa, há efeitos danosos no reconhecimento fotográfico como uma fonte de condenação de pessoas inocentes e, portanto, da mais radical forma de erosão do sentido do Poder Judiciário no campo penal. Condenar pessoas inocentes com base numa prática informal, que não tem sequer lastro cognitivo, eu diria, para produzir uma inteligibilidade de condenação, é algo muito grave porque transforma um ato informal e atécnico num único referente para a tomada de decisão.

Aquele reconhecimento com foto não é um dos elementos do processo de condenação. Ele é o único elemento, muitas

vezes, do processo de condenação. E, nesse sentido, me parece que nada pode ser mais danoso ao sentido ético da justiça do que a condenação de uma pessoa inocente. Eu não estou falando aqui do erro judicial e não estou falando aqui de um problema do desvio que ocorre dentro das formações do entendimento dos atores do sistema de justiça. Eu estou falando de um modelo que é produzido para gerar erro judicial, que é produzido para gerar condenação de inocentes, e que portanto, é a porta de entrada para a repetição dos estereótipos raciais, que são o sustentáculo em torno do qual se produz na sociedade as noções de suspeição.

O PAPEL DOS DIREITOS HUMANOS

E eu, nesse sentido, encerro resgatando o importante papel que me parece que pode ser cumprido pelo Direito Internacional, dos Direitos Humanos e pelo direito comparado, para explorar também, nas nossas teses, argumentos relativos à seletividade e ao perfilamento racial. São conceitos que vêm sendo desenvolvidos, no campo das ciências sociais e a partir das denúncias do movimento negro - e cujo significado jurídico vem sendo explorado no campo do sistema das Nações Unidas como uma prática que vai produzindo a erosão dos sistemas judiciais. A ideia de seletividade ou perfilamento racial aponta que há uma estrutural de chancela judicial a práticas policiais informais, abusivas, que são, ao fim e ao cabo, responsáveis pela erosão do sistema democrático. E [também] são repetidoras de processos de exclusão racial, cujo impacto é letal, e é totalmente desconstitutivo das comunidades, que ficam absolutamente desprotegidas e afastadas de um processo judicial justo, democrático e com garantias.[6]

6. Ver: ADPF 635 STF e Caso 12.315 da CIDH - Alberto Fernández Prieto & Carlos Alejandro Tumbeiro vs. Argentina.

Acho que isso é um conjunto de argumentos importantes, que podem ser manejados, e devem ser manejados, por nós em diferentes esferas para visibilizar essa outra forma de politização das polícias e do sistema de justiça, que me parece tão danosa quanto as outras que vêm sendo fortemente sublinhadas nas últimas semanas, sobretudo diante da postura autoritária do presidente da República - que patrocina, a partir de seu discurso, o horror e a violência como método de governo. Acho que esses são alguns aspectos importantes para a gente avançar na reflexão. Obrigado.

13.

RECONHECIMENTO FACIAL, CULTURA DE VIGILÂNCIA E HERANÇAS COLONIAIS[1]

Bianca Kremer

1. Texto que tem por base a transcrição da palestra apresentada por Bianca Kremer no Painel "Teses: Reconhecimento Facial" no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em 03/09/2021. A transcrição foi revisada pela autora.

Bom dia a todas e a todos. Para mim é um prazer estar aqui com vocês nesse Congresso com uma temática tão importante e tão urgente, relativa ao uso de tecnologias na era digital, fazendo esse tensionamento com a Justiça Criminal e o Processo Penal. Quero agradecer o convite do InternetLab e da Faculdade de Direito da USP, sobretudo na pessoa do Pablo que é, além de um grande querido, um super especialista no tema, por quem nutro uma profunda admiração que não é segredo para ninguém.

Eu venho trabalhando com Direito e Tecnologia há bastante tempo e, nos últimos anos, obviamente por interesse na temática mas sobretudo por questões de urgência, venho me debruçando sobre a temática do reconhecimento facial e as suas aplicações no Brasil. Aplicações, possibilidades, impossibilidades, limites e condições de possibilidades, para falar a verdade.

E hoje, para falar com vocês, eu escolhi uma abordagem talvez um pouco diferente, que a princípio pode parecer acadêmica, mas na verdade esse é um convite de disputa política. Eu venho trabalhando com ativismo digital há bastante tempo, no sentido de promover direitos digitais no combate ao racismo nesse espaço, e posicionando e mobilizando o Direito nesse debate, nessas disputas políticas. Esse é o papel que eu venho desempenhando não só como líder de pesquisa na FGV, mas sobretudo perante a Coding Rights, em que trabalho como *fellow* em políticas de *Advocacy, Public Policy* e também pesquisa.

Então, a conversa que eu quero iniciar nesse painel é, na verdade, muito mais do que falar sobre reconhecimento facial, falar sobre cultura de vigilância. E mais do que falar sobre cultura de vigilância, eu quero conversar sobre cultura de vigilância nessa modernidade digital que nós herdamos a partir de uma disputa de olhares político-epistêmica por uma decolonialidade de perspectiva negra.

O que eu quero dizer com isso, na verdade? Eu quero fazer uma reflexão histórica em relação a processos de naturalização da barbárie que vêm sendo incorporados institucionalmente, e também a partir da nossa consciência enquanto indivíduos, sujeitos de direito, e sociedade. Então, basicamente quero conversar sobre naturalização da barbárie agora a partir do uso de novos aparatos tecnológicos, e para isso vou fazer minhas as palavras da Thula Pires e da professora Ana Flauzina - uma professora da PUC-Rio, e a outra professora da UFBA - em que elas dizem "a importância de tomar assento no lugar que nos cabe e destacar o envolvimento das trincheiras jurídicas na conformação desse estado de coisas".

Nesse sentido, quando nós falamos sobre reconhecimento facial, normalmente nós atrelamos toda sorte de desenvolvimento tecnológico a um tecnossolucionismo, e mais do que isso a um tecnodeterminismo, como se nós naturalizássemos o processo de desenvolvimento tecnológico como natural de uma humanidade universalizante, e como se fizesse sentido para os modos de ser, estar e bem viver de toda essa coletividade construída e projetada como universal, universalizante, quando na verdade o que ocorre é uma invisibilização de hierarquias de humanidade que foram sendo e continuam sendo construídas e reverberadas no tecido social, sobretudo brasileiro.

Então, tomando assento nesse lugar que me cabe de mobilização do Direito para pensar essa cultura de vigilância nessa modernidade digital comprometida com essa disputa político-epistêmica, e portanto de interpretação, dentro dessa disputa por esse olhar de perspectiva negra, eu quero fazer uma reflexão sobre exercício de liberdades sem amarras de vigilância.

Como eu tenho esse compromisso por uma decolonialidade de perspectiva negra, eu não posso me furtar de forma alguma a relembrar o processo de transição que nós vivemos e que nós esquecemos - seja intencional ou não intencionalmente - da transição do período da abolição da escravatura - ou da pretensa abolição da escravatura - que aconteceu no Brasil em 1888, para

a transição do Brasil Império para a República que aconteceu em 1889, portanto, nesse período de um ano. O que aconteceu entre a abolição da escravatura e essa transição desse período histórico que nós vivíamos - o Brasil Império para a República?

Basicamente, uma mudança nos nossos interesses sociais e políticos - e mais do que isso, o que eu quero falar é por quê faz sentido falar dessa invisibilização dos processos de transformação desses interesses na construção desse Estado-nação para essa conformação desse estado de coisas. E o papel do Direito, o envolvimento das trincheiras jurídicas na perpetuação desse cenário hoje experienciado com o uso de tecnologias de reconhecimento facial.

Nesse período o que nós tínhamos era uma sociedade rural aristocrática, familiar paternalista, burguesa mas muito mais ligada a interesses latifundiários e muito ligada a uma colonialidade do poder. Ou seja, no tecido social era uma sociedade que vivia uma série de privilégios e a hierarquização de humanidades construída nesse país, nesse Brasil Colônia, conseguiu ser experienciada de maneira muito mais privilegiada por esses sujeitos que performavam esse espaço de poder dentro das suas propriedades latifundiárias em detrimento dos demais, sobretudo a população negra e indígena.

O que eu quero dizer aqui para os senhores é que os institutos jurídicos que nós construímos nessa transição, que viabilizavam qualquer sorte de liberdade ou que tratavam sobre elementos como liberdade, autonomia, eles vieram sendo construídos aliados a políticas de genocídio e escravização de povos subalternizados e colonizados, sobretudo negros e indígenas.

Então, o que a gente percebe hoje com o uso de reconhecimento facial? Por que a gente tem a reverberação de violências, não só com o uso dessas tecnologias sendo denunciado por pesquisas de ponta como as desenvolvidas pelo Pablo no Panóptico do CESeC, demonstrando em números que 90,5% da

/ HISTORICAMENTE NÓS VIVEMOS UM PROCESSO EM QUE AOS NEGROS NUNCA FOI FACULTADO O EXERCÍCIO DE UMA LIBERDADE SEM AS AMARRAS DA VIGILÂNCIA /

população até então mapeada e diagnosticada por um sistema de reconhecimento facial eram pessoas negras? Por que isso acontece? Por que a gente não pode chamar de erro de sistema? Porque eu quero chamar de naturalização da barbárie com o uso de novos aparatos tecnológicos.

O que aconteceu com essas elites dominantes, para a gente entender o contexto onde a gente está inserido agora? Houve um desencontro entre os interesses sociais e os interesses políticos. Os interesses políticos eram da transição para uma república, mas para a transição para uma república a gente precisava construir um Estado-nação, uma integração social. Mas os interesses sociais dessas elites dominantes não coadunavam com seus interesses políticos. Ou seja, não tinha possibilidade de transformação desse capital comercial produzido por esses latifúndios em um capital industrial. O que acontecia era uma importação das elites europeias, ou do norte global.

Portanto, a produção industrial aqui não foi integrativa, porque não havia interesse de assalariamento dessa população negra. Como é que você iria assalariar algo que era seu, uma coisa que no ano passado era sua? Como denominar esse potencial assalariado, esse potencial trabalho livre, nos termos da liberdade se a própria conformação de liberdade não fazia sentido dentro desses interesses sociais dominados por essa lógica de colonialidade do poder?

Então aí já havia uma dificuldade. Estou falando da Segunda Revolução Industrial, porque ela não estava acontecendo aqui nos mesmos termos de outros espaços do mundo. Basicamente, a Primeira Revolução Industrial foi até 1840, e tinha como sentido a transformação da manufatura. A Segunda Revolução Industrial foi mais ou menos em 1850. Em 1940, 1945 foi a nossa industrialização, portanto nosso capital industrial, não englobou a incorporação da população negra e indígena na construção desse "novo" (com muitas aspas) Estado-nação.

Então, basicamente eu quero trazer para nossa reflexão que, se isso aconteceu na Segunda Revolução Industrial, quando houve a Terceira Revolução Técnico-Informacional, quando houve a Quarta Revolução - a automatização de processos com uso de inteligência artificial - por que existe a reverberação de vieses raciais e toda sorte de categorias de opressão de gênero, raça, sexualidade, classe, deficiência, senioridade e, dessa vez, fazendo esse compromisso com a perspectiva negra, que foi a que iniciei a minha fala e com ela eu encerro?

Historicamente, nós vivemos um processo em que aos negros nunca foi facultado o exercício de uma liberdade sem as amarras da vigilância. Nossos ancestrais - e aqui faço minhas as palavras de Abdias do Nascimento - "quanto a mim sinto-me parte da matéria investigada", nunca puderam exprimir a sua religião/religiosidade, o seu lazer nos espaços públicos, a sua existência e resistência nos espaços com seus corpos, sem que os olhos das elites dominantes replicassem sobre essas corporalidades estereótipos derivados de preconceitos e tornados ação por processos de discriminação ativa.

E é nesse espaço de vigilância, à época o medo do Haitianismo e da Revolução e da perda das dinâmicas de poder herdadas nessa colonialidade do poder, hoje nós experienciamos isso sobre outros circunspectos, mas ainda sob os auspícios desses estereótipos pautados nessa discriminação, nesse preconceito racial, de modo que, tendo no racismo a mola propulsora de toda forma de produção capitalista que foi desenvolvida nesse país, mas não apenas isso, como condição estruturante da forma como nós herdamos esse processo de construção de Estado-nação em que esses interesses sociais de transformação de capital comercial em capital industrial - e aqui, falando sobre novas tecnologias - são diferenciados.

Então, portanto, senhores, faço aqui a finalização da minha fala no sentido de que nós rememoremos que essa realidade

punitivista de herança colonial que nós herdamos, agora com a institucionalização da barbárie - antes de modo privado dentro dos espaços dos latifúndios dominados por senhores de engenho, e agora conformados politicamente, sendo esse processo de vigilância transferido para as instituições - que nós reconheçamos essa realidade punitivista de herança colonial como resultado dessas ideias mitificadas de humanidade e progresso que nós herdamos nesse processo de conformação de coisas.

E nós não esqueçamos que a raça figura nesse processo como um critério básico de classificação, e não será diferente com o uso de reconhecimento facial nos espaços públicos por essas mesmas instituições que, ao argumento de aplicação de Segurança Pública para essa universalidade dessa humanidade construída com o apagamento desses espaços de discriminação, e essas hierarquias de humanidade que se desenvolveram no território brasileiro. E que nós não esqueçamos que as tecnologias de informação e comunicação hoje têm servido de suporte para a intensificação dessas práticas ligadas a monitoramento e controle, não só de identificação, mas de toda uma movimentação dessas corporalidades negras e indígenas, e também para os seus acessos ou impossibilidade de acessos pelos usos de tecnologias de vigilância e de securitização.

Que nós reconheçamos a herança colonial que herdamos, essa herança colonial que nos sobrepõe enquanto sociedade brasileira, e que nós nos posicionemos - de maneira crítica, política e ativa - processos e práticas antirracistas com o uso dessas tecnologias nos espaços públicos e privados.

Então, esse é um convite à reflexão para que nós reconheçamos que os vieses não vêm do acaso, do espaço e da mente de pessoas preconceituosas, pessoas que nasceram com espírito ruim. Que ela vem de um estado de conformação de coisas, de uma herança cultural que se desdobra até os dias atuais por força de uma não incorporação da população negra como projeto de Estado-nação do nosso tecido social brasileiro.

Então, muito obrigada, Pablo, pelo espaço, e eu espero que nós possamos cada vez mais desmistificar esse tecnodeterminismo que continuamos herdando agora a partir dessa suposta - ou denominada - Quarta Revolução Industrial, com a automatização de processos. Muito obrigada.

14.

UMA ESTRUTURA REGULATÓRIA PARA O USO DO RECONHECIMENTO FACIAL

Owen Larter

Bom dia a todos. Muito obrigado por me receberem hoje, e um grande obrigado ao InternetLab por organizarem esta sessão realmente importante com uma seleção fantástica de oradores. Devo admitir que gostei muito dos comentários muito atenciosos de Bianca Kremer e na verdade aprendi muito com eles. Portanto, estou muito satisfeito por poder participar deste painel hoje.

Como Pablo mencionou, meu nome é Owen Larter e estou no departamento responsável pela Inteligência Artificial (I.A.) da Microsoft. E o que eu queria falar é sobre a importância de se criar novas salvaguardas regulamentares para a tecnologia de reconhecimento facial, para que os benefícios da tecnologia possam ser realizados - porque acreditamos que há benefícios - mas de uma forma que garanta que a tecnologia seja utilizada de forma responsável.

Portanto, eu queria começar meus comentários dando um pequeno passo atrás e observando algumas das principais tendências em torno do uso das tecnologias I.A. em geral - porque nos últimos 18 a 24 meses, vimos uma rápida aceleração na implantação da I.A. - seguramente também devido à COVID 19, em que vimos a I.A. sendo usada para alimentar tudo, desde chatbots de saúde até a triagem de pacientes antes de entrarem no hospital, passando pela assistência no desenvolvimento de vacinas e tratamentos.

Também temos visto a crescente implantação da I.A. no setor privado, incluindo, em parte, para responder à necessidade de trabalhar de forma mais remota e mais flexível.

E esta maior implantação de I.A. levou a uma maior consciência pública de seus impactos e também a um maior escrutínio regulatório, o que nós na Microsoft consideramos uma coisa boa. Pensamos que precisamos criar uma nova estrutura regulatória para o uso da I.A., para que estas tecnologias possam ser usadas de forma responsável.

E na frente regulatória, acho que, mais notavelmente, as pessoas terão visto a publicação pela União Europeia (UE) de sua proposta de Lei de Inteligência Artificial[1]. Esta é a primeira tentativa de estabelecer uma estrutura horizontal para a regulamentação da I.A., concentrando-se na regulamentação dos sistemas de maior risco, o que nos parece um passo realmente importante neste caminho para a criação de uma estrutura regulatória.

1. SPproposta para um European AI Act, acessível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792#:~:text=The%20European%20Commission%20unveiled%20a,AI%20systems%20and%20associated%20risks.

E estas conversas regulatórias estão acontecendo em todo o mundo, como sabemos, e estão acontecendo em relação a uma série de diferentes áreas políticas e uma série de tecnologias I.A.

Voltando nossa atenção para a conversa de hoje, certamente algumas das áreas mais significativas do escrutínio regulatório é o reconhecimento facial.

Portanto, este slide aqui dá uma visão geral das conversas legislativas ao vivo nos Estados Unidos em torno da regulação da tecnologia de reconhecimento facial. É um cenário semelhante em outras partes do mundo também. Eu sei que há muitas conversas na UE e que é um tema muito quente também no Brasil. E assim, este slide certamente representa, nos EUA, a grande quantidade de atividades que está ocorrendo.

O que vimos é que, em certos casos nos Estados Unidos é que a conversa saltou direto para proibições sobre a tecnologia. Portanto, temos agora mais de 16 cidades e estados nos EUA que têm alguma forma de proibição do uso da tecnologia de reconhecimento facial.

Achamos que as conversas regulatórias são realmente importantes, mas que as proibições não são a resposta certa, sobretudo dada a significativa oportunidade que o reco-

nhecimento facial pode oferecer à sociedade, e também a forma como a tecnologia continua a se desenvolver quase que no dia-a-dia.

Portanto, eu queria mergulhar em alguns dos benefícios da tecnologia antes de analisar algumas das salvaguardas regulamentares que são necessárias.

Um benefício do qual as pessoas podem estar cientes é a forma como o reconhecimento facial está sendo usado pelo governo e pelas autoridades legais para tratar de questões de tráfico sexual e encontrar crianças desaparecidas. Assim, existe uma organização chamada Thorn, que tem uma ferramenta e um foco de atenção que usa o reconhecimento facial, trabalhando com as autoridades legais para identificar vítimas de tráfico. E os números são realmente impressionantes. Eles identificaram 18.000 vítimas de tráfico nos últimos quatro anos nos Estados Unidos e no Canadá, incluindo 6.000 crianças.

Há também muitos benefícios da tecnologia para as pessoas com deficiência visual. Assim, a Microsoft esteve envolvida em alguns projetos, um chamado Seeing I.A. e outro chamado Project Tokyo, onde a tecnologia está sendo usada para ajudar pessoas com baixa visão a interagir melhor em seu ambiente do dia a dia, inclusive no local de trabalho. A tecnologia ajudou alguém com visão subnormal a direcionar seu olhar para um colega quando ele está em uma reunião. Também é capaz de usar o reconhecimento facial para sinalizar à pessoa que usa o sistema que um de seus amigos, por exemplo, está do outro lado da cantina. Eles poderiam, assim, se envolver mais proativamente com as pessoas.

A tecnologia também é utilizada para prevenir fraudes. O Departamento de Veículos Automotores dos EUA[2] usa o reconhecimento facial para impedir a fraude na carteira de motorista. Eles usam a tecnologia para identificar quando a imagem de uma pessoa está associada a mais de uma carteira de motorista e, somente no estado de Nova York, já houve mais de 14.000 pessoas com duas ou mais carteiras registradas - todas elas fraudulentas.

E então a última que mencionei, e acho que muitas pessoas terão visto, é a forma como esta tecnologia está sendo usada em aeroportos ao redor do mundo para check-in sem contato, o que é realmente importante na abertura segura pós-COVID e também em termos de acelerar as pessoas através do aeroporto mais rapidamente.

Portanto, esperamos que isso transmita um pouco as oportunidades realmente vastas e variadas que o reconhecimento facial pode oferecer à sociedade. Mas acho que é muito, muito importante ser claro sobre os desafios reais que a tecnologia também apresenta se não for usada de forma responsável.

Há claramente desafios muito reais em torno da forma como governos menos democráticos estão usando o reconhecimento facial como parte de sua infra-estrutura de vigilância, muitas vezes de uma forma que prejudica significativamente e ainda mais as liberdades [civis].

Pensamos que isto é algo sobre o qual precisamos estar vigilantes em todos os países do mundo para garantir que o reconhecimento facial não seja usado de forma a minar a democracia e os direitos humanos. E talvez, construindo um pouco sobre o que Bianca Kremer estava falando, também é realmente importante garantir que a tecnologia não seja usada de forma que discrimine qualquer indivíduo ou membros de qualquer grupo em particular, e particularmente quando estiver sendo usada pelo governo e pela aplicação da lei.

E, de repente, vimos alguns exemplos disso quando as devidas salvaguardas e procedimentos não foram colocados em prática. O New York Times cobriu a história de Robert Williams, que foi preso injustamente por roubo, em parte devido a um

2. N/E: Em inglês, o *Department of Motor Vehicles in the U.S.*

reconhecimento facial incorreto tirado de algumas filmagens de CCTV. Assim, ele teve que passar por todo o incômodo de ser preso em casa e levado para interrogatório com base nesta combinação incorreta de reconhecimento facial, porque não havia salvaguardas adequadas no local.

Portanto, esperemos que este tipo de situação estabeleça a forma como realmente acreditamos que existem benefícios significativos em torno da tecnologia, que, naturalmente, se você pular diretamente para as proibições, você perde esses benefícios, mas também os desafios muito reais que devemos enfrentar para que a tecnologia seja usada de forma responsável.

E por isso pensamos que há uma série de passos que precisamos dar para podermos criar este conjunto de salvaguardas para uso responsável.

O primeiro pilar da abordagem, aqui, é a importância de ter conversas inclusivas de múltiplos atores sobre o papel do reconhecimento facial na sociedade.

Em segundo lugar, pensamos que as organizações podem fazer mais para desenvolver internamente sua própria capacidade para garantir que estão usando o reconhecimento facial de forma responsável.

E, importantemente, tudo isso precisa ser sustentado por novas regulamentações que garantam o uso responsável.

Portanto, apenas para gastar um pouco de tempo com cada uma delas, a conversa inclusiva é realmente essencial, e é por isso que eventos como o de hoje são tão importantes. E é fantástico ver a voz da sociedade civil e da academia representada na conversa de hoje. Eles são componentes essenciais da conversa em todos os países do mundo e trazem uma perspectiva realmente importante para a conversa.

Há também a responsabilidade de as empresas de tecnologia se engajarem proativamente nesta conversa, e de forma transparente. É muito importante que as empresas de tec-

/ PRECISAMOS ESTAR VIGILANTES [...] PARA GARANTIR QUE O RECONHECIMENTO FACIAL NÃO SEJA USADO DE FORMA A MINAR A DEMOCRACIA E OS DIREITOS HUMANOS /

/ QUAL FOI O DESEMPENHO? QUAL FOI A TAXA DE FALSAS COMBINAÇÕES? QUE TIPO DE INDIVÍDUOS E AGRUPAMENTOS TIVERAM ESSE IMPACTO? /

nologia compartilhem informações sobre como a tecnologia funciona, quais são as limitações da tecnologia e como ela não deve ser usada. É também muito importante que as empresas de tecnologia falem e também dêem um pouco de visão sobre onde a tecnologia está indo.

Então, apenas tocando rapidamente em como as organizações podem construir sua própria capacidade interna: isto é algo no qual nós da Microsoft, como desenvolvedor de tecnologias I.A. e desenvolvedor de reconhecimento facial, em particular, temos nos concentrado há vários anos.

Você pode ver neste slide nossa jornada de I.A. responsável, que começou em 2016 com um artigo de nosso CEO Satya Nadella, que estabelece que I.A. responsável seria uma prioridade chave para a empresa.

E você pode ver que, nos anos seguintes, construímos os blocos fundamentais de nosso programa de I.A. responsável, que leva nossos princípios de I.A. na Microsoft (que inclui coisas como a importância da inclusão, privacidade, segurança, transparência e responsabilidade) e assegura que nossos colegas estejam implementando esses princípios em seu dia-a-dia de trabalho. E o reconhecimento facial tem sido uma parte particularmente importante do nosso programa de I.A. responsável na Microsoft.

Voltando a 2018, nosso presidente Brad Smith, que lidera muito do trabalho da empresa nestas questões, escreveu um artigo pedindo pela criação de regulamentações para o uso responsável da tecnologia, e continuamos a usar nossa voz para defender a nova regulamentação nesta área.

Realmente importante, além de nos envolvermos na conversa externa, também temos pensado em como podemos ter certeza de que estamos desenvolvendo o reconhecimento facial e usando-o com os clientes de uma maneira responsável.

Uma das coisas que fizemos foi criar um conjunto de princípios específicos de reconhecimento facial que se baseiam em nossos princípios mais amplos da I.A., mas vão um pouco mais além - para incluir coisas como a importância de garantir que o reconhecimento facial não seja usado de forma discriminatória e a importância do aviso e consentimento quando o reconhecimento facial estiver sendo usado em um ambiente comercial. E, importantemente, quando a tecnologia estiver sendo usada pelo governo ou pelas autoridades legais, que qualquer vigilância seja feita de forma lícita, fundamentada em uma lei relevante.

Outra coisa na qual eu trabalho no reconhecimento facial nos levou à criação de um processo de Nota de Transparência. Então, você pode ver um snapshot da Nota de Transparência na tela aqui. Estes são documentos que criamos para cada um de nossos principais serviços de I.A., que são documentos públicos que compartilhamos com clientes, definindo como o sistema funciona. Mais uma vez, muito importante, definindo as limitações do sistema - e os ambientes em que ele não funciona muito bem - e estabelecendo considerações-chave para os clientes sobre como eles podem pensar em usar a tecnologia de uma maneira responsável. Este fornecimento transparente de informações, nós sentimos, é realmente importante e é parte da responsabilidade do criador de uma tecnologia, como é a Microsoft.

E então, finalmente, continuamos a defender a criação de salvaguardas regulamentares para o reconhecimento facial novamente, com um foco particular no uso pelo governo e pelas autoridades legais, dado o impacto que este uso tem/pode ter sobre as liberdades democráticas e os direitos humanos.

Na verdade, pensamos que houve alguns desenvolvimentos realmente positivos nesta frente nos últimos meses. As pessoas podem ter visto os desenvolvimentos no estado de Washington. Em julho deste ano, [Washington] tornou-se a primeira jurisdição no mundo a desenvolver uma lei em torno do uso do reconhecimento facial pelo governo com base na proteção dos direitos humanos.

E há três pilares muito importantes que pensamos que podem ser a base para uma lei robusta em outros lugares. O primeiro é a exigência de testes independentes dos sistemas de reconhecimento facial, portanto, qualquer fornecedor que queira vender o reconhecimento facial a agentes legais deve incluir uma API que permita que esse serviço seja testado independentemente por qualquer pessoa. Há também uma exigência de que a agência governamental que utiliza a tecnologia revele qualquer reclamação ou denúncia de preconceito ou discriminação em relação ao serviço.

O segundo pilar seria uma série de exigências de transparência e prestação de contas que consideramos realmente importantes. Portanto, antes que os agentes governamentais possam usar o reconhecimento facial, eles têm que desenvolver uma política de responsabilidade, definindo como a tecnologia será usada. Isso inclui informações sobre como a agência testa o serviço em condições operacionais, os resultados desses testes (por exemplo, qual foi o desempenho? Qual foi a taxa de falsas combinações? Que tipo de indivíduos e agrupamentos tiveram esse impacto?). Também definindo informações sobre como a agência treinará seu pessoal para usar o sistema corretamente e assegurar que qualquer decisão seja tomada usando os resultados que são emitidos por um ser humano fornecendo uma revisão humana significativa. Esse relatório de responsabilidade deve ser tornado público, deve ser aberto ao público para um período de comentários e revisão por parte do próprio público.

E então o último pilar da lei do estado de Washington é um conjunto de proteções explícitas para as liberdades civis. Por-

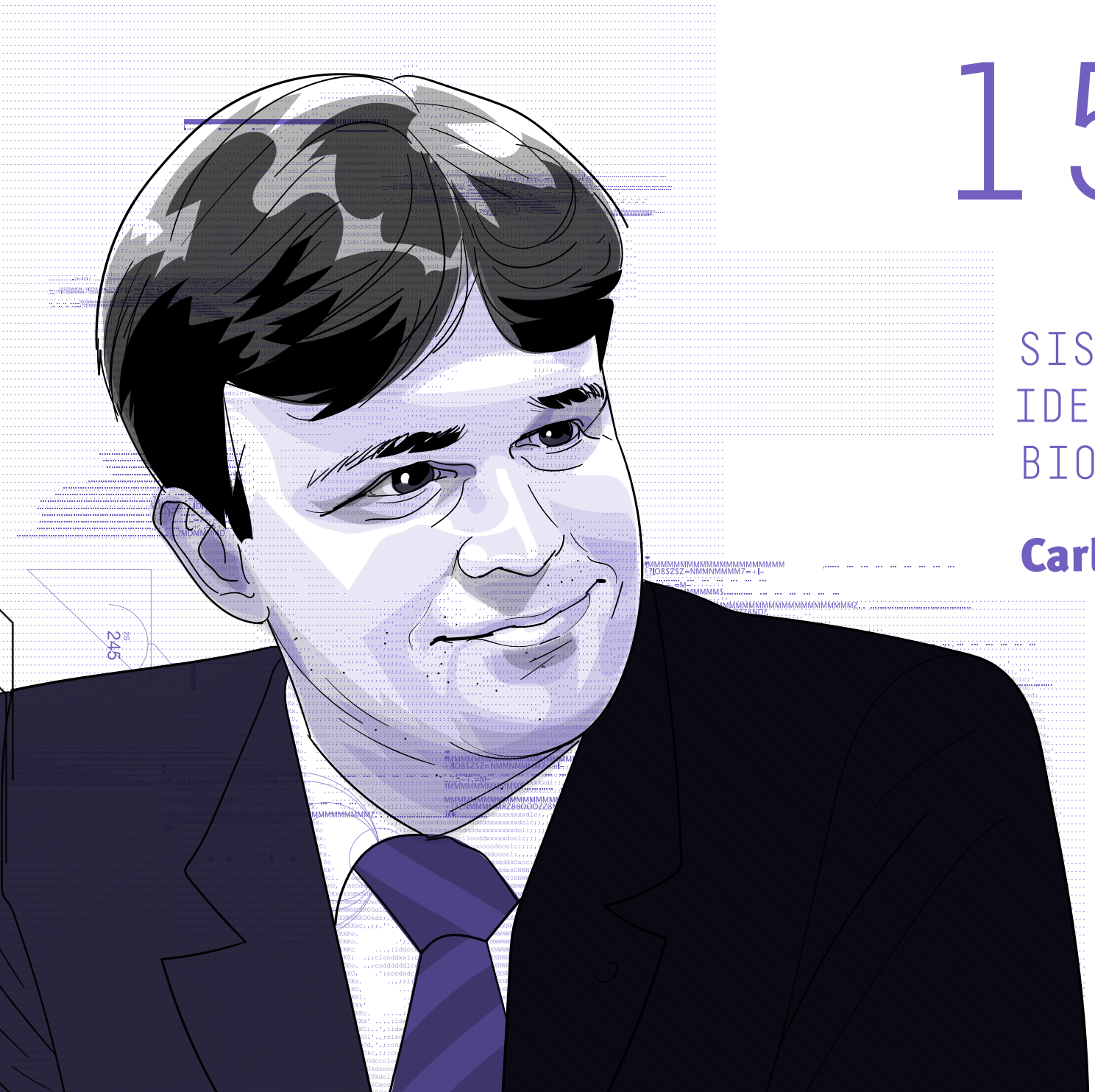
tanto, há uma proibição do uso do reconhecimento facial para rastreamento persistente ou vigilância em massa, a menos que um mandado tenha sido obtido para esse fim específico. Há uma proibição do uso do reconhecimento facial para registrar qualquer indivíduo que exerça seus direitos à liberdade de associação. Há uma proibição do uso da tecnologia para traçar o perfil de qualquer indivíduo com base em qualquer característica pessoal como raça ou raça percebida, idade, sexo, etc. E há também algumas proteções adicionais de liberdades civis em torno do processo de investigação criminal, para que um reconhecimento facial correspondente não possa ser usado como única base para estabelecer a causa provável em uma investigação criminal. Portanto, esta salvaguarda teria significado que o que aconteceu com Robert Williams, do qual falei anteriormente, não teria acontecido, porque o reconhecimento facial naquele caso foi a base para o estabelecimento da justa causa para ação.

Portanto, pensamos que o modelo do estado de Washington fornece uma base realmente sólida, que pode ser construída por outros países para desenvolver leis robustas. Há também algumas partes úteis na proposta de Lei de I.A. da UE, particularmente no artigo 5 (cinco), onde há restrições impostas à aplicação da lei, ao uso de tecnologias de identificação biométrica, incluindo o reconhecimento facial. E há uma exigência ali para garantir que a tecnologia seja usada somente em relação aos crimes mais graves.

Pensamos que esta é uma parte realmente importante da discussão para garantir que o uso da tecnologia seja necessário e proporcional e só seja usado naqueles casos em que haja um benefício proporcional ao uso da tecnologia.

Portanto, espero que esta seja uma visão geral útil sobre como estamos fazendo as coisas na Microsoft e como pensamos sobre a uma maneira de criar uma regulamentação robusta para o uso da tecnologia, que permita que seus benefícios muito reais sejam utilizados, mas de maneira que garanta que isto seja feito de forma responsável e não de maneira que prejudique a democracia e os direitos humanos.

Muito obrigado pelo convite que me fizeram hoje, e estamos realmente ansiosos para continuar a participar da conversa no Brasil em torno das tecnologias I.A. e do reconhecimento facial em geral.



15.

SISTEMAS DE IDENTIFICAÇÃO BIOMÉTRICA[1]

Carlos Bruno Ferreira

1. Texto que tem por base a transcrição da palestra apresentada por Carlos Bruno Ferreira no Painel "Teses: Reconhecimento Facial" no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em 03/09/2021. A transcrição foi revisada pelo autor.

Muito obrigado, Pablo. Bom dia a todos. Queria agradecer a você e à Bárbara pelo convite para estar aqui no InternetLab. Gostaria de saudar inicialmente os meus colegas nessa bancada virtual: Felipe e Isabel, relativamente ao reconhecimento de pessoas, e agora Bianca, Owen e Heloísa relativamente ao reconhecimento facial com o uso de tecnologias.

Pois é, falar depois de alguns colegas apresentarem é sempre um desafio, mas também uma oportunidade. E confesso que me parece que o modo como montei minha apresentação tem muito a ver com as falas do Felipe, da Isabel (que é minha minha colega, pois fui defensor público no Rio de Janeiro também), da Bianca e do Owen.

Tive uma preocupação de pensar como pode ser uma regulação de reconhecimento facial e concordo com a visão da Bianca sobre a questão de vivermos num capitalismo de vigilância. Acho que essa evolução das tecnologias é o modelo que temos de assumir, mas devemos assumi-lo entendendo que elas não são absolutamente neutras, que elas também são capazes de reproduzir as desigualdades que a gente já vem observando na sociedade, principalmente na sociedade brasileira de uma forma histórica, há centenas de anos.

Então, o objetivo da minha apresentação foi, um pouco, pensar nesses problemas, mas também buscar soluções. Assim, já levando em conta que estamos num painel de teses, parto da tese de que o uso das tecnologias de reconhecimento facial no processo penal é inevitável para o eficaz combate à criminalidade. É um avanço que já vem ocorrendo em outros países, e que inevitavelmente vai chegar no Brasil também, mas que necessita de uma regulação específica e restritiva, de forma a impedir injustiças.

Foi, repito, muito boa a apresentação do Owen apontando o caso de uma pessoa em Michigan que foi injustamente condenada por reconhecimento facial. Vou contar também no final da minha apresentação um caso que ocorreu em Lyon, no qual não chegou a haver uma injustiça, mas isso também foi alegado no tribunal.

O racismo é um problema muito grave das tecnologias de reconhecimento facial, e há vários estudos que demonstram como tecnologias de reconhecimento facial são, por diversas razões, mais eficazes em relação a homens brancos do que em relação homens negros - e mais ineficazes ainda em relação a mulheres negras. Além disso, temos também o estabelecimento de uma sociedade de vigilância.

A partir dessa tese inicial, queria trabalhar com vocês nessa proposta de Regulamento Europeu em Inteligência Artificial,[2] que foi apresentada agora em Bruxelas no dia 21 de abril [de 2021] - ou seja, bastante recente - e que está em processo inicial de discussões dentro da União Europeia. Porém, a proposta da Comissão Europeia já dá alguns cenários que demonstram como, também no Brasil, a gente poderia trabalhar essas salvaguardas.

2. Proposta para Regulação da Inteligencia Artificial na União Européia, acessível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

A legislação de proteção de dados brasileira, tema sobre o qual fiz meu doutorado na Universidade de Sevilha com pesquisa no Max Planck de Heidelberg, chegou muito tarde. A discussão europeia já vinha desde a década de 70. A União Europeia já tinha uma diretiva desde 1995, o Regulamento de Proteção de Dados é do meio dos anos 2010. O Brasil só tem uma lei de proteção de dados agora, com a aplicação de sanções a partir de 2021, tendo eficácia a partir de 2020. Então, o Brasil chegou muito atrasado nessa área de proteção de dados. Claro que chegar atrasado permite a nós aproveitar as melhores experiências dos outros países, mas ao mesmo tempo torna difícil a absorção cultural desse modelo de proteção de dados.

Sou também, no Ministério Público Federal, membro do Grupo de Trabalho de Tecnologia da Informação, no qual fazemos um trabalho muito sério de tentar garantir a aplicação da cultura de proteção de dados dentro do cenário do capitalismo, do mercado brasileiro. Estamos envolvidos, por exemplo, na recomendação que foi feita ao WhatsApp sobre a Política de Privacidade. E aqui em Minas Gerais sou Procurador Regional dos Direitos do Cidadão, com enfoque específico na parte de proteção de dados. Tem, inclusive, um procedimento aberto sobre reconhecimento facial, já que o aeroporto de Confins utiliza essa ferramenta, e estamos apurando, entre outros temas de proteção de dados, também a legalidade da atuação da concessionária do aeroporto.

E a primeira coisa que acho uma caracterização importante na legislação europeia é a diferenciação entre as obrigações dos provedores e as dos usuários dessa tecnologia. Foi até importante a presença do Owen, porque há uma diferenciação clara na legislação europeia entre obrigações que envolvem as empresas de tecnologia que vão fornecer reconhecimento facial e outras tecnologias de identificação biométrica - porque o reconhecimento facial, apesar de ser a mais badalada, de ser mais trabalhada, não é a única tecnologia de identificação biométrica. E aí, levando em conta que estamos num congresso de processo penal, naturalmente as forças de segurança, as instituições de *law enforcement* - polícia, Ministério Público - vão ser usuários de sistemas de identificação biométrica à distância. E aí, nisso, já faço essa definição do que chamo de BD, que está lá no artigo 3º desta proposta da União Europeia: são sistemas de identificação biométrica à distância, sistemas de inteligência artificial.

Essa discussão de inteligência artificial já começou no Brasil. O Ministério da Ciência e Tecnologia acabou de divulgar uma política de inteligência artificial que ainda foi conside-

/ MUITAS VEZES NA TECNOLOGIA É IMPORTANTE E FUNDAMENTAL UMA SUPERVISÃO HUMANA PARA EVITAR FALSOS POSITIVOS /

rada pelos especialistas muito rasa, muito básica, mas que evidencia que a gente não precisa, assim como no debate de proteção de dados, chegar tão atrasado. A gente pode começar agora a trabalhar a ideia de uma política de inteligência artificial, e ao mesmo tempo trabalhar dentro do Congresso uma legislação específica de inteligência artificial.

E dentro dessa legislação evidentemente teremos que falar sobre identificação biométrica à distância, que são sistemas de inteligência artificial que verificam, com base em vários dados das pessoas, a capacidade de identificar de forma inequívoca uma pessoa singular à distância. E aí esses dados biométricos que permitem essa identificação envolvem várias características das pessoas. E, ainda mais, não só a identificação através dos detalhes da face, é possível também a identificação biométrica por meio da impressão digital e através da identificação de íris e retina. Então, existe uma multiplicidade de possibilidades de dados biométricos que permitem a identificação inequívoca de uma pessoa, permitindo a identificação biométrica à distância.

E outra definição importante que está na legislação europeia - e que acho importante que venha para o debate brasileiro - é a ideia de que há uma diferenciação entre uma identificação biométrica em tempo real e uma identificação biométrica à distância de maneira diferida - ou seja, uma identificação biométrica à distância que ocorre após a situação naquele momento, que ocorre *a posteriori*.

Outra coisa que também é importante entender que está na legislação europeia, muito bem definida entre os artigos 8º e 15º da proposta de regulação europeia, é que sistemas de inteligência artificial que envolvem identificação biométrica são sistemas com risco elevado. É importante esse termo, - o qual vi o Owen utilizar também na fala dele - é importante a gente falar em risco elevado porque muitas vezes essas tecnologias virtuais parecem não afetar a nossa vida, não afetar a nossa realidade. Parece que, por exemplo, tecnologias de energias e tecnologias que envolvem algum tipo de indústria podem afetar nossa vida física, mas tecnologias virtuais não a afetariam. Mas elas afetam também, e apresentam um risco enorme.

E então, no artigo 8º, e depois do 9º ao 15º, há várias características desses sistemas que têm que ser respeitadas. Muitas que o Owen já falou: transparência e uma boa noção de base de dados - porque isso é o que mais leva à discriminação e a falsos positivos na hora da identificação biométrica -, [e também] haver, antes da implementação da tecnologia, uma boa avaliação de risco inicial, a qual também já está prevista na nossa lei de proteção de dados. É necessário também haver uma supervisão humana, pois se pensa sempre que o envolvimento do humano é prejudicial, mas muitas vezes na tecnologia é importante e fundamental uma supervisão humana para evitar falsos positivos.

Por fim, claro, deve haver segurança de sistemas de informação. Esse sistema de informação sempre deve ser montado de forma que possibilite a sua verificação e também o seu controle quanto às medidas de segurança. Não adianta ter um sistema que em termos de resultados seja bem efetivo, mas que permita com bastante facilidade as ações de *hackers*.

E em relação ao uso para manutenção da ordem pública, que é exatamente o que está no artigo 5º da proposta europeia, há um critério do uso apenas quando estritamente necessário. E esses critérios de proporcionalidade precisam ser melhor avaliados no Brasil. É importante entender que, por exemplo, o uso de informação fora das finalidades, como várias empresas fazem, também deve ocorrer no limite do estritamente necessário, são absolutamente exceção. Então, é preciso haver um juízo muito cauteloso.

Há algumas situações específicas que permitem o uso dos sistemas de BD em tempo real: identificação de vítimas (em especial de crianças), ameaças iminentes e substanciais à vida de pessoas (especialmente em atos de terrorismo) e, fora desses casos, crimes com pena máxima superior a três anos, e [também] nos 32 crimes considerados efetivamente graves listados pela União Europeia. Ou seja, sistemas de identificação biométrica não são para casos menores, casos muito simples de aplicação da lei penal.

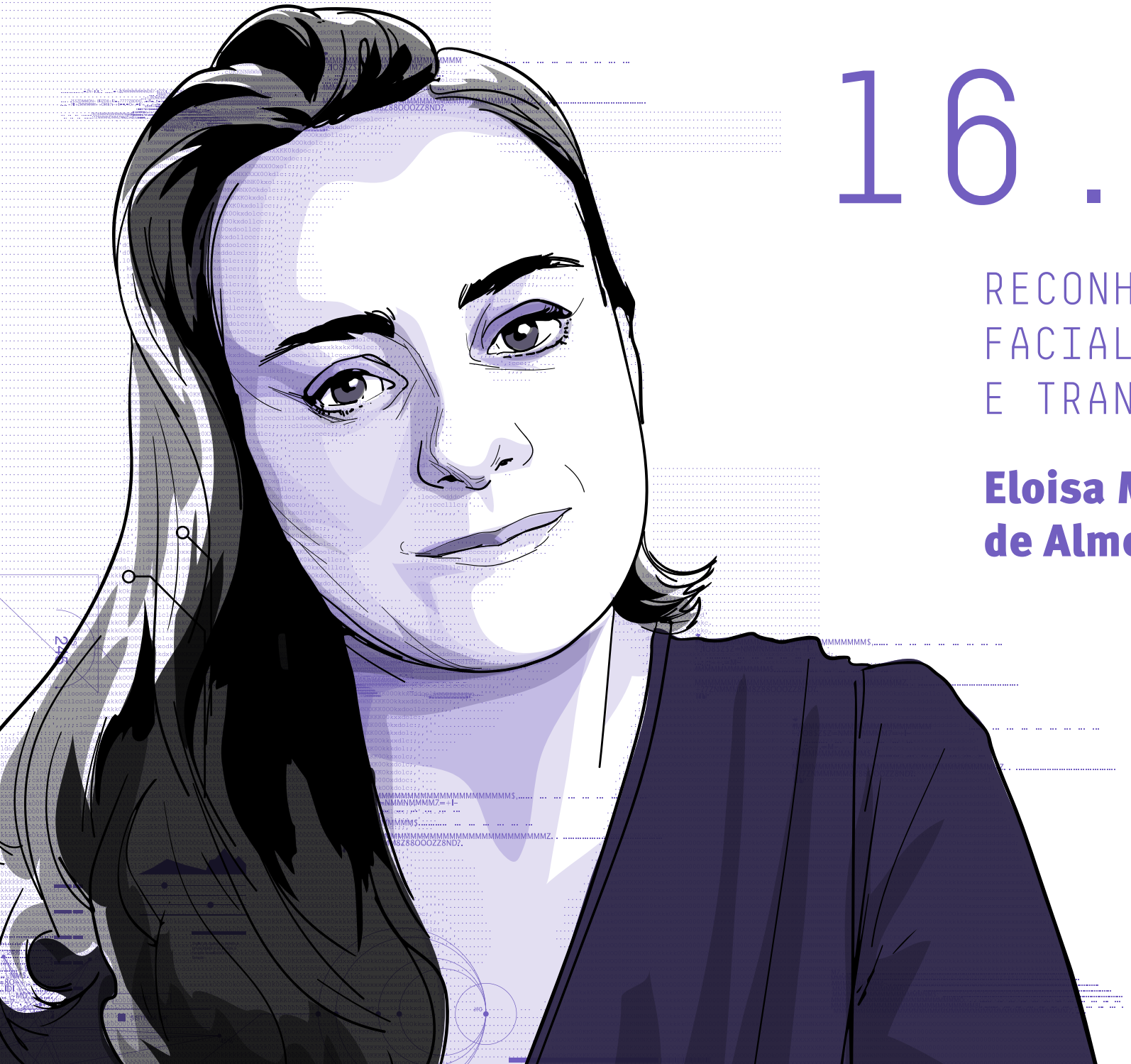
Além disso, deve haver uma análise concreta da gravidade dos fatos e uma limitação geográfica temporal e subjetiva. Não é adequado utilizar sistemas de identificação biométrica à distância para verificações (por exemplo, verificar quem no Rio de Janeiro fez determinada coisa), não funciona assim. Tem de haver fatos concretos, uma análise concreta dos fatos. Ou seja, essas situações vão exigir do Judiciário a concessão de autorizações mediante uma análise muito cuidadosa.

Na União Europeia, o Judiciário ou uma autoridade administrativa independente deverão sempre dar uma autorização prévia, salvo em casos de urgência, quando essa verificação deverá ser feita *a posteriori*. Isso, para sistemas de BD, é uma proposta que ainda vai ser levada a discussão. Muito provavelmente, talvez ao final da discussão, também haja uma regulação para sistemas de BD em tempo diferido e em espaços não abertos ao público. Esse é um sistema que pensa nos espaços abertos ao público e, claro, pensa nisso porque tem uma grande preocupação em não limitar o uso de direitos e liberdades em praça pública - ou seja, não ser utilizado por governos como forma de opressão aos seus indivíduos.

Mas, também para sistemas de BD utilizados em tempo diferido em espaços não abertos ao público, já temos legislação europeia: exatamente o Regulamento Geral de Proteção de Dados no artigo 9º, e a Diretiva 2.016/680 da União Europeia, que é pouco [discutida] no Brasil (e que foi objeto de meu estudo de pós-doutorado na Universidade de Lisboa) e trata especificamente sobre proteção de dados no campo de atuação de polícias e Ministérios Públicos. Não vou poder diferenciar agora regulamento e diretiva, mas o fato é que há um regulamento geral de aplicação imediata pelos países e uma diretiva que tem que ser reproduzida por esses nas suas legislações nacionais. E, nos dois casos, de forma similar ao regulado na nossa Lei Geral de Proteção de Dados, só é permitido o tratamento de dados biométricos com uma noção clara do interesse público que vai permitir essa utilização, e com previsão de garantias afetadas, salvaguarda de direitos e permissão em lei. Então há um cuidado para que não seja banalizado o uso do reconhecimento facial e da identificação de dados biométricos em prol de interesses públicos e interesses estatais.

Ainda, temos como exemplo a primeira condenação que ocorreu em Lyon, na França, relativa a um roubo, em que a defesa alegou a nulidade da condenação exatamente em virtude do reconhecimento facial. Foi até interessante, pois tem a ver com o que o Owen também falou da legislação do estado de Washington nos Estados Unidos, que só foi permitida a condenação nesse caso porque a promotoria de Lyon comprovou que o reconhecimento facial era apenas um dos fatores que levavam à condenação. Havia outros elementos de prova que permitiam também a condenação daquele assaltante.

Com isso, agradeço enormemente a oportunidade do InternetLab nessa fala. Acho que é um debate atualíssimo e importantíssimo no Brasil, e realmente agradeço muito a minha presença nessa bancada virtual. Muito obrigado.



16.

RECONHECIMENTO FACIAL, VIGILÂNCIA E TRANSPARÊNCIA[1]

Eloisa Machado de Almeida

1. Texto que tem por base a transcrição da palestra apresentada por Eloísa Machado de Almeida no Painel "Teses: Reconhecimento Facial" no V Congresso Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em 03/09/2021. A transcrição foi revisada pela autora.

Muito obrigada pela apresentação e pela oportunidade de dialogar com exposições tão completas, interessantes e também díspares. Acho que a gente tem pontos aqui de concordância e consideráveis divergências, também, em relação a essa apresentação. Muito prazer, Carlos, Bianca. É um prazer dialogar com vocês nessa bancada digital. Agradeço ao convite do InternetLab, [por] mais um ano para poder falar um pouquinho sobre esses temas e como é possível incorporar a ideia de proteção de dados pessoais diante de tecnologias de reconhecimento facial no atual contexto de conjuntura brasileira.

Eu não vou tratar do reconhecimento facial eventualmente utilizado para aquelas pessoas que já sofreram uma condenação e, portanto, para as quais juridicamente se cogita a flexibilização, através do devido processo legal, de algumas de suas garantias e direitos fundamentais, inclusive de seus dados pessoais.[2] Eu vou tratar aqui do uso de reconhecimento facial em relação à persecução penal genérica e sobre como ele tem sido usado no Brasil, de maneira aleatória, massiva e absolutamente invasiva em relação a todas as pessoas.

Estou falando do reconhecimento facial que vem com uma justificativa genérica (ex.: de encontrar crianças desaparecidas ou de tornar a persecução penal mais eficiente). Quem pode ser contra isso, não é? Quem pode ser contra que crianças desaparecidas sejam encontradas? Porém, essas são justificativas que não se sustentam na prática, e que têm sido usadas como elementos de afronta massiva a direitos da população. Além do que, é importante destacar que o reconhecimento facial não é neutro. Não podemos, de forma alguma, na aplicação dessa tecnologia, falar em qualquer tipo de pretensão de normalidade da norma ou da tecnologia ou das instituições de aplicação da lei diante do viés da persecução penal no Brasil. O viés tem que ser um pressuposto do debate, baseado em evidências, de como funciona o nosso sistema de justiça criminal.

Tratarei, ao longo da minha fala, de exemplos como o que tem acontecido na cidade de Salvador, ou aqui no metrô de São Paulo, casos que eu estou mais ou menos envolvida diretamente, seja como advogada, seja como pesquisadora, para relatar quais são os desafios que eu consigo mapear na implementação das tecnologias de reconhecimento facial para persecução penal no Brasil.

Vou abordar mitos que precisam ser enfrentados, a falta de transparência nos contratos de uso de reconhecimento facial no país e as exceções à proteção de dados. Por fim, vou apontar alguns cenários para superar esses obstáculos.

CONTESTANDO OS MITOS DA TECNOLOGIA

A primeira grande dificuldade que a gente tem é de fazer uma afronta a mitos envolvendo o uso de tecnologia de reconhecimento facial: o mito da eficiência, o mito de que o uso da tecnologia trará uma maior segurança à aplicação da lei penal - o que, portanto, justificaria uma grande invasão em direitos de privacidade de todas as pessoas. Estou falando de câmeras de reconhecimento facial, usadas nas ruas de Salvador, ali no Pelourinho. Estou falando de uma tecnologia de reconhecimento facial aplicada, por exemplo, no metrô de São Paulo. Não estou falando, especificamente, de reconhecimento facial

2. Importante ressaltar que mesmo para estes casos o Supremo Tribunal Federal tem impedido a violação de dados pessoais em ações relativas à criação de "cadastros de condenados". Em medida cautelar na ação direta de inconstitucionalidade ADI 6561 MC, o ministro Edson Fachin suspendeu leu do estado de Tocantins que criava cadastro de usuários de drogas pois "[...] seletividade social do cadastro é incompatível com o Estado de Direito e os direitos fundamentais que a Constituição de 1988 protege, especialmente, a igualdade (CRFB, art. 5º, caput), a dignidade da pessoa humana (CRFB, art. 1º, III), o direito à intimidade e à vida privada (CRFB, art. 5º, X) e o devido processo legal (CRFB, art. 5º, LIV). Inexistência tampouco de protocolo claro de proteção e tratamento desses dados". Na ADI 6620, de relatoria do ministro Alexandre de Moraes, é questionada lei do estado do Mato Grosso que cria "cadastro de pedófilos"; o julgamento está suspendo por pedido de vistas.

voltado para as pessoas com uma justa causa para a atuação da persecução penal, que terão seus dados flexibilizados, mas da aplicação massiva e indiscriminada dessa tecnologia.

Sabemos que, no atual estado do desenvolvimento do reconhecimento facial, falsos positivos são uma condição inerente dessa tecnologia, pela definição do limiar do reconhecimento ou não, por aproximação e probabilidades. Isso está dado, isso é objetivo, isso é científico. O falso positivo faz parte do atual estado dessa tecnologia, pela aproximação ou distanciamento, a partir de um banco de dados - e já existe toda uma literatura para discutir o seu [possível] enviesamento. Mas, independentemente do enviesamento do banco de dados, [o reconhecimento facial] é uma tecnologia que tem o falso positivo como um elemento constitutivo. E que, aplicado massivamente, se torna estatisticamente inviável. A quantidade de erros será muito maior do que a quantidade de acertos para localizar poucas pessoas dentre uma multidão, milhares de pessoas - ou milhões, falando no caso do Metrô de São Paulo.

Então, feitas essas considerações preliminares, que são importantes de serem ressaltadas sobre o atual estado da tecnologia, quais são os desafios específicos que se impõem ao sistema de justiça [brasileiro]. Primeiro, o espaço e a prática dos tribunais. Nós estamos falando de um sistema seletivo; nós estamos falando de um sistema que não estabeleceu ou construiu fortes exigências de prova para condenação de pessoas; estamos falando de um sistema que está amplamente baseado, por exemplo, única e exclusivamente na palavra policial para condenar milhares de pessoas e, não de maneira coincidente, pessoas negras.

Então nós temos uma baixa exigência do nosso sistema de justiça, no que se refere à produção de provas para condenar alguém. E não há nada, infelizmente, absolutamente nada, que nos indique que o uso do reconhecimento facial se dará

/ O FALSO POSITIVO FAZ PARTE DO ATUAL ESTADO DESSA TECNOLOGIA, PELA APROXIMAÇÃO OU DISTANCIAMENTO, A PARTIR DE UM BANCO DE DADOS /

/ EM RAZÃO DESSES ARGUMENTOS, NÃO HÁ OUTRA OPÇÃO HOJE, [...] QUE NÃO O BANIMENTO DE QUALQUER RECONHECIMENTO FACIAL QUE SE PRETENDA NO BRASIL /

na contramão de um sistema que já é seletivo e é frágil em relação às garantias processuais penais. E aqui estou falando desde o filtro inicial do sistema de justiça criminal da polícia até as nossas cortes superiores. A gente está falando aqui de racismo estrutural e, portanto, presente na formulação do direito, na interpretação e na aplicação do direito também. E aí, queria parabenizar especialmente a fala da Bianca, que foi extraordinária aqui nesse painel.

FALTA DE TRANSPARÊNCIA

A segunda dificuldade que a gente tem nesses casos concretos é de fazer uma argumentação jurídica baseada em evidências para contestar o uso das tecnologias de reconhecimento facial, porque muitas vezes essas evidências estão escondidas, porque os contratos não são públicos, porque as informações sobre a segurança dos bancos não estão abertas, porque não há nenhum tipo de transparência sobre a contratação dessas tecnologias a ponto de exigir de organizações que atuem especificamente nesse tema, isto é, recorrer a litígios específicos apenas para ter acesso aos documentos que se referem à implementação dessa tecnologia. Então o cenário de hoje é de bloqueio absoluto no que se refere à *accountability*,[3] transparência, publicidade e escrutínio público.

3. Termo inglês, em tradução livre, correspondente a "responsabilidade".

E isto se dá de maneira custosa para as organizações da sociedade civil. No caso do Metrô de São Paulo, a gente precisou entrar com uma ação só para produzir provas. "Tem relatório de impacto?". A resposta foi: "não". "Qual banco de dados você vai fazer?". "Não vou te contar se vou fazer, se eu vou guardar dados pessoais, se eu não vou guardar, quem vai mexer, não vou contar nada". Então, o cenário em que a gente está hoje é um cenário muito complicado. No caso de Salvador,

na Bahia, não há um contrato público. O contrato que hoje rege a tecnologia de reconhecimento facial na Secretaria de Segurança Pública do Estado da Bahia não está [publicizado], ninguém sabe como funciona. De ouvir dizer, sabe-se que é um aditivo de um contrato de 2014, por ocasião da Copa do Mundo no Brasil, e que ninguém sabe, ninguém viu, ninguém sabe as cláusulas, ninguém sabe quanto custou, ninguém sabe o que é feito com os dados. Nada.

A EXCEÇÃO DA LGPD

Eu já falei da dificuldade de construir um Direito baseado em evidências sem que haja transparência no uso da tecnologia de reconhecimento facial e também das dificuldades do litígio no espaço do tribunal - que não é um espaço, vamos dizer, garantista para lidar com este tema. O terceiro desafio que eu trago é que a exceção da LGPD está se transformando em regra. A LGPD traz uma exceção para a segurança pública em relação à proteção dos dados pessoais. Especificamente porque, no processo de persecução penal, e em razão do processo, que se pressupõe "devido", [é possível] atingir direitos e garantias fundamentais. Mas, agora, as câmeras do Metrô de São Paulo são justificadas pelo quê? "Por uma questão de segurança, vai ficar mais seguro". Mas o metrô não é um órgão de segurança. Não há problemas específicos de segurança a serem abordados [no metrô] além do [próprio] metrô.

O que se percebe é que a justificativa baseada na excepcionalidade da segurança pública está servindo para a implementação de reconhecimento facial em massa no Brasil, nas ruas, nos meios de transporte, supostamente sob a guarida dessa exceção trazida pela LGPD e que ainda não tem a devida regulamentação[4]. A gente deveria ter um regramento absolutamente estrito sobre as hipóteses de possibilidade de aplicação dessa tecnologia, mas não é isso o que acontece.

A vaga ideia de segurança e o super-trunfo do argumento-mito de que essa tecnologia vai ser capaz de encontrar as crianças desaparecidas e que vai tornar a persecução penal mais eficiente, acaba com qualquer possibilidade de debate público com suficiente escrutínio sobre a pertinência ou não dessa tecnologia, ainda que a gente saiba todas as dificuldades de eficiência mínima dessa tecnologia em relação a crianças desaparecidas - justamente em razão do transcurso do tempo para identificação (mudança das feições), e da nossa legislação garantista em relação a crianças e adolescentes (muito diferente, por exemplo, da legislação que [existe] nos Estados Unidos). Então, teoricamente, como [poderíamos] fazer o reconhecimento facial de crianças desaparecidas? Além de pouco eficiente, isso já seria vedado pela legislação que nós temos hoje. Já seria impossível. Mas, ainda assim, é o argumento usado para implementação de tecnologias de reconhecimento facial massivas nas cidades brasileiras.

4. Segundo o art. 4º, §1 da LGPD, "O tratamento de dados pessoais previsto no inciso III [referente a segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais] será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei."

CENÁRIO ATUAL E SOLUÇÃO

E, por fim: essa não é uma discussão que se dá descolada do contexto. E qual é o contexto que nós estamos hoje? Nós estamos vivendo sob um governo que pode ser classificado de militar-civil, dada a extensão de militares nos cargos de comando, seja dentro do governo, seja nas empresas públicas ou nas instâncias de segurança. Nós estamos diante de um governo com fortes características autocratas, com descompromisso

em relação à Constituição. E nós estamos vivendo um governo de caráter populista, que escolhe, dentre a sua própria população, inimigos que não devem ser considerados brasileiros e merecedores de igual respeito e consideração(por exemplo, os povos indígenas, os negros, os pobres, os trabalhadores, os opositores, ou qualquer um que não entre na ideia de nação brasileira que preencha a cabeça do presidente Jair Bolsonaro).

Em razão desses argumentos, não há outra opção hoje, seja pelo estado da tecnologia, seja pelo desenvolvimento de nosso sistema de justiça, seja pela jurisprudência e pelos requisitos legais, neste contexto político, que não o banimento de qualquer reconhecimento facial que se pretenda no Brasil. Eu sei que é uma posição, vamos dizer assim, um pouquinho mais extrema, que eu trago aqui para esse painel - mas eu faço questão de firmar. O argumento do banimento é baseado em evidências, baseado na história das nossas instituições jurídicas e o único capaz de nos prevenir de um estado de vigilância massiva, que transforme essa sociedade em sabe-se lá o que nos próximos anos. Muito obrigada.

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.