

TRATAMENTO DE DADOS PESSOAIS EM INVESTIGAÇÕES CRIMINAIS: O DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMATIVA COMO LIMITE CONSTITUCIONAL

PERSONAL DATA PROCESSED FOR CRIMINAL INVESTIGATION MATTERS: THE FUNDAMENTAL RIGHT OF INFORMATIONAL SELF-DETERMINATION LAW AS CONSTITUTIONAL LIMIT

ANDRÉ DA ROCHA FERREIRA

Mestre em Ciências Criminais pelo Programa de Ciências Criminais da PUC-RS (2017). Pesquisador no projeto de pesquisa: "A recepção da criminologia crítica na América Latina: um estudo histórico acerca da sua influência no pensamento social e político-criminal em tempos de Estado de Exceção", do Programa de Ciências Criminais da PUC-RS.

Lattes: [<http://lattes.cnpq.br/6101770805111941>].

ORCID: [<https://orcid.org/0000-0002-8509-9366>].

andredarochaferreira@gmail.com

Recebido em: 30.03.2021

Aprovado em: 03.05.2021

Última versão do autor: 18.06.2021

ÁREAS DO DIREITO: Penal; Constitucional; Digital

RESUMO: Quais são limites jurídicos para que agências de segurança possam tratar dados pessoais em investigações criminais? A partir desse problema, o artigo objetiva entender se o direito brasileiro já impõe, no âmbito penal, limites ao uso de dados pessoais em investigações e, caso positivo, quais seriam esses limites. A metodologia escolhida foi hipotético-dedutiva. Para tanto, inicia com uma contextualização geral acerca do problema. Propõe, após, um debate a existência de um conceito para "dado pessoal", bem como de que modo é aplicado no sistema de justiça criminal. Em seguida, realiza breve revisão bibliográfica sobre os riscos associados ao tratamento massivo de dados por agências de segurança. Defende que, a partir do julgamento

ABSTRACT: What are the legal limits for security agencies to process personal data in ongoing criminal investigations? This paper aims to understand whether Brazilian criminal justice law already imposes limits on personal data use in investigations, and If so, what those limits would be. This work adopts a hypothetical-deductive methodology starting with a general contextualization of the problem. Afterwards, it proposes a debate on the existence of a concept for "personal data" and its application in the Brazilian criminal justice system. A brief bibliographic review displays the risks associated with the massive data gathering by security agencies. In the judgment of the IBGE case (ADI 6,387), this work argues that the Brazilian Supreme Court

da ADI 6.387 (caso IBGE), o STF reconhece o direito fundamental à autodeterminação informativa, sendo esse o limite que deve ser enfrentado pelo interesse público da persecução penal. Para dar sentido ao termo, nos valem os princípios presentes no art. 6º da LGPD, entendendo-os como a dimensão objetiva da autodeterminação informativa.

PALAVRAS-CHAVE: Sistema de justiça criminal – Investigações criminais – Proteção de dados – Autodeterminação informativa.

recognizes the fundamental right to informational self-determination, which is the limit that the public interest in a criminal prosecution must face. To define this fundamental right's meaning, this paper proposes applying the charter of principles present in the art. 6 of the Brazilian Data Protection Regulation (LGPD), understanding those principles as a part of informative self-determination.

KEYWORDS: Criminal justice system – Criminal investigations – Data protection – Informational self-determination.

SUMÁRIO: 1. Introdução. 2. Formulando o problema: o como, o porquê e o quando do uso de dados nas investigações criminais brasileiras. 2.1. O como e o porquê do uso de dados em investigações criminais. 2.2. O quando: a legalidade do uso de dados em investigações criminais. 3. O que é um dado, afinal? Os conceitos expansionista e reducionista de dado pessoal e sua aplicação no direito penal brasileiro. 3.1. Dado pessoal: um conceito jurídico. 3.2. A aplicação de um conceito restritivo de dado pessoal e a proteção dos metadados no direito penal brasileiro: exemplos da ADI 4.739 e do PL 2630/2020. 3.3. Resultados parciais. 4. Compartilhamento de dados pessoais em investigações criminais: o risco da vigilância permanente e a proteção constitucional do devido processo informacional e do direito à autodeterminação informacional. 4.1. Uma dimensão do problema: o risco da vigilância a partir de dados pessoais. 4.2. O direito fundamental à autodeterminação informativa dos dados enquanto barreira constitucional à utilização de dados em matéria penal. 5. Considerações finais. 6. Referências bibliográficas. 6.1. Jurisprudência. 6.2. Legislação.

1. INTRODUÇÃO

Recentemente, o Superior Tribunal de Justiça determinou que a empresa de tecnologia *Google* entregasse às agências de segurança responsáveis pela investigação do assassinato da vereadora Marielle Franco e de Anderson Gomes os endereços de IP (*Internet Protocol*) dos usuários que tivessem pesquisado uma lista de palavras-chave relacionadas à vereadora. O objetivo da medida é ajudar na identificação dos possíveis autores do crime. Ainda que a medida venha a ser efetiva, tem um importante *trade-off*: usuários, sem qualquer relação com o caso, terão dados pessoais entregues para o escrutínio de agências de segurança. Pela complexidade e relevância do caso, a decisão pela medida invasiva pode se justificar; no entanto, a extensiva aplicabilidade desse método investigativo gera o grave risco de ferimento a princípios constitucionais.

Apresenta-se, portanto, o seguinte problema de pesquisa: quais os limites jurídicos para o tratamento de dados pessoais por agências de segurança em investigações

criminais? Por limite jurídico, compreende-se a ideia de que a decisão sobre a legalidade de um determinado ato deve passar por uma análise de permissibilidade normativa, ou seja, se ele é aceitável, ou não, dentro do sistema jurídico (LORENZETTI, 2009). O conceito de dados pessoais será tratado em ponto específico, mas, de modo amplo, entende-se que dados são “fatos conhecidos que podem ser registrados e possuem significado implícito” (ELMASRI; NAVATHE, 2011, p. 3); um dado se torna pessoal quando por meio dele é possível a identificação de uma pessoa natural.

A quantidade de dados pessoais coletados e as tecnologias de processamento a eles associadas (de inteligência artificial, por exemplo) têm o potencial de trazer um impacto positivo em diversos aspectos de nossa sociedade, inclusive na resolução de graves delitos. A adoção de uma postura radical, ou seja, absolutamente contrária à utilização de dados pessoais em investigações, mostra-se inefetiva do ponto de vista da complexidade dos problemas que se apresentam. Em que pese os benefícios trazidos pela tecnologia, é importante ressaltar que a ausência de mecanismos eficientes de proteção desses dados e da privacidade já demonstrou resultados bastante preocupantes, o que ocasionou um movimento de regulamentação da matéria a nível internacional. O Brasil já conta com uma série de atos normativos de proteção dos dados pessoais, nenhum, no entanto, é específico para questões criminais. O mais recente passo nessa direção foi a apresentação do anteprojeto sobre uso de dados na segurança pública.

Em outras situações, como a do compartilhamento de dados pessoais para fins de aplicação de uma política pública, por exemplo, a Lei Geral de Proteção de Dados (LGPD) traz eficientes mecanismos de proteção dos dados e da intimidade dos cidadãos. Recentemente, foi criada a Agência Nacional de Proteção de Dados (ANPD), sendo a agência reguladora da matéria. No entanto, a LGPD faz uma exclusão de sua aplicação em seu art. 4º, inc. III, não sendo utilizada para resolução de questões criminais.

Conta-se, ainda, com o Marco Civil da Internet (MCI), o qual fornece uma série de regras mais amplas para a regulamentação da Internet. No entanto, para o caso de investigações criminais, o seu ponto mais importante é o de determinar que a retenção de dados de navegação e telecomunicação dos usuários. No que diz respeito ao problema desse artigo, os limites jurídicos para utilização de dados pessoais em investigações, a legislação não é clara; determinando, contudo, que é necessária decisão judicial para a entrega de dados pessoais em investigações criminais. Assim, temos uma dimensão do problema: o Brasil conta com uma série de bancos de dados, públicos ou privados, que já estão à disposição das agências de segurança para o uso em investigações criminais. Afinal, qual o limite do uso desses dados?

A hipótese que se traz aqui é de que, apesar de não contar com uma legislação protetiva específica, o Brasil já conta com um conjunto de normas (regras e princípios) que submete limites ao processo de tratamento de dados pelo poder punitivo estatal. Mais: esses limites são o alicerce em que se deve assentar a legislação que se avizinha. O objetivo do artigo é, portanto, realizar um panorama geral desse arcabouço normativo, apontando caminhos para determinar esses limites.

Para tanto, teve-se por adotar uma metodologia hipotético-dedutiva, em que esse mapeamento será feito a partir de um estudo das questões constitucionais e infraconstitucionais relevantes para o tema. Faremos, dessa maneira, uma revisão bibliográfica e uma análise legislativa, bem como uma análise qualitativa de relevantes precedentes dos tribunais superiores.

No segundo ponto do trabalho, trataremos de apresentar uma contextualização geral do problema proposto. Após, apresentaremos um conceito jurídico de dado pessoal, bem como discutiremos sua utilização na justiça criminal. No quarto ponto, avançaremos para os aspectos constitucionais, abordando a questão a partir dos conceitos de devido processo informacional e do direito de autodeterminação informativa¹.

2. FORMULANDO O PROBLEMA: O COMO, O PORQUÊ E O QUANDO DO USO DE DADOS NAS INVESTIGAÇÕES CRIMINAIS BRASILEIRAS

Antes de respondermos ao problema central do problema de maneira detalhada, parece-nos adequado a realização de uma melhor contextualização do tema que se apresenta a partir de uma sucinta resposta a três perguntas: de que modo situações de tratamento de dados pessoais ocorrem? (como); qual a importância delas em investigações criminais? (o porquê); e, quais os requisitos para que ocorra o tratamento? (quando).

2.1. O como e o porquê do uso de dados em investigações criminais

A próxima opção de música, as fotos que veremos primeiro na rede social, os produtos que mais combinam com o nosso gosto: nossa vida tem sido marcada por decisões, importantes ou não, tomadas pela inteligência artificial, os já famosos “algoritmos”, redes neurais, ou aprendizado de máquina (*machine learning*)². A partir da coleta e subsequente análise de imensas quantidades de dados, combinado com estratégias e algoritmos inovadores tais sistemas alcançam novos patamares de inteligência e capacidade decisória, uma habilidade antes restrita aos seres humanos.

1. Na literatura especializada, há registros do termo “autodeterminação informativa” ou, ainda, “autodeterminação informacional”. Optou-se pelo primeiro, pois esse o utilizado nas legislações atinentes à matéria, bem como na decisão que serve de paradigma para o presente artigo.
2. “Um algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer. Os computadores são compostos por bilhões de minúsculas chaves chamadas transistores, e os algoritmos ligam e desligam essas chaves bilhões de vezes por segundo. O algoritmo mais simples é: gire a chave. O estado de um transistor contém um único bit de informação: um, se o transistor estiver ativado, e zero, se estiver desativado. Um único bit em algum local dos computadores de um banco informa se nossa conta tem ou não saldo. Outro bit dos computadores da administração da previdência social informa se estamos vivos ou mortos. O segundo algoritmo mais simples é: combine dois bits”. (DOMINGOS, 2015, p. 21).

A ciência da computação já debate, há muito, a capacidade que esses sistemas poderiam alcançar em termos de tomadas de decisão, bem como os riscos que o uso dessa tecnologia poderia acarretar (WEISENBAUM, 1976). De qualquer modo, a partir do desenvolvimento de algoritmos que conseguem tomar decisões automaticamente e aprender com essas decisões, é que tivemos uma virada tecnológica que toma conta de quase todo nosso cotidiano.

Para aprender e tomar melhores decisões, esses algoritmos precisam ser alimentados com imensos bancos de dados (*input*), em que, a partir da identificação de padrões, são capazes de prever as probabilidades mais prováveis (*output*) para determinadas situações. Assim funcionam as chamadas redes neurais, desenvolvidas à semelhança de como se dá o processo de pensamento humano, essas redes têm a capacidade de agrupar, classificar e aprender a partir de dados.

Normalmente, esses algoritmos se utilizam de interações do usuário na internet (*sites* de pesquisa, redes sociais, ou qualquer outro serviço na internet). Essa captura ocorre em vários níveis, desde o fornecedor da internet (a operadora de telecomunicação) até o serviço fim (e.g., *Facebook*, *Spotify*). Por exemplo, companhias de telecomunicação rastreiam os sites acessados pelo cliente (*DNS server*). São essas ações que criam perfis de consumo individualizados, conseguem determinar preferências por determinados esportes ou *hobbies*, conseguem prever como terminaremos uma frase, enfim, tomam decisões.

Assim, para o melhor funcionamento dos algoritmos, é necessária uma quantidade imensa de dados, fazendo com que o aprendizado e as respostas da máquina sejam melhores, fornecendo decisões que podem auxiliar muito em nossas vidas, por exemplo, na realização de políticas públicas. Com o crescimento exponencial do uso de aparelhos eletrônicos e da internet, as condições ideais para a propagação dessas tecnologias se fizeram presentes: todos os aplicativos, sites, entre outros serviços que fazem parte de nossa rotina, coletam dados. A dimensão é tão grande que há autores, como veremos em ponto específico, que defendem uma mudança de estágio no capitalismo, sendo a coleta de dados o centro do debate.

Como costumeiramente ocorre na história do poder punitivo, a tecnologia trouxe reflexos para a questão criminal: constata-se um aumento de cibercrimes no país, fenômeno que se expandiu ainda mais com a pandemia, são cada vez mais comuns notícias a respeito de grandes vazamentos de dados³ ou de estelionatos praticados pela internet⁴.

3. Recentemente, houve um vazamento de dados pessoais de 220 milhões de pessoas, sendo o maior incidente de segurança do país. Pelas características dos dados vazados, especula-se que tenham origem no banco de dados da instituição de proteção ao crédito SERASA, o que ainda não restou confirmado. (SOUZA, 2021).
4. Recentemente, entrou em vigor a Lei 14.155, cujo objetivo é “tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet”. O recrudescimento da pena para crimes cibernéticos é uma resposta ao aumento de

Assim como qualquer outra atividade de nossa vida, parece-nos que, em algum momento, o *iter criminis* passará pela internet, deixando, assim, informações de conexão. Seja na consumação (crimes praticados pela internet) ou nos atos preparatórios (como o assassino que pesquisa na internet sobre a arma do crime), é muito difícil que um crime não deixe uma pegada digital.

Por essa razão, o tratamento desses dados coletados é cada vez mais importante nas investigações criminais, tendo sido decisiva na solução de diversos crimes: rastreamento da localização de criminosos 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 resolução de crimes. Inegavelmente, portanto, há um interesse público para que a persecução penal tenha acesso a essa nova tecnologia (inclusive, para fornecer uma resposta penal adequada e atual).

Para garantir o acesso das agências de segurança a essas informações, o Brasil conta com ampla legislação determinando que provedores de conexão e aplicações da internet guardem os registros das conexões, notadamente o Marco Civil da Internet, em seus artigos 13 e 15⁵ e a Lei de Organizações Criminosas em seu art. 17⁶. Assim também a Lei de Lavagem de Dinheiro que, em seu art. 10⁷, determina a manutenção de dados cadastrais e financeiros pelas instituições a que se refere a Lei em seu art. 9º. Aliada à essas legislações, uma série de outros atos normativos faz com que as investigações criminais no Brasil tenham, à disposição, um imenso banco de informações e registros dos seus cidadãos (além, é claro, daqueles que o próprio Estado coleta⁸). Um mapeamento completo

estelionatos nas redes sociais (crime de fraude eletrônica) e de casos de *ransomware* (com especial atenção aos órgãos da administração pública).

5. Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (...) Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (BRASIL, 2014).
6. Art. 17. As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no art. 15, registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais. (BRASIL, 2013).
7. Art. 10. As pessoas referidas no art. 9º: I – identificarão seus clientes e manterão cadastro atualizado, nos termos de instruções emanadas das autoridades competentes; II – manterão registro de toda transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar limite fixado pela autoridade competente e nos termos de instruções por esta expedidas; (BRASIL, 1998).
8. São muitos os exemplos de bancos de dados da administração pública que têm relevância para fins penais e que dão dimensão da atualidade do problema, sendo alguns exemplos: Cadastro Base do Cidadão, regulamento pelo Decreto 10.046/2019, que prevê o compartilhamento de dados na

da situação, já foi realizado por Abreu e Antonialli (2017). Na publicação, se constata o aumento de requisições das autoridades de segurança para ter acesso a esses dados (ABREU e ANTONIALLI, 2017).

2.2. *O quando: a legalidade do uso de dados em investigações criminais*

Após breve apresentação da importância dos dados para investigações criminais, bem como do acervo disponível para agências de segurança, adentramos naquele que é o problema central do artigo: em quais situações é legal que sejam tratados esses dados? A operação de tratamento de dados envolve a coleta, produção, recepção, classificação, enfim, uma série de atividades que constituem ações que podem ser necessárias para investigações criminais, estando sujeitas aos limites constitucionais.

Necessário, para fins de apresentação do problema, entender que se trata de questão complexa, com diversos entendimentos; o debate está em construção e constante movimento, justamente pela velocidade e importância que o tema suscita. Tentaremos, nesse ponto, apontar alguns contornos que já se apresentam.

Parte-se de um ponto de partida: a proteção constitucional da inviolabilidade da correspondência, dos dados e das comunicações, prevista pelo art. 5º, inc. XIIº, da Constituição Federal. A partir desse limite constitucional ao poder punitivo, foi editada, por exemplo, a Lei de Interceptações Telefônicas (LIT), a qual traça os limites para a permissão de ações de escuta telefônica.

Para decisões que quebram o sigilo dos dados, não há uma legislação correlata para regulamentar especificamente a matéria. Sobre essa questão, os tribunais pátrios têm entendido que o âmbito de proteção constitucional a dados não é o mesmo dado às comunicações, não aplicando, portanto, os requisitos da LIT¹⁰.

Isso porque o entendimento dominante na jurisprudência brasileira é de que a proteção constitucional prevista pelo art. 5º, inc. XII, diz respeito ao fluxo da comunicação, não ao dado propriamente dito:

administração pública; o Sistema Nacional de Estatística de Segurança Pública (Sinesp); o Banco Nacional Multibiométrico e de Impressões Digitais; o Banco Nacional de Perfis Genéticos; e, ainda, o Banco Nacional de Perfis Balísticos, entre outros bancos de dados (existentes e futuros), cujo objetivo é o tratamento de dados pessoais para fins criminais.

9. XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (BRASIL, 1988).
10. A jurisprudência entende majoritariamente que “[n]ão se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados” (STF, HC 91.867/PA, rel. DJe 20/9/2012).

“O alcance da proteção constitucional conferida a comunicações em fluxo e a dados armazenados é tema controverso. Atualmente, a interpretação dominante, reafirmada em decisões paradigmáticas do STJ e do STF, entende que o inciso XII da Constituição Federal garantiria apenas o sigilo das comunicações *em fluxo*, não se estendendo às comunicações armazenadas. Em paralelo, a Lei das Interceptações regulamenta as hipóteses de quebra desse sigilo. Assim, enquanto a interceptação das comunicações em fluxo, que permite o acesso a uma quantidade temporalmente limitada de informações, tem suas hipóteses e requisitos estritamente regulamentados pela Lei de Interceptações, o mesmo não acontece com o acesso a dados armazenados, cuja proteção se limita à exigência de ordem judicial, sem requisitos delimitados, por força do art. 7º, inciso III, da Lei 12.965 (Marco Civil da Internet).” (ANTONIALLI; FRAGOSO; MASSARO, p. 22, 2019).

Essa compreensão, já bastante delineada pela doutrina, sendo ainda a que vigora na jurisprudência, tem origem em artigo de Tércio Sampaio Ferraz Júnior, “Sigilo de dados: o direito à privacidade e os limites a função fiscalizadora do Estado”:

“Visto deste ângulo, toma seu correto sentido o disposto no inciso XII do art. 5 da CF quando ali se admite, apenas para a comunicação telefônica e, assim mesmo, só para fins de investigação criminal ou instrução processual penal, por ordem judicial, a quebra do sigilo. Conquanto haja quem caminhe para uma interpretação literal deste texto, não nos parece razoável aceitá-la na sua inteira singeleza. Note-se, antes de mais nada, que dos quatro meios de comunicação ali mencionados – correspondência, telegrafia, dados, telefonia – só o último se caracteriza por sua instantaneidade. Isto é, a comunicação telefônica só *é enquanto ocorre*. Encerrada, não deixa vestígios no que se refere ao relato das mensagens e aos sujeitos comunicadores. É apenas possível, *a posteriori*, verificar qual unidade telefônica ligou para outra. A gravação de conversas telefônicas por meio chamado “grampeamento” é, pois, uma forma subreptícia de violação do direito ao sigilo da comunicação mas, ao mesmo tempo, é a única forma tecnicamente conhecida de preservar a ação comunicativa. Por isso, no interesse público (investigação criminal ou instrução processual penal), é o único meio de comunicação que exigiu, do constituinte, uma ressalva expressa. Os outros três não sofreram semelhante ressalva porque, no interesse público, é possível realizar investigações e obter provas com base em vestígios que a comunicação deixa: a carta guardada, o testemunho de quem leu o nome do endereçado e do remetente, ou de quem viu a destruição do documento, o que vale também para o telegrama, para o telex, para o telefax, para a recepção da mensagem de um computador para outro, etc.” (FERRAZ JÚNIOR, 1993, p. 447, 448).

A ideia defendida pelo artigo está relacionada com o estado tecnológico existente à época: quando escrito, a preocupação era a de proteger o cidadão de uma interferência estatal no caminho percorrido pela informação (fluxo), não nos registros por ela deixados. Essa concepção dialoga com a efemeridade da comunicação por meios telefônicos, quando ligações telefônicas eram dominantes em se tratando de comunicação,

inexistindo as mesmas preocupações referentes às informações registra­is delas oriundas ou a quaisquer outras existentes. O STF incorporou, à sua jurisprudência, esse entendimento, notadamente no Mandado de Segurança 21.729/DF, cuja síntese já foi realizada:

“MS 21.729/DF: tratava-se de mandado de segurança impetrado pelo Banco do Brasil contra ato do Procurador-Geral da República, que demandava, por ofício, lista de nomes dos beneficiários de liberação de recursos públicos ao setor sucroalcooleiro, além de dados específicos sobre existência de débitos e naturezas das operações que os originaram. A argumentação do impetrante não chegava a mencionar o artigo 5º, inciso XII, da Constituição, mas limitava-se a insistir na necessidade de ordem judicial para o acesso a tais informações, que equivaleria a quebra de sigilo.

A autoridade coatora prestou informações, confirmando os fatos e alegando que havia questionamentos quanto à autoridade do Ministério Público para requerer os dados em questão. Alegaram suspeitar de violação tanto da Lei Complementar (LC) 75/1993, quanto do art. 129, inciso VI, da Constituição Federal. Em extenso parecer, o Vice Procurador Geral da República introduziu a discussão sobre o inciso XII, juntamente com trecho do artigo de Ferraz Júnior (Vice Procuradoria Geral da República, 1994). Foi a primeira aparição de “Sigilo de dados” nos autos do caso. O parecer da PGR argumentava que o sigilo bancário não teria guarida constitucional, nem a partir de interpretação do artigo 5º, inciso X, nem a partir do inciso XII. Nesse sentido, sem natureza constitucional, as exceções estabelecidas ao sigilo bancário seriam válidas enquanto motivadas pela salvaguarda de interesses constitucionalmente protegidos – como seria o caso do art. 8º da LC 75, em sintonia com o art. 129, inciso VI da Constituição Federal. Segundo o parecer, o inciso XII do art. 5º não protegia o sigilo bancário, porque blindaria, através do sigilo, apenas as comunicações de dados – e não os dados em si, uma vez recebidos e armazenados.

Por maioria de 6 a 5, o STF indeferiu o mandado de segurança. A tese encampada pela PGR, da inviolabilidade do sigilo de comunicações, mas não dos dados armazenados, elaborada com apoio no texto de Ferraz Júnior, sagrou-se vencedora. Em dois votos vencedores, dos Ministros Sepúlveda Pertence e Francisco Rezek, o texto foi expressamente citado. A *ratio* comum da maioria do Tribunal, entretanto, extraída dos votos dos Ministros Octavio Gallotti, Sidney Sanches, Néri da Silveira, Moreira Alves e Sepúlveda Pertence, fundamentou-se na aplicação do princípio da publicidade às operações envolvendo recursos públicos. Tratava-se, afinal, de um caso envolvendo financiamentos rurais concedidos pelo Banco do Brasil.” (QUEIROZ; PONCE, 2020, p. 72).

De qualquer sorte, como se verá mais adiante, a jurisprudência pátria encampou esse entendimento – de que a proteção constitucional do art. 5º, inc. XII é do fluxo comunicacional e não dos dados registra­is –, sendo esse, via de regra, o limite que as decisões judiciais na matéria adotam. Muito antes de realizar uma crítica a essa concepção, o que se propõe é o debate a respeito das mutações havidas em nossa sociedade

(fundamentalmente, as catapultadas por inovações tecnológicas) e ao modo com que elas interferem na interpretação do texto constitucional. Em melhores termos:

“Ainda nesse contexto, é preciso recordar que uma concepção satisfatória de direitos fundamentais somente pode ser obtida com relação a uma ordem constitucional concreta, pois o que é fundamental para uma sociedade pode não o ser para outra, ou não o ser da mesma forma, o que não afasta a necessidade de se considerar a existência de categorias universais (portanto, universalizáveis) no que diz com respeito à fundamentalidade de certos valores, como é o caso da vida, da dignidade da pessoa humana, assim como da liberdade, igualdade e segurança, entre outros, ainda que também esses valores careçam de uma adequada contextualização, especialmente quando se cuida de transformá-los em realidade. É, pois, justamente considerando o elo entre direitos fundamentais, liberdade e dignidade da pessoa humana que, na sequência, se estará a examinar o direito à proteção de dados pessoais como direito fundamental.” (SARLET; SAVEEDRA, 2020, p. 40-41).

O caso trazido na introdução, sintetiza bem o entendimento que vem sendo majoritário. A requisição da autoridade investigante, Ministério Público do Rio de Janeiro, foi de obter acesso aos endereços de IP de pessoas que procuram uma série de palavras-chave relacionadas ao caso Marielle Franco e Anderson Gomes no sistema de buscas do Google, o que foi autorizado por decisão judicial de 1º Grau.

O Google, a quem se dirigia a decisão, recorreu alegando uma série de ofensas constitucionais que a decisão poderia acarretar. Principalmente, que a medida fere o sigilo de uma série de pessoas inocentes, devendo haver uma individualização da medida de forma fundamentada, que é um requisito, por exemplo, da LIT.

O TJRJ manteve a decisão em segunda instância e a empresa recorreu ao STJ. No julgamento do RMS 60.698, a Terceira Seção da Corte teve por manter a decisão. De acordo com o entendimento firmado pelo julgamento, não é aplicável a LIT, senão o Marco Civil da Internet (MCI) para solucionar a questão, legislação que não obriga a individualização do investigado. O julgado entende que o MCI adota política mais permissiva para casos de investigações criminais, sendo necessários menos requisitos para a decisão que autoriza a quebra de sigilo¹¹.

A mesma lógica foi utilizada em outra decisão, a qual afastou incidência da LIT em decisão que quebrou o sigilo de conteúdo de mensagens de *e-mail*. Apesar de serem atividade típica de comunicação, entendeu-se que, por se tratar de dados registraes, prevalece a aplicação do MCI, não da LIT¹²:

“Agravos regimentais. Recurso em mandado de segurança. Sustentação oral. Previsão regimental ou legal. Inexistência. Descabimento. Comunicação privada. Guarda em

11. STJ, RMS 60.698, rel. Min. Rogerio Schietti Cruz, 3ª S., j. 26.08.2020.

12. STJ, AgRg no RMS 63041, 5ª T., rel. Min. Ribeiro Dantas, j. 17.11.2020.

conta de e-mail. Quebra do sigilo. Decisão judicial. Possibilidade. Crimes punidos com detenção. Irrelevância. Art. 2º, da Lei n. 9.296/1996. Não incidência. Art. 7º, III, da Lei n. 12.965/2014. Regra específica e posterior. Aplicação. Recurso não provido. (...) 2. A quebra de sigilo de conteúdo de comunicação privada armazenada em conta de e-mail depende de prévia autorização judicial, mediante decisão devidamente fundamentada, a qual, porém, diferentemente do que acontece com as interceptações telefônicas e com o fluxo de comunicações pela *internet*, independe dos requisitos estabelecidos no art. 2º, da Lei n. 9.296/1996, em face da incidência, específica e posterior, do previsto no art. 7º, III, da Lei n. 12.965/2014 – Marco Civil da Internet. 3. Agravo regimental não provido. (...).”

Mesmo a obrigatoriedade de decisão judicial é alvo de debate: das legislações que determinam o registro, tanto a Lei de Organizações Criminosas como a de Lavagem de Dinheiro, permitem a entrega dados apenas com requisição da autoridade investigante. Veja-se a diferenciação prática para dados coletados pelo *Whatsapp*, de acordo com literatura sobre investigação criminal e tecnologia

“Mediante requisição do delegado de polícia, em crimes de maior gravidade (a exemplo dos artigos 13-A do Código de Processo Penal, 17-B da Lei n. 9.613/985 e 15 da Lei n. 12.850/16), o WhatsApp informa os dados cadastrais das contas de seus clientes (informações do aparelho e sistema operacional, versão da App, data e horário do registro, status de conexão, última conexão com data e hora, nome e endereço de e-mail se disponível, informações de cliente Web etc.) e por intermédio de ordem judicial, além dos dados cadastrais, informa também: registros de acesso (IPs) dos últimos 6 meses; histórico de mudança de números; grupos (data de criação, descrição, identificador do Grupo (“group-ID”), foto, quantidade de membros e nome do Grupo); agenda de contatos simétricos e assimétricos. Também é possível realizar, mediante ordem judicial, a interceptação telemática da conta do WhatsApp do alvo, que permitirá receber o extrato das mensagens, mas cabe esclarecer que não será possível ter acesso ao conteúdo dessas comunicações.” (WENDT e JORGE, 2021, p. 140).

Assim, o limite das decisões judiciais na matéria parece ser o da proteção do fluxo de comunicações, sendo os dados classificados como “registros”. É justamente ao não incorporar o conceito de dado pessoal, mas de dados registrais, que a proteção constitucional apenas do fluxo de comunicações é possível, pois, ao assumir o conceito de “dado pessoal”, uma série de outras proteções são acionadas, como se verá adiante.

Da mesma maneira com que o tratamento de dados ganhou importância no nosso cotidiano, e nas atividades de segurança pública, legislações de proteção da privacidade e da intimidade dos usuários passaram a ser criadas. No Brasil, a Lei Geral de Proteção de Dados é um marco regulatório importante para resolver uma série de problemas de tratamentos de dados, conferindo ampla proteção a cidadãos. Não há, como dito, uma legislação específica para matéria penal no Brasil; no entanto, o Direito comparado tem produzidos normas mais protetivas e específicas em questão penal, como é o caso da

Diretiva 680 do Parlamento Europeu. Conforme referido *en passant*, em novembro de 2020, uma comissão de juristas entregou ao Congresso Nacional o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, o qual tenta adequar o Brasil a padrões internacionais de proteção de dados em questão criminal, bem como fornece bases mais democráticas para a matéria no país. A adequação a *standards* internacionais de proteção de dados é um fator importante também para as investigações criminais no país, conforme a exposição de motivos do Anteprojeto:

“De fato, destaca-se que a grande lacuna legislativa existente hoje no ordenamento jurídico brasileiro nessa matéria se manifesta em duas problemáticas centrais. O primeiro problema diz respeito à própria eficiência investigativa dos órgãos brasileiros, visto que a falta de adequação aos padrões internacionais de segurança quanto ao fluxo e ao tratamento de dados obsta a integração do Brasil com órgãos de inteligência e de investigação de caráter internacional (v.g., INTERPOL), obstando o próprio acesso a bancos de dados e a informações relevantes, e coloca o uso de aplicações tecnológicas em segurança pública e a adoção de técnicas modernas de investigação sob questionamento de sua validade jurídica.

Em segundo lugar, há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão). Nesse contexto, o titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal.” (BRASIL, 2020, p. 1 e 2).

É justamente nesse “déficit de proteção dos cidadãos” que está centrado o problema do artigo: mesmo sem legislação própria, há limites protetivos aos cidadãos na utilização de dados pessoais em investigações criminais?

3. O QUE É UM DADO, AFINAL? OS CONCEITOS EXPANSIONISTA E REDUCIONISTA DE DADO PESSOAL E SUA APLICAÇÃO NO DIREITO PENAL BRASILEIRO

Na introdução do artigo, apresentamos uma definição de dado: “fatos conhecidos que podem ser registrados e possuem significado implícito” (ELMASRI; NAVATHE, 2011, p. 3). Ainda, nos referimos a dados pessoais como sendo aqueles dados que podem ser ligados a uma pessoa natural. Essa acepção se aproxima de um senso comum, que é quase intuitiva, tamanha a relevância que o tema ganhou em nossa sociedade.

No entanto, tal definição não dá conta de responder o problema proposto. Necessário, para isto, compreender a dimensão jurídica do termo. Na sequência, problematizaremos a utilização do termo no direito penal brasileiro no âmbito jurisprudencial e na produção legislativa.

3.1. *Dado pessoal: um conceito jurídico*

A definição de dado pessoal é amplamente debatida pela doutrina, na medida em que é do conceito que se decide pela aplicabilidade, ou não, de princípios, pressupostos e legislações de proteção de dados. A proteção da inviolabilidade dos dados pessoais, como vimos, pode ser extraída de direitos fundamentais garantidos pela Constituição Federal (notadamente, no art. 5º, incisos IX, X e XII). É justamente o conceito de dado pessoal que define o escopo de que se dará a determinada informação.

Para o presente artigo, iremos conceituá-lo a partir de duas orientações: a expansionista e a reducionista. Para compreender a noção jurídica, é preciso entender a linguagem por trás do conceito e o significado dela para a aplicação da norma. Com isso, nas duas concepções propostas, expansionista e reducionista, “há um vocabulário que, respectivamente, alarga (pessoa identificável) ou restringe (pessoa identificada) o escopo de uma lei de proteção de dados pessoais” (BIONI, 2016, p. 4).

Para que se compreenda melhor, há de se entender que ambas as conceituações têm o mesmo ponto de partida: definir se, a partir do contexto em que está inserido, um dado pode ser relacionado a uma pessoa natural. A diferença está, justamente, na maneira com que é feita essa correlação de informações (dado e pessoa). No conceito reducionista, dado pessoal é aquele que identifica uma pessoa natural de maneira específica ou determinada, estabelecendo um vínculo imediato e direto entre as duas informações. Por exemplo, um número de CPF pode identificar uma pessoa natural de forma direta.

Já em uma conceituação expansionista, o dado é pessoal quando identificável a uma pessoa natural. O vínculo entre as duas informações, portanto, pode se dar de maneira indireta. Assim:

“[a] expansionista aposta em uma lógica mais flexível, que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta. Um dado para ser pessoal deve ser, portanto, a projeção de uma pessoa identificável.” (BIONI, 2016, p. 17).

Desse modo, expande-se o conceito para uma análise não de correlação direta, mas para uma análise do quão identificável é um dado. A definição faz sentido no contexto das novas tecnologias de processamento de dados e de inteligência artificial, as quais

tornam cada vez mais difícil, senão inviável, o processo de anonimização de um dado (BIONI, 2016).

Com as tecnologias disponíveis hoje, a tarefa de produzir a suposta antinomia do dado pessoal, isto é, o dado anônimo, se torna tão difícil que já considerada como impossível (BIONI, 2016). Dito de outra maneira: o conceito reducionista entende que um dado anônimo seria aquele que não tem relação direta com uma pessoa natural, ao passo que o expansionista leva em consideração a ideia de que aquele dado, aparentemente anônimo, pode ser vinculado a uma pessoa a partir de processos de reversão.

Por essa razão, em busca de um maior escopo de proteção dos dados pessoais, decisões¹³ e legislações¹⁴ atinentes à proteção de dados têm adotado um conceito expansionista. Da mesma forma, a legislação brasileira adotou uma conceituação expansionista para dado pessoal.

O Marco Civil da Internet (MCI), aplicável como legislação específica na matéria para fins penais, traz, no decreto que o regula, 8.771, uma conceituação do termo, inclusive com um rol exemplificativo:

“Art. 14. Para os fins do disposto neste Decreto, considera-se:

I – dado pessoal – dado relacionado a pessoa natural identificada ou *identificável*, inclusive números identificativos, *dados locacionais* ou *identificadores eletrônicos*, quando estes estiverem relacionados a uma pessoa; e II – tratamento de dados pessoais – 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.” (Grifamos).

A LGPD traz, em seu art. 5º, uma série de definições que ajudam a delinear o problema proposto:

“Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: informação relacionada a pessoa natural identificada ou *identificável*;

13. Para os fins desse artigo, é de se mencionar a decisão da Corte Europeia de Justiça no caso *Patrick Breyer v. Bundesrepublik Deutschland* (2016).

14. A General Data Protection Regulation (GDPR), legislação europeia de proteção de dados define o dado pessoal, em seu art. 4(1): “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”.

II – dado pessoal sensível: dado pessoal 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;

III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.”

No entanto, para fins de investigação criminal, veremos que o conceito expansionista de dado não é comumente utilizado na jurisprudência e na doutrina. Conforme referimos na introdução, a LGPD exclui, em seu art. 4º, sua atuação para fins de investigação criminal. A sua vez, o Marco Civil da Internet (MCI) já é aplicado nas decisões criminais, no entanto o conceito adotado pelo legislador não costuma ser aplicado.). Veja-se o âmbito de proteção que a legislação confere aos dados pessoais:

“Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II – proteção da privacidade; III – proteção dos dados pessoais, na forma da lei; (...)

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. (...).”

Assim, o conceito de dado pessoal, bem como a garantia de proteção das comunicações e do fluxo de informações são protegidos para fins de Direito Penal. O conceito expansivo de dado pessoal já foi assentado no julgamento do caso IBGE (ADI 6387)¹⁵, quando o STF aplicou uma conceituação expansiva com fundamentos constitucionais:

“Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, 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. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.”

15. Adiante, faremos uma análise mais detalhada dessa decisão.

Veja-se que, a proteção é aplicada não apenas aos dados que poderiam identificar uma pessoa natural de forma direta, senão também de maneira potencial, ou seja, identificáveis. Resta entender, de modo geral, o que é identificável, pois, em se expandindo exageradamente o conceito (a partir de uma ideia que anonimização é impossível) todos os dados serão pessoais. Nesse sentido:

“Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o sufixo identificável (Article 29 WP 29, 2007: 15). Essa vinculação deve ser objeto de um esforço razoável, sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável. A *contrarium sensu*, de acordo com as regulações europeias, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o filtro da razoabilidade barra o seu enquadramento como aquele relacionado a uma pessoa identificável (Article 29 WP, 2007: 21). Trata-se de uma estratégia normativa alinhada à premissa de que os dados anônimos são sempre passíveis de reversão. Daí porque, o critério da razoabilidade nada mais é do que uma diretriz acerca do que venha a ser um risco aceitável em torno da reversibilidade do processo de anonimização, a fim de que os dados anonimizados estejam fora do conceito de dados pessoais. Com isso, há coerência em se estabelecer conceitos diferentes para tais espécies de dados, sobretudo sob o ponto de vista de uma dicotomia mutuamente excludente entre eles que é delimitada pelo fator da razoabilidade. Do contrário, repita-se, haveria uma redundância normativa, na medida em que dados anônimos – sem o critério da razoabilidade – seriam sempre enquadrados dentro do conceito de dado pessoal, como aquele relacionado a uma pessoa identificável.” (BIONI, 2016, p. 32).

É paralelo a essa ideia o entendimento do STF acima mencionado, entendendo como o escopo de proteção à inviolabilidade dos dados se dá para aqueles em que há uma identificação direta e indireta (identificável). Com isso, percebe-se a existência de uma conceituação jurídica de dado pessoal expansionista no direito brasileiro, seja pelo fornecimento de dispositivo legal para tanto ou pela garantia de proteção constitucional a dados que potencialmente podem identificar uma pessoa natural. No entanto, há relutância de se adotar o conceito para investigações criminais. A seguir, analisaremos a aplicação do conceito no direito penal.

3.2. *A aplicação de um conceito restritivo de dado pessoal e a proteção dos metadados no direito penal brasileiro: exemplos da ADI 4.739 e do PL 2630/2020*

Apesar do demonstrado no ponto anterior, o emprego de um conceito expansionista de dado pessoal ainda não é recorrente no direito penal, o que pode ser compreendido a partir da leitura do ponto 2.2., em que os tribunais vêm relegando uma proteção menos ampla para a inviolabilidade dos dados.

Para aprofundarmos a matéria, no entanto, precisamos entender de que modo o direito penal tem lidado com o conceito de dado pessoal. Como demonstração, buscamos dois exemplos: um jurisprudencial e uma proposta legislativa. Em ambos, a aplicabilidade de proteções constitucionais é afastada quando se trata de metadados, ou seja, definições ou informações descritivas de um outro dado¹⁶.

Na ADI 4739, o STF declarou a inconstitucionalidade da Lei 2.569/2011, do estado de Rondônia, a qual obrigava que operadoras de telefonia móvel fornecessem, por simples requerimento da polícia judiciária (ou seja, sem a necessidade de amparo em uma decisão judicial), a geolocalização de aparelhos celulares para fins de investigações criminais. A geolocalização consiste na informação descritiva (coordenada geográfica) do ponto em que se encontra um determinado aparelho celular, resultando no apontamento da localização da pessoa, caso ela esteja portando o aparelho monitorado.

Em que pese o inteiro teor do acórdão não tenha sido publicado no momento de escrita desse artigo, já está disponível o voto vencedor¹⁷, de relatoria do Ministro Marco Aurélio, o qual, teve por decretar a inconstitucionalidade por uma questão de competência: é privativa da União a competência de legislar sobre telecomunicações.

Contudo, resta a indagação: poderia o Congresso Nacional criar idêntica lei, possibilitando o acesso, em investigações criminais, a geolocalização de aparelhos celulares sem prévia decisão judicial¹⁸?

Tal situação poderia ferir a proteção constitucional da inviolabilidade dos dados (art. 5º, inc. XII, CF) em se entendendo a geolocalização como sendo um dado pessoal, bem como a obrigação do MCI em haver decisão judicial fundamentada para o uso de dados pessoais em investigações criminais. Lembrando-se que a geolocalização trata de um objeto – cujo uso está amplamente difundido na vida diária das pessoas atualmente – que há de revelar a localização da pessoa, permitindo um monitoramento de seus deslocamentos diários. O voto do relator aponta uma direção menos protetiva, retirando a proteção constitucional a metadados:

16. “Consideram-se metadados todos os dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI), etc.” (ABREU, ANTONIALI, 2017, p. 17).
17. Votaram com o relator, os Ministros Luiz Fux, Cármen Lúcia e Gilmar Mendes. Por fundamentação diversa, mas com o mesmo resultado, votaram os Ministros Luiz Edson Fachin, Rosa Weber, Dias Toffoli, Luís Roberto Barroso, Ricardo Lewandowski e Nunes Marques. Desses, apenas o Min. Luis Barroso entendeu que as informações requeridas demandam uma decisão judicial. Com a publicação do inteiro teor do acórdão, será possível estabelecer melhor de que modo se deu o debate.
18. A leitura dos artigos do MCI acima colacionados (art. 7º, inc. III, principalmente) já responde à pergunta a respeito da decisão judicial. Mas o presente artigo busca justamente os limites internos dessa decisão, no que seguiremos com a argumentação.

“A razão é única: conforme assentado, pelo Pleno, no julgamento do recurso extraordinário 389.808, da minha relatoria, com acórdão publicado no Diário da Justiça de 10 de maio de 2011, a vedação contida no inciso XII do artigo 5º refere-se à correspondência, às comunicações e aos dados porventura existentes nos referidos aparelhos, alcançando não apenas as chamadas telefônicas realizadas e recebidas mas também o acesso à agenda eletrônica e ao conteúdo das mensagens de texto, arquivos e documentos eletrônicos. Tem-se circunstância diversa considerada a diretriz normativa constante do diploma impugnado, o qual não trata de acesso às informações, às mensagens ou a quaisquer dados armazenados em aparelho celular, versando apenas a comunicação, à autoridade policial, de informação alusiva à localização do dispositivo móvel – a qual não se enquadra no conceito de ‘dado’, na forma tutelada pelo constituinte.”

Veja-se, portanto, que, em linhas gerais, a geolocalização de um aparelho móvel recebeu, nesse voto, uma conceituação restritiva na medida que afasta a ideia de pessoalidade da informação, pois se trata de um dado descritivo, a localização do aparelho, não sobre o indivíduo em si.

Aplicando-se a conceituação expansiva, no entanto, percebe-se que a geolocalização é um dado que é facilmente identificável a uma pessoa natural: a observação de um conjunto de geolocalizações supostamente anônimas permite saber uma série de informações a respeito do usuário daquele aparelho telefônico (local de residência, local de trabalho, rotas de deslocamento, forma de deslocamento, além de lugares frequentemente visitados). A geolocalização, inclusive, é elencada pelo decreto regulador do MCI, 8.771, como um dos exemplos de dado pessoal.

O pano de fundo desse debate é o âmbito de proteção dos chamado metadados, que são “uma espécie de envelope do processo comunicacional” (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, 2020, p. 11), pois fornecem informações descritivas a respeito de outros dados. Desse modo, quando enviamos uma mensagem em um aplicativo, para além do conteúdo do texto, uma série de outras informações é colhida: hora de envio, aparelho de origem etc. É comum a ideia de que esses dados não identificam uma pessoa natural; o que ensejaria, portanto, em uma menor restrição para o tratamento desses dados.

A geolocalização se enquadra nessa categoria, bem como uma série de outros registros de serviços de telecomunicação: endereços de IP, data e hora de ligações, número de telefones, endereços de e-mail, entre diversos outros metadados¹⁹. Conforme visto, a legislação

19. Com mais detalhe a respeito do que são metadados e sobre sua identificabilidade: “The term ‘metadata’ relates to information generated or processed as a consequence of a communication’s transmission. Much can be revealed from this data including: ‘latitude, longitude and altitude of the sender’s or recipient’s terminal, direction of travel...any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection’ (Young, 2004). Metadata therefore concerns the context as opposed to the content of a communication and covers many types of information such as traffic data, location data, user data and the subscriber data of the device/

brasileira já obriga, para fins investigativos, a retenção de metadados por parte de empresas de telecomunicação e aplicações da internet, fundamentalmente a partir das definições do Marco Civil da Internet. A partir de uma decisão judicial devidamente fundamentada é possível o acesso a tais registros.

É justamente em torno dessa questão que gira o debate a respeito do PL 2630/2020, a “Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet”, cujo texto foi aprovado no Senado e está em tramitação na Câmara dos Deputados²⁰. Sob o pretexto de combater a disseminação das *fake news*, o PL amplia o escopo de registro de informações para fins penais, determinado a guarda do registro (metadado) de mensagens que atinjam um determinado número de pessoas em um determinado período de tempo. Para além do debate a respeito da criminalização das chamadas *fake News*, o artigo 10 do PL é bastante criticado:

“Art. 10. Os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens.

§ 1º Considera-se encaminhamento em massa o envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários.

§ 2º Os registros de que trata o caput devem conter a indicação dos usuários que realizaram encaminhamentos em massa da mensagem, com data e horário do encaminhamento e o quantitativo total de usuários que receberam a mensagem.

§ 3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento em massa de conteúdo ilícito, para constituição de prova em investigação criminal e em instrução processual penal, mediante ordem judicial, nos termos da Seção IV do Capítulo III da Lei 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

§ 4º A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcancem quantitativo total inferior a 1.000 (mil) usuários, devendo seus registros ser destruídos nos termos da Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).”

service being used (e.g. cellular phone network or Internet service provider). As a result, metadata is a rich source of personal information as it reveals the ‘who’ (parties involved), the ‘when’, how long and how often, (time, duration and frequency), the ‘what’ (type of communication, e.g. phone call, message, e-mail), the ‘how’ (the communication device used, e.g. landline telephony, smartphone, tablet) and the ‘where’ (location of devices used) involved in every communication we make. Moreover, the collection, aggregation and analysis of metadata can provide very detailed information regarding an individual’s beliefs, preferences and behaviour” (NI LOIDEAIN, 2015, p. 2).

20. CAMARA DOS DEPUTADOS, 2020a.

Tratamos, novamente, do armazenamento de metadados para fins de investigações criminais (lembrando que a proteção aos dados deve se dar em todas as etapas do tratamento, sendo a decisão do registro deles também submetida à análise aqui proposta). Ao mesmo tempo que os registros podem possibilitar a identificação de propagadores de desinformação (a medida é apontada como inefetiva²¹), a lei cria um imenso banco de dados de pessoas que se utilizam dos aplicativos de mensagem para transmissão de informações de qualidade.

A defesa em torno do projeto é no sentido de que esse seria meio efetivo para o combate da desinformação sem que a privacidade dos usuários fosse violada, tendo em vista que “PL trata do dever de guarda dos registros de envio de encaminhamento de mensagens massivas, o que em nenhuma hipótese abre caminho para a formação de perfis individuais” (ABRUSIO et al., 2020), não levando em conta a identificabilidade de um metadado ou, ainda, o risco que sua utilização massiva em investigações criminais representa.

A medida é alvo de críticas por atingir um sem-número de indivíduos, inclusive jornalistas e acadêmicos, pois fere o princípio da presunção de inocência²². O tratamento de metadados como dados pessoais é chave para determinar o grau de proteção que se dá a eles:

“Assim, metadados enquadram-se, via de regra, na definição de dado pessoal, na medida em que tornam uma pessoa identificada ou identificável. Trata-se, portanto, de uma informação protegida pela legislação e pelo direito fundamental à proteção de dados pessoais. Logo, metadados, ao contrário do que percorreu em parte da discussão ao longo da célere tramitação do PL 2630/2020, são tão ou talvez mais críticos que outros tipos de dados pessoais, como o conteúdo em si de mensagens.” (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, 2020, p. 12).

No mesmo sentido, a Comissão de Juristas criada para propor o Antreprojeto de Lei Geral de Proteção de Dados em matéria criminal apresentou críticas semelhantes ao Projeto.²³ A crítica vai, justamente, no sentido de não haver, na legislação proposta, qualquer parâmetro de proteção aos dados pessoais ou, ainda, respeito aos princípios que versam sobre a matéria.

21. BIONI; ZANATTA, 2020.

22. Um debate aprofundado sobre o PL: Associação Data Privacy Brasil de Pesquisa (2020).

23. De acordo com reportagem intitulada “Rastreabilidade em serviços de mensagens prevista no projeto de fake news é criticada em seminário” (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020), diversos integrantes da Comissão manifestaram preocupação com relação ao projeto.

A propósito da proteção aos metadados no direito penal, parece haver um entendimento majoritário, inclusive na doutrina mais clássica²⁴, de que metadados não estão cobertos pela proteção constitucional, justamente por serem “registros”, quando a proteção constitucional seria do fluxo da comunicação, como visto. Assim, percebe-se que, em se tratando de justiça criminal, é comum que um conceito reducionista, ou seja, menos protetivo, seja adotado. Essa tendência está evidenciada tanto na decisão do voto-vencedor, como na proposição do PL 2630/2020; há uma exclusão da proteção constitucional dos metadados sob a justificativa de que se trata de registro, não se relacionando diretamente com uma pessoa natural.

Vimos, na apresentação do problema, que os tribunais nacionais têm diversos julgados que entendem ter o MCI um regime de proteção menor para dados registrais (sem tratar do termo dados pessoais) do que a Lei de Interceptações Telefônicas (LIT), tendo sido, no entender desses julgados, uma opção do legislador dar uma maior preponderância à persecução penal do que à proteção da intimidade²⁵. A mesma situação (utilização do conceito de dado registral para reduzir o escopo de proteção do indivíduo) já foi identificada quando analisada a jurisprudência de tribunais estaduais (ABREU; ANTONIALLI et al., 2019) ou, ainda, enquanto opção legislativa em outros projetos que tratam da matéria²⁶.

24. “O entendimento doutrinário até hoje predominante, que também encontra eco em decisão do Supremo Tribunal Federal, é no sentido de que (i) a proteção do inciso XII do art. 5º não se refere ao conteúdo das informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas sim à sua comunicação, isto é, ao seu fluxo enquanto ocorrem e que (ii) apenas o sigilo da comunicação por telefonia, enquanto está em fluxo, poderia ser restringido para fins de investigação criminal e instrução processual penal, não se estendendo essa possibilidade para o fluxo de dados, telegrafias e cartas. Esse entendimento exclui, portanto, do âmbito de proteção do dispositivo não somente o conteúdo de comunicações armazenadas, registradas ou gravadas como também as informações geradas a respeito das circunstâncias nas quais as comunicações ocorreram (metadados). Em razão dessa limitação, diversos autores têm argumentado em favor de novas interpretações desse dispositivo, no sentido de levar em conta os avanços da tecnologia e as enormes quantidades de conteúdos e registros de comunicações que passaram a ser armazenadas em dispositivos pessoais, como computadores e aparelhos celulares. Diante disso, as disputas interpretativas a respeito da extensão dessa garantia constitucional reacenderam, tal como exploraremos abaixo” (ABREU, ANTONIALLI, 2017, p. 16).
25. Notadamente: STJ, AgRG no RMS 63.041, rel. Min. Ribeiro Dantas, 5ª T., j. 17.11.20. No entanto, percebe-se, como se verá adiante uma movimentação da jurisprudência no sentido de assimilar as definições da matéria de proteção de dados.
26. Sobre a não utilização do conceito de dado pessoal no PL 8.789/16: “[f]rente a isso, o decreto é marcado por um silêncio constrangedor. Ele não menciona uma vez sequer o termo “dados pessoais” – optando por falar em “dados cadastrais” e “dados individualizados”. A opção não é trivial. O decreto parece querer evitar a tensão fundamental que carrega com os princípios à base de regimes de proteção de dados pessoais – agora também em discussão no Congresso brasileiro” (ABREU, 2016).

3.3. *Resultados parciais*

Primeiramente, buscamos demonstrar já haver um conceito jurídico de dado pessoal no Brasil, tendo sido adotado um conceito expansionista (dado identificado ou identificável a uma pessoa natural), com relevância constitucional assentada pelo STF em recente julgamento, bem como pela adoção legal do conceito pelo MCI e pela LGPD (além de outras normas setoriais) (ponto 2.1.). O termo deve ser utilizado para fins penais, na medida que o Marco Civil da Internet (MCI) garante essa proteção em todos os âmbitos do direito pátrio, trazendo relevantes princípios a serem respeitados a partir da concepção de dado pessoal.

Ao mesmo tempo, percebemos que não há ampla adesão ao conceito quando se trata de investigações criminais: metadados – que, no conceito expansionista são, na maioria dos casos, conceituados como dados pessoais – não recebem a proteção constitucional de inviolabilidade dos dados. Tal fato se dá pelo entendimento ainda majoritário de que a proteção de que trata o art. 5º, inc. XII, CF é do fluxo das comunicações. Assim, dados que não têm um vínculo direto com a pessoa natural (conceito reducionista) são, geralmente, tratados como “dados registraes”, permitindo que a noção de proteger tão somente o “fluxo” da comunicação se mantenha.

Antes mesmo, quando apresentado o problema, já houve a demonstração de que recentes entendimentos do Superior Tribunal de Justiça têm entendido que o MCI adotou regime menos protetivo para a quebra de sigilo de dados. Essas decisões, contudo, não adentram na conceituação (e nas consequências dela) de “dado pessoal”, utilizando a definição de dado registral. A adoção do conceito de dado pessoal, contudo, enseja em um âmbito de proteção maior do que apenas a do fluxo comunicacional.

4. COMPARTILHAMENTO DE DADOS PESSOAIS EM INVESTIGAÇÕES CRIMINAIS: O RISCO DA VIGILÂNCIA PERMANENTE E A PROTEÇÃO CONSTITUCIONAL DO DEVIDO PROCESSO INFORMACIONAL E DO DIREITO À AUTODETERMINAÇÃO INFORMACIONAL

Nota-se, portanto, que se trata de uma questão de linguagem: ao utilizar classificações como “dados registraes” ou “dados informacionais”, opta-se por não os chamar por aquilo que também são: dados pessoais. Para além das críticas de política criminal, o objetivo aqui é entender se já há um dever de aplicação do conceito de dados pessoais no sistema de justiça criminal.

No entanto, não se pode deixar enganar: por trás de definições, há um impacto real no funcionamento do sistema penal. A manipulação indiscriminada de dados em investigações criminais já se demonstrou um risco a princípios básicos do Estado Democrático de Direito e do Direito Penal. Após uma rápida incursão a respeito dos riscos e da dimensão no problema do Brasil, buscaremos mecanismos constitucionais de proteção do indivíduo face a atuação estatal.

4.1. Uma dimensão do problema: o risco da vigilância a partir de dados pessoais

É importante a compreensão do debate que se apresenta: ao fim e ao cabo, estamos falando de limites à persecução penal em grande escala: 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 democráticos²⁷. 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, como é, justamente, o caso de Marielle Franco: 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:

“(...) a retenção de metadados pode gerar potenciais riscos para outras liberdades, relacionados à criação de um ambiente de vigilância, colocando em xeque o exercício de direitos fundamentais como o da liberdade de expressão. É o que se convencionou a chamar de efeito de resfriamento – *chilling effects* – pelo qual as pessoas deixam de livremente se expressar diante do receio das suas opiniões estarem sendo compiladas e, futuramente, voltarem-se contra elas, especialmente em ambientes autoritários.” (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, 2020, p. 7).

27. Cathy O’Neil (2016) mapeia muito bem o problema, além de cunhar um termo bastante explicativo: “weapons of math destruction”.

Estudos da vigilância tem o panoptismo²⁸ como categoria de análise²⁹ fundamental para a compreensão da matéria³⁰. É a partir de Vigiar e Punir que Michel Foucault realiza uma arqueologia da punição e coloca a vigilância, através do modelo panóptico, como um dos pilares do moderno punitivismo; a obra influenciou os autores de vigilância a partir de então.

Aliado à ideia de vigilância, a criminologia de viés crítico oferece uma série de leituras a respeito do sistema punitivo como reprodutor de desigualdades sociais, de mecanismos de controle social e de “gestões de risco”³¹. Ao pensar na vigilância como criadora de padrões de comportamento, como veremos adiante, é inescapável a categoria do *labeling approach* ou da ideia de direito penal do inimigo como fundamentos dos instrumentos

28. O termo dispensa maiores apresentações. A categoria advinda do modelo arquitetônico de prisão de Jeramim Bentham é uma representação simbólica da vigilância clássica: “[a] existência de todo um conjunto de técnicas e de instituições que assumem como tarefa medir, controlar e corrigir os anormais, faz funcionar os dispositivos disciplinares que o medo da peste chamava. (...) O panóptico de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia uma construção em anel; no centro, uma torre: está vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção (...)” (FOUCAULT, M. 2010 [1975]. p. 190).
29. “O panóptico ao contrário deve ser compreendido como um modelo generalizável de funcionamento; uma maneira de definir as relações do poder com a vida cotidiana dos homens.” (FOUCAULT, 2010 [1975], p. 194).
30. “Panoptic and post-panoptic studies of surveillance have both drawn heavily from French post-structuralist and postmodernist philosophies. Foucault’s incisive analyses of panoptic environments, particularly in *Discipline and Punish: The Birth of the Prison* (1979), provided the basis both for a disciplinary understanding of surveillance, i.e. control of visibility in confined space, and what one could call a “control model” understanding in which electronic surveillance is the norm. There has been a lively theoretical debate over the extent to which historically the disciplinary model has been abandoned in favor of the control model, and how they differ, both conceptually and in practice (cf. Lyon 2007; Hardt and Negri 2004; Haggerty and Ericson 2000) (see also McCahill, this volume)” (BOGARD, 2012, p. 30).
31. As conclusões de “Prisões da Miséria” oferecem importante aviso: “[a]ssim, propaga-se na Europa um novo senso comum penal neoliberal – sobre o qual vimos precedentemente como atravessou o Atlântico pelo viés de uma rede de ‘geradores de ideias’ neoconservadoras e de seus aliados no campo burocrático, jornalístico e acadêmico –, articulado em torno da maior repressão dos delitos menores e das simples infrações (com o slogan tão sonoro como oco, da ‘tolerância zero’), o agravamento das penas, a erosão da especificidade do tratamento da delinquência juvenil, a vigilância em cima das populações e dos territórios considerados ‘de risco’, a desregulamentação da administração penitenciária, e a redefinição da divisão do trabalho entre público e privado, em perfeita harmonia com o senso comum neoliberal em matéria econômica e social, que ele completa e conforta desdenhando qualquer consideração de ordem política e cívica para estender a linha de raciocínio economicista, o imperativo da responsabilidade individual – cujo avesso é a irresponsabilidade coletiva – e o dogma da eficiência do mercado ao domínio do crime e do castigo” (WACQUANT, 2001, p. 136). Ainda sobre o tema: O’MALLEY (2006) e CHRISTIE (1998).

de controle tecnológicos. Dieter (2012), por exemplo, é interessante chave de leitura para os riscos de processos de automatização e de utilização de dados no direito penal. Ao estudar a lógica atuarial³² em processos de criminalização secundária, tal qual como cálculos de reincidência nos Estados Unidos, ajuda a entender os problemas do Sistema COMPAS³³. Nesse sentido:

“É o controle do risco, ligado à noção de perigo, que passa a ser essencial às chamadas técnicas securitárias ou de controle. No campo criminológico, por exemplo, podemos vê-lo na Criminologia Atuarial, que tem em cálculos de probabilidade seu método de desenvolver conhecimento, uma legítima criminologia dura, da mesma maneira como trabalham as empresas de seguros. A partir desse raciocínio, podemos entender que há uma relação de similaridade entre as tecnologias do poder, as tecnologias de controle e as técnicas securitárias.” (EILBERG; SANTOS, 2020, p. 267-268).

Ainda que estudos criminológicos anteriores já forneçam uma base para a compreensão do problema (pois falam da lógica de funcionamento do sistema punitivo em si), apenas pesquisas específicas sobre a utilização de dados pessoais e sistemas de inteligência artificial no direito penal conseguem dar a dimensão do problema. A partir dos avanços tecnológicos no tratamento de dados, nem mesmo a figura clássica de panóptico de Foucault é tida como suficiente para compreender a questão³⁴.

32. “A expressão lógica atuarial remete à adoção sistemática do cálculo atuarial como critério de racionalidade de uma ação, definindo-se como tal a ponderação matemática de dados – normalmente inferidos a partir de amostragens – para determinar a probabilidade de fatos futuros concretos.” (DIETER, 2012, p. 6).
33. Acrônimo para *Correctional Offender Management Profiling for Alternative Sanction*, trata-se de sistema de inteligência artificial criado para realizar prognósticos de periculosidade no sistema de justiça criminal norte-americano, sendo decisivo em decisões da execução penal, como a liberdade condicional. “O programa COMPAS é frequentemente declarado racista: ele atribui a pessoas de pele escura, em princípio, uma maior probabilidade de reincidir. Isso ocorreria apesar de que o programa não leve de forma explícita a raça do afetado; a raça se correlacionaria com fatores como morar em região de alta criminalidade, falta de emprego fixo existência de conhecidos criminosos etc., fatores esses que estariam mais presentes em pessoas de pele escura que em outros grupos demográficos” (GRECO, 2020, p. 29). Com detalhes: ANGWIN; et al., (2016) e TOVO 2020).
34. “Consumer surveillance entails a massive intensification of surveillance throughout society, and technological innovation is constantly enhancing its capacity. Subject transparency is especially augmented. Connections with the nation state and with the capitalist workplace – Social Taylorism – should be pursued, but consumer surveillance must also be viewed as part of an emerging set of social arrangements, articulated with consumption, that is also a departure from what we already know about surveillance. Similarly, the Orwellian and panoptic metaphors still offer insights but cannot be expected to tell the whole store” (LYON, 1994, p. 156).

A sua vez, Lyon (1994) considerou a existência de um “superpanóptico” (p. 190 e ss.). Também, estudos da vigilância aproximam-na do conceito de biopolítica, fazendo da vigilância um instrumento de controle não apenas individual, mas também coletivo³⁵.

Avançando na ideia de uma economia baseada na coleta de dados e categorização de indivíduos, Zuboff (2019) – ao abordar o tratamento de dados por companhias privadas – defende a existência de um capitalismo de vigilância, em que o lucro não mais advém da exploração de recursos naturais e do trabalho (capitalismo industrial), senão da instrumentalização de métodos de coleta e análises de dados pessoais para fins de construir padrões de comportamento (capitalismo de vigilância)³⁶.

Ainda que com maior enfoque ao uso de dados no setor privado, o livro de Zuboff (2019) faz paralelo com referencial teórico que se aproxima com o da biopolítica, ao dialogar com os conceitos de “A origens totalitarismo” de Hannah Arendt. Além disso, traça paralelo com a utilização de metadados em investigações da *National Security Agency* a partir das denúncias de Edward Snowden³⁷, as quais demonstraram que a agência de segurança norte-americana utilizava metadados indiscriminadamente em uma série de investigações (ZUBOFF, 2019, p. 480).

35. Panoptismo e biopolítica fazem parte dos dois eixos de poder identificados pelo autor: “Foucault, detecta não um, mas dois tipos de poder que começam a descentralizar a soberania do século XVIII. São dois polos de controle, situados nos extremos de uma linha que vai desde a vigilância individualizada de todos e de cada corpo até a incitação de certos modos de comportamento na totalidade das populações” (GAMBETTI, 2019, p. 31). O panoptismo é justamente o eixo da “vigilância individualizada” e a biopolítica diz respeito com o manejo da vida da população. A conexão entre as teorias criminológicas anteriormente citadas, as quais apontam para uma política criminal da gestão do risco e do controle de setores da população, com o tratamento de dados na justiça criminal se dá, justamente, pela biopolítica: “One of the most distinctive features of this surveillance is that its predictive orientation is aimed at the detection of criminal acts, and at all human behavior in order to detect the risky ones. Even if this surveillance is processed through sensors, mathematical instructions and sequences of computer operations and thus appears neutral, such emphasis enhances in fact the biopolitical character of surveillance. Indeed, following the Foucauldian analysis of population management by security technologies we may then argue that through sophisticated surveillance mechanisms behavioral features of individuals and populations became an object of the political strategy of biopower. As aforementioned the principal technique of this power is the calculation of probabilities within a series of events, calculation of costs of action, normalization and correlations between different probabilities” (CEYHAN, Ayse, 2012, p. 43).

36. “Industrial capitalism depended upon the exploitation and control of nature, with catastrophic consequences that we only now recognize. Surveillance capitalism, I have suggested, depends instead upon the exploitation and control of human nature. The market reduces us to our behavior, transformed into another fictional commodity and packaged for others’ consumption. In the social principles of instrumentarian society, already brought to life in the experiences of our young, we can see more clearly how this novel capitalism aims to reshape our natures for the sake of its success” (ZUBOFF, 2019, p. 440).

37. As denúncias já são conhecidas desde 2013: Disponível em: [www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance]. Último acesso em: 17.03.2021.

Em se tratando de segurança pública, os exemplos de tratamento de dados penais são vários (e os seus riscos também): para além da quebra de sigilo em investigações criminais, já há utilização de sistemas de decisões automatizadas (como o já citado sistema COMPAS), uso de tecnologias de reconhecimento facial³⁸, bem como táticas de polícia preditiva.

Policimento preditivo é a série de tratamento de dados 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, o outros tipos de perfilização, e já são implementados em polícias no mundo para, inclusive, prever quais cidadãos têm mais tendência de cometer crimes³⁹.

É com esse evento que se percebe de maneira crucial que a proteção constitucional de dados pessoais é um imperativo para uma gestão de segurança pública que se proponha democrática⁴⁰. O tratamento dessas informações se mostrou tão ou mais invasiva que a interceptação de telecomunicações (FERGUSON, 2017a, p. 113). A ausência de *standards* legais bem definidos para a retenção e tratamento de metadados foi entendida pelo Tribunal de Justiça da União Europeia como violadora de direitos fundamentais de personalidade e da presunção da inocência (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, p. 7).

Há de se ressaltar, também, a urgência do tema. Uma série de leis e atos administrativos determinam a retenção de registros para fins investigativos, criando um imenso banco de dados pessoais, cujo acesso, pelas agências de segurança, deve ser regulamentado:

“O artigo mostrou que a Lei das Organizações Criminosas, de 2013, e o Marco Civil da Internet, de 2014, primeiro instituíram o dever legal de retenção de registros de telecomunicações para fins de segurança pública no Brasil. Essa obrigação é mais antiga no Brasil a nível infralegal: no âmbito da regulamentação de serviços de telecomunicações, as Resoluções 426 de 2005, 477 de 2007 e 614 de 2013 da ANATEL asseguram a disponibilidade de metadados já há mais tempo. A existência de tais obrigações insere o Brasil em um debate global acerca da constitucionalidade de tais disposições dentro de um Estado democrático de Direito que assegura o direito à privacidade e a presunção de inocência.” (ABREU et al., 2019, p. 9).

38. Sobre os riscos e a utilização desses sistemas no Brasil: Elesbão, Timm e Medina (2020). Na mesma obra, há uma série de outros artigos que ilustram os riscos relacionados ao tratamento massivo de dados na segurança pública.

39. A polícia de Chicago foi a pioneira. Com mais informações: Ferguson (2017b).

40. O argumento da agência é similar ao que vimos no ponto 2.2; não haveria uma proteção constitucional dos metadados: “Despite such privacy concerns, the government has consistently argued that the metadata program – because it was a non- content- based collection system – did not reveal constitutionally protected personal information” (FERGUSON, 2017a, p. 113).

O ponto específico relativo ao tratamento de dados e a vigilância é matéria extensa e que demanda uma análise específica. O que se tentou, no presente ponto, é demonstrar os riscos que uma ausência de proteção dos dados pessoais pode levar (e apontar os caminhos para uma melhor compreensão da matéria). Alguns aspectos teóricos do debate foram apontados em notas de rodapé, bem como a indicação de obras que abrem o debate a respeito dos perigos do uso de dados pessoais no sistema de justiça criminal.

Não é demais dizer que o direito penal brasileiro falhou em entregar bases democráticas de enfrentamento à questão criminal sendo notoriamente seletivo, repressivo e estigmatizador. Seja qual for a medida da crítica apresentada, é certo que o uso de dados pessoais pode amplificar essa situação⁴¹.

4.2. *O direito fundamental à autodeterminação informativa dos dados enquanto barreira constitucional à utilização de dados em matéria penal*

Buscamos demonstrar, até aqui, do que estamos falando (conceito de dados pessoais) e os riscos associados ao tratamento de dados pessoais no campo penal, especialmente em se tratando de investigações criminais. Nos parece que já é seguro dizer que uma ausência de regulamentação fere princípios básicos do estado democrático de direito, bem como do direito penal (presunção de inocência, mínima intervenção e fragmentariedade, por exemplo).

Cabe entender quais são os mecanismos de proteção que o direito penal possui para o problema. Para tanto, vamos nos valer de dois conceitos doutrinários que já receberam relevância constitucional pelo Supremo Tribunal Federal: o devido processo informacional e o direito à autodeterminação informativa.

Recentemente, o Supremo Tribunal Federal proferiu decisão na Medida Cautelar das ADIs 6.387, 6.388, 6.389, 6.393 e 6.390⁴². As ações referiam-se à Medida Provisória 954/2020, em que empresas de telecomunicação deveriam compartilhar informações pessoais com o Instituto Brasileiro de Geografia e Estatística (IBGE). Tal medida visava a garantir a realização de pesquisas do IBGE por meio telefônico, face às restrições impostas pela pandemia.

No julgamento dessas ADIs, questões importantes trazidas no presente texto foram utilizadas para argumentar pela inconstitucionalidade da MP, sendo a importância e o sentido da decisão resumidas da seguinte maneira:

“O Tribunal formulou, assim, uma tutela constitucional mais ampla e abstrata do que o direito à inviolabilidade da esfera íntima e da vida privada. Essa tutela poderá ser

41. Não são poucas as publicações que demonstram preocupação com a situação no Brasil. Além das já citadas. Associação Data Privacy Brasil de Pesquisa e Centro de Análise Da Liberdade e do Autoritarismo (2020) publicaram retrospectiva a respeito do assunto que demonstra a quantidade de situações em que se apresentam riscos.

42. STF, ADI 6.387; 6.388; 6.389; 6.390; 6.393, Plenário, rel. Min. Rosa Weber, j. 06 e 07.05.2020.

aplicada em inúmeros casos futuros envolvendo a coleta, o processamento e o compartilhamento de dados pessoais no Brasil. O conteúdo desse direito fundamental exorbita aquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados, ao revés, refere-se a qualquer dado que identifique ou possa identificar um indivíduo.” (MENDES, 2020, p. 3).

Voltando-se, à análise do caso IBGE, ainda que a finalidade para a colheita dos dados pudesse ser justificável, a ausência de parâmetros de controle no tratamento dos dados foi fundamental para a decisão, sendo necessárias que sejam adotadas “providências mínimas de cunho organizacional e preventivo voltadas à segurança dos cidadãos envolvidos e à diminuição dos riscos à sua personalidade” (MENDES, 2020, p. 4). Tal situação, de acordo com a decisão, feriria o postulado da proporcionalidade, como se lê do voto-relator, da Min. Rosa Weber:

“As leis que tratam de coleta e processamento de dados devem (i) atender a propósitos legítimos, específicos, explícitos e informados; (iii) limitar a coleta ao mínimo necessário para a realização das finalidades normativas; (iv) prever medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados e (v) prevenir a ocorrência de danos, consoante os parâmetros desenhados no direito comparado e no art. 6º da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18).”

Da decisão da Suprema Corte, extrai-se a existência de uma proteção constitucional baseada no direito à autodeterminação informativa. Em caso similar, o Tribunal Constitucional Alemão, entendeu que ser inconstitucional a legislação de recenseamento que não tinha parâmetros claros para o processo dos dados dos cidadãos daquele país:

“Assim declara o Tribunal que o processamento automático dos dados ameaçaria o poder do indivíduo em decidir por si mesmo se e como ele desejaria tornar públicos dados pessoais no sentido de que o processamento de dados possibilitaria a elaboração de um ‘quadro completo da personalidade’ por meio de ‘sistemas integrados sem que o interessado possa controlar o suficiente sua correção e aplicação’. Assim, aumentaria a influência do Estado sobre o comportamento do indivíduo, que não mais seria capaz de tomar decisões livres em virtude ‘da pressão psíquica da participação pública’. Uma sociedade, ‘na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação’, seria contrária ao direito à autodeterminação informativa, o que prejudicaria tanto a personalidade quanto o bem comum de uma sociedade democrática.” (MENDES, 2018, p. 188).

Surge, portanto, a ideia de um direito fundamental coletivo da proteção de dados: a autodeterminação informativa, a qual garante ao indivíduo o poder de determinação com relação à coleta e ao tratamento de seus dados pessoais (MENDES, 2018, p. 188). Em outras palavras,

“Nos termos do Tribunal Constitucional, o direito geral de personalidade baseia-se na ‘ideia da autodeterminação’, o que significa que: ‘o indivíduo deve basicamente [...] poder decidir por si mesmo como ele deseja se apresentar frente a terceiros ou ao público, se e em que medida terceiros podem dispor de sua personalidade; disto também faz especialmente parte a decisão de como ele quer se colocar em evidência com suas próprias palavras’.” (MENDES; FONSECA, 2020, p. 9).

A bem da verdade, é a autodeterminação informativa que consegue dar o escopo de proteção necessário à nova dinâmica de dados pessoais – especialmente, em um contexto cada vez mais complexo. No caso da disputa judicial entre IBGE e empresas de telecomunicação, faz-se necessário destacar do acórdão:

“A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do *habeas data* (art. 5º, LXXII), todos previstos na Constituição Federal de 1988. (...).

A força normativa da constituição pode e deve ser atualizada e reconceitualizada para preservar garantias individuais que constituem a base da democracia constitucional e que hoje são diretamente ameaçadas pelo descompasso entre o poder de vigilância e a proteção da intimidade. Embora as novas tecnologias de comunicação tenham se tornado condição necessária para a realização de direitos básicos – como se faz evidente no campo da liberdade de expressão, de manifestação política e de liberdade religiosa – verifica-se que esses mesmos avanços tecnológicos suscitam riscos generalizados de violação de direitos fundamentais básicos, para além da questão comunicacional.”

Existe debate a respeito da natureza de um direito fundamental à proteção de dados, se autônomo do direito à privacidade. Para além dessa discussão, é de se referir que, para fins penais, a proteção de dados pessoais, ao tentar dar limite à mencionada vigilância permanente, é de preocupação coletiva, não apenas do indivíduo. Para além de uma decisão que quebra o sigilo de determinada pessoa, a falta de proteção aos dados pessoais no sistema criminal expõe a riscos toda a sociedade, surgindo, assim como direito autônomo:

“Não há sobreposição, contudo, entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar uma dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão dos seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de

destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*) (cf. Hornung; Schnabel, 2009, p. 85-86). Dito de outro modo, 'a proteção de dados é, enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal' (cf. Spiecker, 2018, p. 55-56)." (SARLET; SAAVEDRA, p. 49).

Em tramitação no Congresso Nacional, a PEC 17/2019 busca agregar a autodeterminação informativa ao rol de direitos fundamentais, apresentando uma positivação que vai além da interpretação constitucional realizada pelo Supremo Tribunal Federal. Tanto a decisão do STF como a PEC apontam uma eficácia limitada do direito em contraposição a outros direitos fundamentais. Assim, seu reconhecimento pelo STF não impede o tratamento de dados, senão garante que isso se dê a partir de uma série de procedimentos e princípios que protegem a coletividade dos riscos associados ao tratamento massivo de dados pessoais.

Isso significa que a consolidação dos direitos fundamentais em matéria de proteção de dados e da privacidade tem avançado na jurisprudência nacional. Assim, até mesmo entendimentos acima demonstrados já passam por reformulações.

Recentemente, no julgamento do ARE 1.042.075, o Min. Gilmar Mendes abriu divergência para defender a tese de que o acesso a registro telefônico de celulares apreendidos com acusados depende de prévia decisão judicial, equiparando a proteção constitucional da inviolabilidade dos dados às das comunicações (VITAL, 2020). O mesmo é perceptível na decisão do HC 168.052⁴³, onde há uma assunção de uma mutação constitucional:

"Habeas corpus. (...) 2. Acesso a aparelho celular por policiais sem autorização judicial. Verificação de conversas em aplicativo WhatsApp. Sigilo das comunicações e da proteção de dados. Direito fundamental à intimidade e à vida privada. Superação da jurisprudência firmada no HC 91.867/PA. Relevante modificação das circunstâncias fáticas e jurídicas. Mutação constitucional. Necessidade de autorização judicial. 3. Violação ao domicílio do réu após apreensão ilegal do celular. 4. Alegação de fornecimento voluntário do acesso ao aparelho telefônico. 5. Necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação. 6. Ordem concedida para declarar a ilicitude das provas ilícitas e de todas dela derivadas." (HC 168052; Órgão julgador: Segunda Turma; Relator(a): Min. GILMAR MENDES; Julgamento: 20.10.2020; Publicação: 02.12.2020). Grifamos.

No inteiro teor do voto, o relator aponta para uma mudança no entendimento que interpreta a proteção constitucional do art. 5º, inc. XII, como apenas do fluxo comunicacional:

43. STF HC 168.052, 2ª T., rel. Min. Gilmar Mendes, j. 20.10.2020.

“No julgamento do HC 91.867/PA (Segunda Turma, de minha relatoria, DJe 20.9.2012), destaquei a diferença entre *comunicação telefônica* e *registros telefônicos*, os quais receberiam proteção jurídica distinta. Naquela oportunidade, defendi a impossibilidade de interpretar-se a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral, porquanto a proteção constitucional seria da comunicação, e não dos dados. Creio, contudo, que a *modificação das circunstâncias fáticas e jurídicas*, a promulgação de *leis posteriores* e o significativo *desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos smart phones* leva, nos dias atuais, à solução distinta. Ou seja, penso que se está diante de típico caso de *mutação constitucional*.”

Desse modo, percebe-se que, caso seja necessário a utilização de dados pessoais em investigações criminais, a autodeterminação informativa serve como limitadora, tal qual o direito à privacidade protege a inviolabilidade das comunicações, seguindo o voto do HC 168.052:

“No âmbito infraconstitucional, as normas do art. 3º, II, III; 7º, I, II, III, VII; 10 e 11 da Lei 12.965/2014 – o marco civil da internet – estabelecem diversas proteções à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da internet. A norma do art. 7º, III, da referida lei é elucidativa ao prever a inviolabilidade e sigilo das *comunicações privadas armazenadas (dados armazenados)*, *salvo por ordem judicial*. Percebe-se, portanto, que a legislação infraconstitucional avançou para possibilitar a proteção dos dados armazenados em comunicações privadas, os quais só podem ser acessados mediante prévia decisão judicial – matéria submetida à reserva de jurisdição. Entendo que o avanço normativo nesse importante tema da proteção do direito à intimidade e à vida privada deve ser considerado na interpretação do alcance das normas do art. 5º, X e XII, CF.”

Assim, avança-se na ideia de um reconhecimento da autodeterminação informativa no contexto da justiça criminal. No caso que vem acompanhando esse texto, da vereadora Marielle Franco e de Anderson Gomes, foi justamente o reconhecimento desse direito fundamental, no caso IBGE, que serviu como paradigma constitucional na análise de admissibilidade do Recurso Extraordinário. Assim a decisão monocrática:

“Compulsando-se os autos, verifica-se que a controvérsia cinge-se à questão do sigilo de dados telemáticos, com expressa interpretação do art. 5º, X e XII, da Constituição Federal pelo acórdão recorrido, para validar decisão judicial de invasão da privacidade de pessoas indefinidas, para fins de investigação criminal, na vigência do Marco Civil da internet (Lei 12.965/2014). Em tal caso, tendo em vista a óbvia repercussão geral da controvérsia e a constatação de encontrarem-se satisfeitos os requisitos formais extrínsecos e intrínsecos do recurso extraordinário, tem-se que a súplica está a merecer, da Suprema Corte, pronunciamento, com vistas à pacificação da questões constitucionais expressamente debatidas e julgadas. Aliás, em recente pronunciamento, o plenário do Supremo Tribunal Federal, referendou medidas cautelares, em diversas ADIs (6387

MC-Ref/DF, 6388 MC-Ref/DF, 6389 MC-Ref/DF, 6390 MC-Ref/DF e 6393 MC-Ref/DF), suspendendo a eficácia da Medida Provisória 954/2020 que dispõe sobre o compartilhamento de dados de empresas de telecomunicações prestadoras de serviço móvel pessoal.” (STJ, RE no RMS 60.698, rel. Min. Jorge Mussi, dec. mon., 23.10.2020).

Retornarmos, portanto, ao caso IBGE para compreender de que modo a autodeterminação informativa pode influenciar em decisões atinentes ao Direito Penal. Na decisão da ADI do IBGE, o voto de Gilmar Mendes atribui ao direito duas dimensões, subjetiva e objetiva:

“A dimensão subjetiva impõe que o legislador assuma o ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional. Nesse aspecto, a autodeterminação do titular sobre os dados deve ser sempre a regra, somente afastável de maneira excepcional. A justificativa constitucional da intervenção deve ser traduzida na identificação da finalidade e no estabelecimento de limites ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área. (...)”

Já em uma dimensão objetiva, a afirmação do direito fundamental à proteção de dados pessoais impõe ao legislador um verdadeiro dever de proteção (*Schutzpflicht*) do direito à autodeterminação informacional, o qual deve ser colmatado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (*Recht auf Organisation und Verfahren*) e normas de proteção (*Recht auf Schutz*).”

A dimensão subjetiva da autodeterminação informacional exsurge da própria ideia de devido processo legal, quando o STF reconhece a existência de um devido processo informacional. Ainda no voto do Min. Gilmar Mendes:

“É possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro ‘devido processo informacional’ (*informational due process privacy right*), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios.”

Em se tratando de 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. Isso porque a operação de tratamento de dados é também um processo que resulta em decisões (automatizadas ou não).

A ideia de um devido processo informacional diz respeito que esse processo decisório deve estar escrutinado por uma série de princípios e regras para que ele seja aceito e válido:

“Assim, o devido processo legal, para além de sua dimensão de ser um instrumento de garantias processuais em sede judicial (servindo de base para princípios como do juiz natural, inafastabilidade da jurisdição e todas demais garantias previstas pelo sistema processual), deve também ser entendido como uma ferramenta de assegurar a simetria e proporcionalidade de uma forma mais ampla. Tanto as relações indivíduo-estado, quanto as relações privadas em que há uma assimetria de poder devem ser permeadas pela garantia do devido processo, evitando que ações arbitrárias e intrusivas sejam tomadas sem que o sujeito tenha a capacidade de se defender. Essa capacidade vem sendo ameaçada com a adoção de sistemas de tomada de decisão automatizada, que, seja por razões técnicas (dificuldade de auditar uma decisão algorítmica que emprega técnicas de *machine-learning*, por exemplo), seja por razões jurídicas (proteção do segredo comercial ou industrial), levam a decisões que são determinantes para a vida do sujeito, sem que este possa ao menos saber os fatores que levaram àquela decisão, sendo mais difícil ainda uma eventual contestação do resultado.” (BIONI; MARTINS, 2020).

A complementação da autodeterminação se dá, justamente, com a criação de regras protetivas para os direitos de personalidade dos cidadãos, possibilitando a análise dos riscos efetivos do tratamento de dados, a partir de sua dimensão objetiva. Por essa razão, há uma discussão valorativa com relação a normas protetivas da *internet* (no Brasil, a LGPD e o Marco Civil da Internet de maneira principal): elas podem ser entendidas não apenas como normas no sentido de regras (em seu aspecto de norma infraconstitucional), senão também de princípios⁴⁴. Esse o entendimento presente no voto de Gilmar Mendes:

“Ao mesmo tempo em que todas essas iniciativas normativas não implicam formalmente alterações dos textos constitucionais, elas consagram materialmente categorias de direitos, princípios e normas de governança para a *internet*, limitando drasticamente o poder de autoridades públicas e de atores privados nas suas relações com os usuários.”

O voto do ministro indica que as legislações protetivas da *internet* teriam um *status* protoconstitucional, ao citar estudo que defende a existência de um constitucionalismo digital (GILL et al., 2015) a partir de iniciativas de proteção dos usuários, muitas vezes representadas por leis como o MCI e a LGPD.

44. Adotada aqui a classificação em Ávila (2011, p. 194).

Uma crítica que poderia ser feita aos argumentos aqui trazidos é que, ao utilizarmos a LGPD como fonte de direito em diversos momentos (na conceituação de dado pessoal, por exemplo), estaríamos ferindo vedação expressa da própria legislação:

“Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...) III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (...) § 1º O tratamento de dados pessoais previsto no inciso III 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. (...) § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.”

A partir da compreensão de que as leis de proteção de dados assumem também uma dimensão de princípio, pois permitem dar sentido a direitos fundamentais reconhecidos pelo STF, a LGPD aparece como suporte para a proteção de dados em matéria penal. Essa nos parece a leitura adequada da diretiva do § 1º: o dispositivo indica a necessidade de legislação específica, mas já a condiciona a princípios que ela sustenta, os quais estão intrinsicamente ligados a uma ideia de autodeterminação informativa.

No mesmo sentido, deverão se dar as opiniões técnicas da Agência Nacional de Proteção de Dados previstas pelo § 3º. Sabe-se que a autoridade brasileira para centralizar os temas de proteção de dados foi, recentemente, criada e terá muito trabalho pela frente. Há de se monitorar como a Agência Nacional de Proteção de Dados irá se portar, especialmente, no tema da autodeterminação dos dados.

Assim, a LGPD reivindica-se enquanto limite principiológico, apontando diretrizes para futuras legislações e atos administrativos na matéria. Em havendo reconhecimento do caráter constitucional desses princípios pelo STF, acredita-se que eles devem ser aplicados em matéria penal, servindo, portanto, como balizador de decisões que influem na utilização de dados pessoais em matéria penal. De qualquer sorte, a aplicação pacífica do Marco Civil da Internet em matéria penal deveria apontar para o mesmo caminho, na medida que também fundada na autodeterminação informativa, bem como pelos brevemente citados no art. 3º, inc. II e III e no art. 7º e seguintes da legislação, que conferem o mesmo ideal protetivo e principiológico (já apontamos que a jurisprudência do STJ entende de maneira contrária).

A opção de compreender a LGPD como aplicável para os casos se dá em razão de que se trata de legislação mais apropriada para auxiliar na concretização da autodeterminação informacional em casos que o artigo apresenta como problema. Dessa forma, para que seja possível o tratamento de dados em matéria penal, ainda que sem a aprovação de matéria específica, nos parece que o rol de princípios constantes do art. 6º da LGPD deve ser observado como fator de ponderação nas decisões que autorizam o tratamento de

dados em investigações criminais⁴⁵. Não é por acaso que também o art. 6º do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal adota esses princípios como a serem observar na aplicação da lei. Compartilhando de nossa conclusão:

“Esses bancos de dados precisarão respeitar os princípios gerais de proteção e os direitos do titular previstos na LGPD. Os referidos princípios encontram-se arrolados no art. 6º. Como decorrência da aplicação desses princípios, as polícias devem garantir, por exemplo, livre acesso e consulta sobre a forma e a duração do tratamento de dados, bem como sobre quais dados estão sendo manipulados (art. 6º, IV). Ademais, ainda serão observados os direitos do titular previstos na LGPD.” (ASSUNÇÃO E SILVA, 2019, p. 78).

Já há outras pesquisas no tema que também auxiliam no ponto aqui debatido⁴⁶:

“Pode-se afirmar que, da mesma forma que os princípios da LGPD são aplicados ao tratamento de dados autorizados por ela, os princípios constitucionais da dignidade humana, da proporcionalidade, da autodeterminação informativa e os direitos da intimidade e da vida privada devem ser aplicados no tratamento e custódia de dados pessoais excluídos pela LGPD. As decisões formalizadas na ADI n. 6.387 e na ADPF n. 722 demonstram que o STF entende que o tratamento de dados pessoais por

45. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

46. Da mesma forma: DOMINGOS et al., 2020, p. 160; ASSUNÇÃO E SILVA, 2019, p. 76, entre outros que já argumentam no mesmo sentido.

parte do Estado, mesmo nas hipóteses excluídas pela LGPD, submete-se aos princípios constitucionais já explicitados pela própria estrutura do estado democrático de direito que experimenta o Brasil desde a promulgação da Constituição Federal de 1988. Nesse sentido, legislações anteriores e posteriores à LGPD que vinculem a captação, o tratamento e o compartilhamento de dados pelo Estado ao gestor de dados, sem levar em consideração, principalmente, os princípios da proporcionalidade e da autodeterminação informativa, devem ser interpretados na conformidade constitucional, sob pena de servirem como dados de Troia para a democracia.” (TOCSHI; LOPES, 2020, p. 113).

Abreu e Antonialli (2017) utilizam como referência os “13 Princípios Internacionais sobre a aplicação de Direitos Humanos à Vigilância das Comunicações, elaborados por uma coalizão global de especialistas em privacidade e tecnologia da sociedade civil” (p. 54)⁴⁷, que em muito se assemelham aos trazidos por nós e podem auxiliar na aplicação dos princípios da LGPD.

As organizações da sociedade civil que debatem a temática de proteção de dados oferecem importantes contribuições ao debate, apresentando documentos importantes que auxiliam na compreensão das questões aqui colocadas. De maneira especial, recomenda-se a leitura de Notas Técnicas que tratam do Anteprojeto de Lei de Proteção de dados para segurança pública e persecução penal realizadas pelo Laboratório de Políticas Públicas da Internet (LAPIN) e pela Associação Data Privacy Brasil de Pesquisa⁴⁸.

Em suma, remetendo-se ao problema do presente artigo: dos limites jurídicos para o tratamento de dados pessoais em investigações criminais, acreditamos que ele deve se dar por decisões judiciais que têm como limite o direito à autodeterminação informativa, cujo sentido se dá pelos princípios acima elencados.

O significado de adotar a seguinte direção é que os princípios básicos da LGPD são aqueles que fornecem a garantia de que o tratamento dos dados se dará seguindo essa espécie de teste (os propósitos do tratamento são legítimos? [inc. I] adequados? [inc. II]; são necessários? [inc. III] e assim por diante).

Sabemos, também, que a resposta que trazemos aqui é mais diretiva do que definitiva, até porque ainda há muitas questões em aberto tanto em decisões judiciais quanto na evolução legislativa. O significado de aplicar esses princípios dentro dos juízos de valorização do direito penal exige, sem dúvida, um esforço próprio. No entanto, os diversos estudos na matéria de proteção de dados, utilizados para outros âmbitos da tutela administrativa e jurisdicional, já nos auxilia em prestar uma melhor defesa dos direitos constitucionais, face à ausência de regulamentação específica da matéria.

47. Os princípios estão disponíveis no site da organização: Disponível em: [<https://necessaryandproportionate.org/principles>]. Último acesso em: 28.03.2021.

48. REIS et al., 2021 e BIONI et al., 2021.

5. CONSIDERAÇÕES FINAIS

Partindo-se do problema sobre quais eram os limites jurídicos para o tratamento de dados pessoais em investigações criminais, com uma metodologia hipotético-dedutiva, confirmou-se a hipótese inicial, a saber, a existência de um conjunto de normas que limita o tratamento de dados penais no Brasil. As conclusões a que se chegou foram as seguintes:

(i.) Há um conceito de “dado pessoal” expansionista no direito brasileiro, consagrado pelo Marco Civil da Internet, pela LGPD, bem como de *status* constitucional já reconhecido pelo STF.

(ii.) Ainda assim, doutrina e jurisprudência do direito penal brasileiro se utilizam de uma definição reducionista de dado pessoal, utilizando termos como “dado registral” para afastar a proteção constitucional da privacidade e da intimidade. Tal opção tem origem no entendimento de que a proteção constitucional do art. 5º, XII, CF é do fluxo comunicacional, o qual já apresenta sinais de superação (HC 168.052). A opção por esse conceito pode gerar uma expansão da persecução penal que fere princípios basilares do direito penal.

(iii.) Com uma breve revisão bibliográfica, buscamos apresentar os riscos do tratamento massivo de dados pessoais por algoritmos em questões relacionadas à segurança pública.

(iv.) A partir da decisão do caso IBGE, o STF consagrou a tese de que a autodeterminação informativa é um direito fundamental; devendo, também, ser aplicado na justiça criminal.

(v.) Para dar sentido ao direito à autodeterminação informativa, deve-se levar em consideração sua dimensão subjetiva (devido processo informacional, derivado do devido processo legal) e objetiva (adequação principiológica da LGPD).

(vi.) O tratamento de dados pessoais em investigações criminais deve, portanto, ser sempre autorizada por decisão judicial fundamentada, a qual deve sopesar os princípios encartados no art. 6º da LGPD, estabelecendo parâmetros protetivos para a utilização de dados pessoais no âmbito criminal.

(vii.) O artigo não adentra na discussão a respeito de como esses princípios devem ser aplicados no caso concreto; no entanto, o estudo de proteção de dados no Brasil já fornece sólidas bases para a compreensão de como esses princípios devem ser aplicados.

(viii.) Por questões metodológicas, entendemos por não analisar a fundo o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, tendo em vista que o objetivo era identificar os atuais mecanismos de proteção a dados pessoais em investigações criminais. O próprio objetivo da pesquisa traz à tona a urgência de uma legislação de proteção de dados, à intimidade e à vigilância. Assim o Anteprojeto se apresenta como importante iniciativa legislativa, sendo imprescindível o debate público em torno da matéria.

(ix.) Partimos da premissa, ainda na introdução, de que o tratamento de dados em investigações penais é ferramenta atual e necessária para investigações criminais. Os próprios limites que aqui trazemos possibilitam ao Brasil uma maior cooperação internacional com outras agências de segurança, como a exposição de motivos do referido Anteprojeto bem explica.

6. REFERÊNCIAS BIBLIOGRÁFICAS

- ABREU, Jacqueline de Souza. *O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?* Publicado em 8.7.2016. Disponível em: [www.jota.info/opiniao-e-analise/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro-08072016]. Último acesso em: 21.03.2021.
- ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais*. 2. ed. São Paulo: InternetLab, 2017.
- ABREU, Jacqueline de Souza; ANTONIALLI, Dennys; MASSARO, Heloísa; LUCIANO, Mari. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. In: *Revista Brasileira de Ciências Criminais*, São Paulo, v. 154, p. 177-214, 2019.
- ABRUSIO, Juliana; CAMPOS, Ricardo; KETTEMANN, Mathias; WITTNER, Florian. *Vigilância em massa ou combate à desinformação: o dilema do rastreamento*. Publicado em 4 ago. 2020. Disponível em: [www.conjur.com.br/2020-ago-04/direito-digital-dilema-rastreamento-pl-fake-news]. Último acesso em: 20.03.2021.
- ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. *Machine Bias*. Publicado em 23 de maio de 2016. Disponível em: [www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing]. Último acesso em: 21.03.2021.
- ANTONIALLI, Dennys; FRAGOSO, Nathalie; MASSARO, Heloisa Maria Machado. Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime. In: *Boletim do IBCCrim*, São Paulo, ano 27, n. 318, edição especial, maio 2019.
- ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. *Rastreabilidade, metadados e direitos fundamentais: Nota Técnica sobre o projeto de Lei 2630/2020*. Publicado em 24 jul. 2020. Disponível em: [www.dataprivacybr.org/wp-content/uploads/2020/07/Data-Privacy-Brasil.-Rastreabilidade-e-Direitos-Fundamentais.-PL-2630.2020.pdf]. Último acesso em: 21.03.2021.
- ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). *Retrospectiva:*

- Tecnoautoritarismo. Publicado em 2020. Disponível em: [<https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf>]. Último acesso em: 20.03.2021.
- ASSUNÇÃO E SILVA, Alexandre. A Proteção de Dados Pessoais nas atividades de investigação e repressão de infrações penais publicado em Brasil; Ministério Público Federal. In: *Sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados*. Brasília: MPF, 2019.
- ÁVILA, Humberto. *Teoria dos princípios: da definição à aplicação dos princípios jurídicos*. São Paulo: Malheiros Editores, 2011.
- BIONI, Bruno Ricardo. *Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil*. São Paulo: Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI-USP), 2016.
- BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. In: *Revista do Advogado*, São Paulo, n. 144, p. 22-32, nov. 2019.
- BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. GenForense: Rio de Janeiro, 2020.
- BIONI, Bruno Ricardo; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. *Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020. Disponível em: [www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-TÉCNICA-PROTEÇÃO-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURANÇA-PÚBLICA-VF-31.11.2020.pdf]. Último acesso em: 25.03.2021.
- BIONI, Bruno Ricardo; MARTINS, Pedro. *Devido processo informacional: um salto teórico-dogmático necessário?* Publicado em 15.07.2020. Disponível em: [www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020]. Último acesso em: 20.03.2021.
- BIONI, Bruno Ricardo; ZANATTA, Rafael. *Levando os metadados a sério*. Publicado em 13.08.2020. Disponível em: [www.conjur.com.br/2020-ago-13/bioni-zanatta-levando-metadados-serio]. Último acesso em: 27.03.2021.
- BOGARD, William. Simulation and post-panopticism. In: David Lyon, Kevin D. Haggerty and Kirstie Ball (Coord.). *Routledge handbook of surveillance studies*. Nova Iorque: Routledge, 2012.
- CEYHAN, Ayse. Surveillance as biopower. In: David Lyon, Kevin D. Haggerty and Kirstie Ball (Coord.). *Routledge handbook of surveillance studies*. Nova Iorque: Routledge, 2012.

- CHRISTIE, Nils. *A indústria do controle do crime*. Trad. Luís Leiria. Rio de Janeiro: Forense, 1998.
- CORTE EUROPEIA DE JUSTIÇA. Acórdão de 19 de outubro de 2016, C-582/14. *Patrick Breyer v. Bundesrepublik Deutschland*. Disponível em: [<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582>]. Último acesso em: 18.03.2021.
- DIETER, Maurício Stegemann. *Política criminal atuarial: a criminologia do fim da história*. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade Federal do Paraná: 2012.
- DOMINGOS, Fernanda Teixeira et al. Transferência internacional de dados pessoais para fins de investigações criminais à luz das Leis de Proteção de Dados Pessoais em Associação Nacional dos Procuradores da República. In: Ministério Público Federal; ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (Orgs.). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, 2020.
- DOMINGOS, Pedro. *O algoritmo mestre: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo*. São Paulo: Novatec, 2017.
- EILBERG, Daniela Dora; SANTOS, Jádía Larissa Timm. Velhos preconceitos mascarados de verdades científicas: como a inteligência artificial. In: GONZÁLEZ, Javier García; LOZANO, Álvaro Alzina; RODRÍGUEZ, Gabriel Martín (Orgs.). *El derecho público y privado ante las nuevas tecnologías*. Madrid: Editorial Dykinson, 2020.
- ELESBÃO, Ana Clara Santos; TIMM, Jádía Larissa; MEDINA, Roberta. Quando as Máscaras (do reconhecimento facial) caírem, será um grande carnaval. In: AMARAL, Augusto Jobim do; SALES, Eduardo Baldissera Carvalho (Orgs.). *Algoritmos*. São Paulo: Tirant lo Blanch, 2020.
- ELMASRI, Ramez; NAVATHE, Sham. *Sistemas de banco de dados*. São Paulo: Pearson Addison Wesley, 2011.
- FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. In: *Revista da Faculdade de Direito*, São Paulo, Universidade de São Paulo, n. 88, p. 439-459, 1993.
- FERGUSON, Andrew Guthrie. *The rise of big data policing: surveillance, race, and the future of law enforcement*. Nova Iorque: New York University Press, 2017a.
- FERGUSON, Andrew Guthrie. The Police Are Using Computer Algorithms to Tell If You're a Threat. Publicado em 3 out 2017b. Disponível em: [<https://time.com/4966125/police-departments-algorithms-chicago/>]. Último acesso em: 25.03.2021.
- FOUCAULT, Michel. *Vigiar e punir: história da violência nas prisões*. Trad. Raquel Ramalhete. Petrópolis: Rio de Janeiro, 2010.

- GAMBETTI, Zeynep. *Agir em tempos sombrios*. Trad. Christiane Amoretti et al. Porto Alegre: Criação Humana, 2019.
- GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights (November 9, 2015). Publicado em Berkman Center Research Publication N. 2015-15. Disponível em: [http://dx.doi.org/10.2139/ssrn.2687120]. Último acesso em: 20.03.2021.
- GRECO, Luís. *Poder de julgar sem responsabilidade de julgador: a impossibilidade jurídica do juiz-robô*. São Paulo: Marcial Pons, 2020.
- LORENZETTI, Ricardo Luis. *Teoria da decisão judicial: fundamentos de direito*. Trad. Buno Miragem. São Paulo: Ed. RT, 2009.
- LYON, David. *The electronic eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press, 1994.
- MENDES, Laura Schertel. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. In: *Direitos Fundamentais & Justiça*, Porto Alegre, n. 39, 2018.
- MENDES, Laura Schertel; FONSECA, Gabriel. STF reconhece Direito Fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. In: *Revista do Direito do Consumidor*, São Paulo, v. 130, 2020.
- NI LOIDEAIN, Nora. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. In: Special Issue on Surveillance: Critical Analysis and Current Challenges University of Cambridge Faculty of Law Research Paper: 2015. Disponível em: [https://ssrn.com/abstract=2613424]. Último acesso em: 13.12.2020.
- O'MALLEY, Pat. *Riesgo, neoliberalismo y justicia penal*. Buenos Aires: Ad-Hoc, 2006.
- O'NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Londres: The Crown Publishing Group, 2016.
- PARLAMENTO EUROPEU. Conselho Da União Europeia. *Regulamento Geral de Proteção de Dados* 2016/679. União Europeia: Jornal Oficial da União Europeia, 2016. Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT]. Último acesso em: 27.01.2021.
- QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Perdigoni. Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. In: *Internet & sociedade*, n. 1, v. 1. p. 64 a 90, fev. 2020.
- REIS, Carolina; COSTA, Eduarda; SILVA, Felipe; BAWDEN, Henrique; LARANJEIRA DE PEREIRA, José Renato; SARMENTO, Paulo. *Nota técnica sobre o anteprojeto de lei de proteção de dados para a segurança pública e investigação criminal*. Laboratório de Políticas Públicas e Internet (LAPIN). Março de 2021. Disponível em: [https://lapin.org.br/wp-content/uploads/2021/03/NT_AP-

- J-para-Seguranca-Publica-e-Investigacao-Criminal.pdf]. Último acesso em: 25.03.2021.
- SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à Proteção de Dados Pessoais. In: Assunto Especial. *RDP, Brasília*, v. 17, n. 93, 58-81, maio-jun. 2020. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias.
- SOUZA, Ramon. *Investigamos! Tudo o que você queria saber sobre o vazamento de 220 milhões de CPFs*. Publicado em 1º fev. 2021. Disponível em: [https://thehack.com.br/investigamos-tudo-o-que-voce-queria-saber-sobre-o-vazamento-de-220-milhoes-de-cpfs/]. Último acesso em: 28.03.2021.
- TOSCHI, Aline Seabra; LOPES Herbert Emílio Araújo. Dados de Troia. In: Associação Nacional dos Procuradores da República; Ministério Público Federal; ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (Orgs.). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, 2020.
- TOVO, Antonio. *O periculosômetro digital?* Notas sobre o uso de algoritmos e de inteligência artificial no sistema penal. Publicado em 6 jan. 2019. Disponível em: [www.jota.info/opiniao-e-analise/artigos/o-periculosometro-digital-06012019?amp]. Último acesso em: 12.03.2021.
- VITAL, Danilo. STF suspende julgamento sobre violação de sigilo de celular de suspeito. Publicado em 9.11.2020. Disponível em: [www.conjur.com.br/2020-nov-09/stf-suspende-julgamento-violacao-sigilo-celular]. Último acesso em: 10.03.2021.
- WACQUANT, Loïc. *As prisões da miséria*. Trad. André Telles. Rio de Janeiro: Zahar Ed., 2001.
- WEISENBAUM, Joseph. *Computer and Human Reason: from judgment to calculation*. Nova Iorque: W. H. Freeman & Co, 1976.
- WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Interceptação Telemática de contas do Whatsapp: Bilhetagem – Extrato De Mensagens – Versão 2019.4. In: JORGE, Higor Vinicius Nogueira (Coord.). *Tratado de Investigação Criminal Tecnológica*. Salvador: Editora JusPodivm, 2021.
- ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Nova Iorque: Publicaffairs, 2019.

6.1. Jurisprudência

- SUPERIOR TRIBUNAL DE JUSTIÇA, AgRG no RMS 63.041, rel. Min. Ribeiro Dantas, 5ª T., j. 17.11.2020.
- SUPERIOR TRIBUNAL DE JUSTIÇA, RMS 60.698, rel. Min. Rogerio Schietti Cruz, 3ª S., j. 26.8.2020.

SUPREMO TRIBUNAL FEDERAL, STF, HC 168.052, 2ª T., rel. Min. Gilmar Mendes, j. 20.10.2020.

SUPREMO TRIBUNAL FEDERAL, ADIs 6.387; 6.388; 6.389; 6.390; 6.393, Plenário, rel. Min. Rosa Weber, j. 06 e 70.05.2020.

SUPREMO TRIBUNAL FEDERAL, HC 91.867/PA, rel. Min. Gilmar Mendes, j. 20.09.2012.

6.2. Legislação

BRASIL. *Constituição da República Federativa do Brasil*, de 1988. Disponível em: [www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm]. Último acesso em: 20.03.2021.

BRASIL. Lei 12.850, de 02 de agosto de 1989. *Lei de Organizações Criminosas*. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm]. Último acesso em: 20.03.2021.

BRASIL. Lei 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Último acesso em: 20.03.2021.

BRASIL. Lei 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados*. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm]. Último acesso em: 20.03.2021.

BRASIL. Lei 9.296, de 24 de julho de 1996. *Lei de interceptações telefônicas*. Disponível em: [www.planalto.gov.br/ccivil_03/leis/l9296.htm]. Último acesso em: 20.03.2021.

BRASIL. Lei 9.613, de 03 de março de 1998. *Lei da Lavagem de Dinheiro*. Disponível em: [www.planalto.gov.br/ccivil_03/leis/l9613.htm]. Último acesso em: 20.03.2021.

CÂMARA DOS DEPUTADOS, 2020. *Projeto de Lei 2.630/2020*. Disponível em: [www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735]. Último acesso em: 23.03.2021.

CÂMARA DOS DEPUTADOS, 2020. *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*. Disponível em: [www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/ou-tros-documentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf]. Último acesso em: 18.03.2021.

PESQUISAS DO EDITORIAL

Veja também Doutrinas relacionadas ao tema

- A política do policiamento preditivo: pressupostos criminológicos, técnicas algorítmicas e estratégias punitivas, de Daniel Edler Duarte e Luisa Cruz Lobato – *RBCCrim* 183/57-98;
- *Blockchain* como mecanismo de criminal *compliance* à luz da lei 13.709/2018, de Décio Franco David e Bruno Henrique Zanette Minski – *RDPEC* 5/71-97;
- Inteligência artificial, *big data* e algoritmos: policiamento e as novas roupagens de um agir discriminatório, de Rodrigo Ghiringhelli de Azevedo e Luiza Correa de Magalhães Dutra – *RBCCrim* 183/247-268; e
- Justiça criminal negociada como resposta penal alternativa, de Leonardo Dantas Milhomem e Antonio Henrique Graciano Suxberger – *RePro* 318/51-74.