

**INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA - IDP
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA - EDAP
GRADUAÇÃO EM DIREITO**

ANDRÉ LUÍS FALCÃO DA GAMA MARTINS CARVALHO

**A PROTEÇÃO NORMATIVA DOS DADOS PESSOAIS CARECE DE
TUTELA PENAL?
A PROPORCIONALIDADE DA CRIMINALIZAÇÃO DO
COMPARTILHAMENTO INDEVIDO DE DADOS PESSOAIS**

BRASÍLIA - DF

2021

ANDRÉ LUÍS FALCÃO DA GAMA MARTINS CARVALHO

**A PROTEÇÃO NORMATIVA DOS DADOS PESSOAIS CARECE DE
TUTELA PENAL?
A PROPORCIONALIDADE DA CRIMINALIZAÇÃO DO
COMPARTILHAMENTO INDEVIDO DE DADOS PESSOAIS**

Trabalho de Conclusão de Curso apresentado como requisito para a conclusão da graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP.

Orientador: Prof. Dr. Guilherme Pereira Pinheiro

BRASÍLIA - DF

2021

ANDRÉ LUÍS FALCÃO DA GAMA MARTINS CARVALHO

**A PROTEÇÃO NORMATIVA DOS DADOS PESSOAIS CARECE DE
TUTELA PENAL?
A PROPORCIONALIDADE DA CRIMINALIZAÇÃO DO
COMPARTILHAMENTO INDEVIDO DE DADOS PESSOAIS**

Trabalho de Conclusão de Curso apresentado como requisito para a conclusão da graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP.

Orientador: Prof. Guilherme Pereira Pinheiro.

Brasília - DF, 2 de julho de 2021.

Professor Dr. Guilherme Pereira Pinheiro
Membro da Banca Examinadora

Professora Dra. Miriam Wimmer
Membro da Banca Examinadora

Professor Me. Alexandre Sankievicz
Membro da Banca Examinadora

**A PROTEÇÃO NORMATIVA DOS DADOS PESSOAIS CARECE DE
TUTELA PENAL?
A PROPORCIONALIDADE DA CRIMINALIZAÇÃO DO
COMPARTILHAMENTO NÃO AUTORIZADO DE DADOS PESSOAIS¹**

André Luís Falcão da Gama Martins Carvalho²

Orientador: Prof. Dr. Guilherme Pereira Pinheiro³

SUMÁRIO: Introdução; Desenvolvimento: 1. O direito fundamental à proteção de dados pessoais em meio ao tratamento massivo de dados pessoais na sociedade da informação do século XXI; 2. O mandado de criminalização decorrente do dever constitucional objetivo de proteção do direito fundamental à proteção de dados pessoais; 3. A tutela penal a partir do regime jurídico do direito fundamental à proteção de dados pessoais; Conclusão; Referências.

RESUMO: Este trabalho visa defrontar a insuficiência de proteção efetiva da dignidade humana presente nos dados pessoais por parte do ordenamento jurídico em vigor no Brasil, consoante pesquisa bibliográfica exploratória. A explicitação da origem e dos limites do direito à privacidade e a constatação da existência de um direito fundamental à proteção de dados pessoais, balizador da construção de uma rede infraconstitucional de proteção e controle dos dados pessoais pelo seu titular, conduziram à necessidade de se utilizar do dever constitucional de proteção de dados pessoais possibilitado pela análise da dimensão objetiva dos direitos fundamentais. Inúmeros casos de violação da privacidade individual demonstraram a necessidade de uso do potencial de coerção jurídica propiciado pela intervenção do Direito Penal para a proteção do titular de dados pessoais. Diante disso, a partir da Constituição de 1988, utilizou-se do mandado criminalizador de qualquer discriminação atentatória do direito fundamental à privacidade do titular de dados pessoais para a sugestão de um tipo penal consistente na proibição de conduta resultante no tratamento indevido de dados pessoais, isto é, sem o consentimento específico ou em desconformidade com a finalidade determinada para a qual o uso dos dados pessoais foi consentido.

Palavras-chave: direitos fundamentais; dados pessoais; mandado de criminalização; tutela penal; proporcionalidade.

ABSTRACT: This work aims to confront the insufficiency of effective protection of human dignity present in personal data by the legal system in force in Brazil, according to exploratory bibliographic research. The explanation of the origin and limits of the right to privacy and the solid verification of the existence of a fundamental right to the protection of personal data, which is the basis for the construction of an infra-constitutional network for the protection and

¹ Artigo Científico apresentado à disciplina Trabalho de Conclusão de Curso II, da Graduação em Direito.

² Aluno da graduação em Direito, bacharel em Comunicação Social, pós-graduado em Relações Institucionais e em Direito Penal e Processo Penal. E-mail: andrefalcaocarvalho@gmail.com.

³ Orientador: professor no IDP, pós-doutor em Direito e Democracia, advogado, consultor legislativo na Câmara dos Deputados, <http://lattes.cnpq.br/7086001928425929>, guilherme.pinheiro@idp.edu.br.

control of personal data by the holder, led to the need to use the constitutional duty to protect personal data made possible by the analysis of the objective dimension of fundamental rights. Countless cases of violation of individual privacy have demonstrated the high potential for legal coercion provided by the intervention of Criminal Law for the protection of the holder of personal data. Therefore, as from the 1988 Constitution, the criminalization warrant was used to criminalize any discrimination that undermines the fundamental right to privacy of the holder of personal data for the suggestion of a criminal type consisting of the prohibition of conduct resulting in the improper treatment of personal data, that is , without specific consent or in disagreement with the determined purpose for which the use of personal data was consented.

KEYWORDS: fundamental rights; personal data; criminalization warrant; criminal protection; proportionality.

INTRODUÇÃO

A existência de um direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro parte da hermenêutica de dispositivos da Constituição Federal de 1988 (CF), desassociando-o da proteção do fluxo comunicacional. Seu reconhecimento na esfera jurídica brasileira tem se demonstrado premente diante da escalada de violações à privacidade dos dados pessoais, largamente tratados ora sem a autorização do titular dos dados, e até sem seu conhecimento, ora em desacordo com o consentimento dado por ele.

O mero elenco de direitos subjetivos dos titulares de dados pessoais na legislação civil e administrativa tem se mostrado insuficiente para a tutela do direito fundamental à proteção de dados pessoais. Desse modo, é imperioso proteger tal direito no Brasil com maior coerção jurídica, que não se adstrinja apenas a sanções pecuniárias, visto se tratar de um direito individual elementar aos seres humanos e cuja finalidade é resguardar a privacidade dos indivíduos, sobretudo em meio à constante evolução tecnológica vivida no século XXI que possibilita uma exposição massiva das informações pessoais.

Ver-se-á que a construção doutrinária da justificativa da existência e substância do direito fundamental à proteção de dados pessoais está umbilicalmente ligada ao gigantesco avanço da capacidade de processamento de dados propiciado pelo desenvolvimento das tecnologias de informação e comunicação (TIC), intensificado durante o século XX e aperfeiçoado no século atual. Essa circunstância será posta como elemento fulcral motivador do fortalecimento da proteção jurídica do titular dos dados pessoais, em virtude da violação ao princípio da proibição de proteção deficiente do direito fundamental à proteção de dados pessoais.

Com efeito, avolumam-se as ocasiões noticiadas onde se vê a utilização de dados pessoais para finalidades jamais imaginadas pelos titulares e, por vezes, ilícitas. A observância de tais fatos relativos à comercialização e ao compartilhamento indevido revela as inúmeras violações que ocorrem a vários direitos fundamentais (liberdades públicas, igualdade material, privacidade, proteção de dados pessoais etc.). Elas tendem a crescer com o avanço da capacidade tecnológica de tratamento de dados pessoais em massa em um mundo hiperconectado.

Como início da configuração de uma solução que proveja maior tutela jurídica ao direito fundamental à proteção de dados pessoais, colher-se-á da Constituição de 1988 e da dimensão objetiva dos direitos fundamentais um dever objetivo de ação estatal para

proteger o direito fundamental à proteção de dados pessoais de maneira eficaz por meio do mandado de criminalização. Assim, uma das tentativas de solucionar a questão pode se dar por meio da instituição de uma tutela penal que seja adequada, necessária e proporcional à luz dos princípios do Direito Penal. Para tanto, utilizar-se-á da pesquisa exploratória, bibliográfica e documental, de abordagem qualitativa e quantitativa na apresentação do conteúdo encontrado nas fontes bibliográficas.

1 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS EM MEIO AO TRATAMENTO MASSIVO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO DO SÉCULO XXI

A concepção de um direito fundamental à proteção de dados pessoais, com autonomia diante do direito fundamental à privacidade, surge a partir da tutela da personalidade humana em face do avanço tecnológico, catalisador do tratamento massivo de informações pessoais. O contínuo progresso da informática possibilitou o aprimoramento da capacidade de as máquinas processarem dados, correlacionando-os, a fim de se tornarem funcionais para diversos fins. A potencialização dessas atividades, que alcançou dimensão incomparável a momentos pretéritos, terminou por ocasionar na fragilidade da proteção jurídica à privacidade dos indivíduos (TADEU, 2011; GUARDIA, 2020).

Sob essa ótica, para compreender a razão de se constatar a presença de um direito fundamental à proteção de dados pessoais na ordem jurídica nacional, é preciso entender sua efetiva função e real necessidade. Para tal, importa conhecer a abrangência da ampla gama de possibilidades geradas por meio do tratamento massivo de informações vivenciado na Sociedade da Informação⁴ do século XXI.

A atividade de processamento de informações pessoais é utilizada, basicamente, para armazenar, categorizar, classificar ou correlacionar dados de clientes, pacientes,

⁴ Essa expressão passou a ser usada em substituição a “sociedade pós-industrial”, cujo processo de resignificação é explicado com profundidade por Castells (2005, p. 32): “A virada fundamental data, talvez, dos anos 70. O desenvolvimento e a comercialização do microprocessador (unidade de cálculo aritmético e lógico localizada em um pequeno chip eletrônico) dispararam diversos processos econômicos e sociais de grande amplitude. Eles abriram uma nova fase na automação da produção industrial: robótica, linhas de produção flexíveis, máquinas industriais com controles digitais etc. Presenciaram também o princípio da automação de alguns setores do terciário (bancos, seguradoras). Desde então, a busca sistemática de ganhos de produtividade por meio de várias formas de uso de aparelhos eletrônicos, computadores e redes de comunicação de dados aos poucos foi tomando conta do conjunto das atividades econômicas. Esta tendência continua em nossos dias.”

contribuintes, eleitores, usuários, passageiros, moradores etc. A partir daí, o controlador dos dados, costumeiramente uma instituição privada ou pública, utilizará da forma de tratamento adequada que o auxilie no alcance da finalidade da existência da organização e dos correspondentes objetivos traçados por ela, seja para promover a venda de produtos e serviços, criar novos, seja para a divulgação de ideias e conteúdos de diversos tipos (MATTIUZZO, 2014; ESTRADA, 2016).

Isso só é possível porque a posse dos dados pessoais propicia a identificação de características e gostos pessoais capazes de formar um retrato completo do indivíduo a partir de informações que, se analisadas separadamente, não se prestariam a qualquer fim (PASSI; TEIXEIRA, 2018)⁵. A presença de aparelhos eletrônicos capazes de produzir tais informações no cotidiano das pessoas é cada vez maior, vide a disseminação dos computadores multifuncionais não apenas nos lares familiares, mas em todos os âmbitos da sociedade, na forma de celulares, relógios, câmeras, *tablets*, *chips* e demais dispositivos móveis⁶.

Assim, tornou-se possível a coleta de dados pessoais sobre os hábitos dos indivíduos que antes ficavam restritos apenas a ele ou às pessoas mais próximas. Como Fernandes e Oliveira (2020) demonstram, o que antes fazia parte da privacidade das pessoas, hoje é utilizado para a produção de novos produtos no mercado, oferta de serviços personalizados, monitoramento da segurança pública, gerência do funcionamento de uma empresa etc.

Paralelamente à observação das potencialidades do desenvolvimento tecnológico no funcionamento da economia de mercado, notou-se um certo aumento da atenção da doutrina jurídica e dos Tribunais brasileiros às proteções possibilitadas ao indivíduo pela ordem jurídica, sobretudo de matriz constitucional. A preocupação da Carta Maior de 1988 de agasalhar o fenômeno da informação é visível na leitura dos dispositivos que abarcam a tutela dos atributos da personalidade humana (honra, imagem, vida privada e intimidade: art. 5º, X, CF), a garantia das liberdades públicas de comunicação (expressão,

⁵ Vale citar a constatação de vanguarda de Rodotà (1973, p. 14-15) sobre a capacidade de a congregação de dados proporcionar um dossiê inteiro sobre certa pessoa, explicitando o poder de controle conferido por quem a detenha: “Cada um dos dados, considerado em si, pode ser pouco ou nada significativo: ou melhor, pouco ou nada diz além da questão específica a que diretamente se refere. No momento em que se torna possível conhecer e relacionar toda a massa de informações relativas a uma determinada pessoa, do cruzamento dessas relações surge o perfil completo do sujeito considerado, que permite sua avaliação e seu controle por parte de quem dispõe do meio idôneo para efetuar tais operações”.

⁶ Assim concorda Siqueira Jr. (2015, p. 177) quando constata os efeitos gerados pela substituição da sociedade industrial do século XX pela sociedade da informação do século XXI: “A informação não é a grande novidade da era atual, mas a velocidade e quantidade da informação que evoluíram em termos inimagináveis. Até mesmo o Estado é colocado em xeque frente à informação”.

manifestação do pensamento, direito de resposta, acesso à informação, sigilo da fonte: art. 5º, IV; V; IX; XIV, CF) e a salvaguarda de comunicações sigilosas (sigilo das comunicações de dados, telegráficas e telefônicas: art. 5º, XII, CF).

Assim, vê-se que o constituinte buscou formas de proteger a livre circulação de informações ao mesmo tempo em que procurou tutelar direitos fundamentais personalíssimos e próprios do regime democrático. Entretanto, no ordenamento jurídico nacional não é tão evidente a presença de um direito fundamental à proteção de dados pessoais, como atributo do direito à privacidade, mas uma análise acurada permite ver as bases para a sua identificação.

De antemão, importa assentar que a análise detida do arcabouço jurídico nacional permite constatar a existência de um direito fundamental à proteção de dados pessoais oriundo da interpretação conjunta do princípio constitucional da dignidade humana, da igualdade substancial, da liberdade, da inviolabilidade da vida privada e da intimidade, do sigilo das comunicações, da proteção às informações pessoais instrumentalizada pelo *habeas data* e da proteção de direitos e garantias reconhecidos pelo legislador infraconstitucional nos marcos legais de defesa do consumidor (Lei nº 8.078/1990), de acesso à informação (Lei nº 12.527/2011), do uso da internet (Lei nº 12.965/2014) e de proteção dos dados pessoais (Lei 13.709/2018)⁷.

Com efeito, a supracitada afirmação acerca da existência de tal direito fundamental apoia-se na doutrina de Schertel Mendes (2014), Doneda (2019), Sauaia (2018) e Bioni, Rielli e Zanatta (2020), os quais, por meio de uma leitura constitucional dogmática a ser explanada neste primeiro tópico do trabalho, somada à legislação infraconstitucional e ao acervo doutrinário acerca da proteção de dados pessoais, identificam uma tutela constitucional dos dados pessoais voltada a proteger a autodeterminação do indivíduo e os direitos da personalidade, os quais o protegem contra práticas abusivas no tratamento de dados⁸. Foi o que o Supremo Tribunal Federal

⁷ Desde já se ressalta a insuficiência das garantias de sigilo de comunicações e de inviolabilidade da privacidade para a proteção da personalidade em face dos riscos gerados pelo processamento e utilização de informações pessoais do tratamento de dados insito à Sociedade da Informação. “Afinal, não se trata de tornar sigilosas informações que podem causar a discriminação ou a limitação da liberdade pessoal, mas de regular os efeitos das informações da sociedade, por meio da regulação de seu fluxo e da instituição de procedimentos de controle” (SCHERTEL MENDES, 2014, p. 165).

⁸ Atualmente, no Brasil, a fonte normativa do direito fundamental à proteção de dados pessoais pode passar a ter origem expressa no elenco do artigo 5º da Carta Magna de 1988 em razão do estágio avançado do trâmite legislativo da Proposta de Emenda à Constituição (PEC) nº 17/ 2019. Essa proposta insere ao referido artigo o inciso LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. Caso a PEC venha a ser promulgada pelo Congresso Nacional, o ordenamento

constatou em recente decisão em sede de medida cautelar nas Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6393, 6390, por meio das quais se suspendeu a aplicação da Medida Provisória 954/2018, que obrigava as empresas de telecomunicações ao compartilhamento dos dados pessoais de seus clientes ao Instituto Brasileiro de Geografia e Estatística (IBGE) para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente da Covid-19 (STF..., 2020)⁹.

Em continuidade à identificação das bases jurídicas de um direito fundamental à proteção de dados pessoais na ordem jurídica nacional, impõe-se primeiramente afirmar a insuficiência da inviolabilidade constitucional da comunicação, disposta no inciso XII do art. 5º da CF, para tutelar os dados pessoais, vez que, conforme interpretação assente na jurisprudência pátria¹⁰, a proteção conferida por esse dispositivo é a da comunicação, e não dos dados em si. Nesse sentido, assevera Ferraz Jr. (1994, p. 446-447) em conhecido trabalho sobre o tema:

A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação.

Há que ser inicialmente destacado também que, ao contrário do que se pode afirmar, a Constituição não tutela apenas os dados sigilosos presentes em um processo comunicacional por meio da inviolabilidade prevista no inciso XII do art. 5º da CF/88. Deve-se atentar para a distinção a ser feita entre o âmbito de proteção do direito exposto nesse inciso, que são os dados, ainda que não pessoais, objeto de fluxo comunicacional, e o âmbito de proteção do direito à privacidade previsto no inciso X do art. 5º da CF, que abarca qualquer dado pessoal como desdobramento da privacidade e elemento constitutivo da personalidade.

Consoante Bioni, Rielli e Zanatta (2020), as garantias constitucionais dos incisos X e XII do art. 5º da CF diferenciam-se também no tocante à interpretação. Enquanto o inciso X resulta em uma tutela dinâmica sobre a forma pela qual uma informação, ou sua

jurídico brasileiro passará a conceder a merecida tutela máxima aos dados pessoais, de forma expressa e inequívoca.

⁹ Para uma exposição das inconstitucionalidades da Medida Provisória 954/2018, ver Schertel Mendes (2020).

¹⁰ RE 418.416-8/SC, Rel. Min. Sepúlveda Pertence, 10-5-2006; HC 91.867/PA, Rel. Min. Gilmar Mendes, 24-4-2012.

divulgação, pode ser prejudicial ao seu titular, o inciso XII, por sua vez, fixa uma tutela estática sobre uma informação necessariamente originária de um fluxo comunicacional.

Visto isso, ao contrário do que se possa cogitar, depreende-se que a definição do direito à proteção de dados pessoais no Brasil advém, primordialmente e majoritariamente, da construção hermenêutica conjunta dos seguintes dispositivos dos títulos dos Princípios Fundamentais e dos Direitos e Garantias Fundamentais da CF/88 (BRASIL, 1988), *in verbis*:

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) II - a cidadania; III - **a dignidade da pessoa humana**; (...)

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, **à igualdade**, à segurança e à propriedade, nos termos seguintes: (...)

X - são invioláveis a intimidade, **a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...)

LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de **informações relativas à pessoa** do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (grifo nosso).

O princípio constitucional da dignidade da pessoa humana, previsto no inciso III do art. 1º da Carta Magna, ampara sobremaneira a concepção protetiva da pessoa humana. Esse princípio reclama um tratamento de dados pessoais que considere a autonomia individual, garantida pela liberdade e igualdade material do *caput* do artigo 5º da Carta Política. A proteção conferida pelo princípio da igualdade substancial, por sua vez, salvaguarda os direitos da personalidade contra práticas abusivas no tratamento de dados que acarretam situações potencialmente discriminatórias (CALABRICH, 2020; MATTIUZZO, 2020)¹¹. É imperioso, portanto, reconhecer que a dignidade humana se encontra na origem axiológica da proteção de dados pessoais.

O remédio constitucional do *habeas data*¹², garantia fundamental prevista no inciso LXXII do artigo 5º da CF, complementa a proteção dada pelo constituinte aos

¹¹ O amplo monitoramento e uso de informações pessoais contidas em banco de dados públicos ou privados pode impactar as oportunidades concedidas às pessoas pelas Instituições, uma vez que atividades de seleção e classificação de indivíduos partem dessas bases de dados.

¹² Doneda (2019, RB-4.3) identifica que Vittorio Frosini, em seu artigo “La protezione dela riservatezza nella società informatica”, publicado em 1981, foi o primeiro a se referir ao termo. Para Frosini, “poder-se-ia dizer, com uma paráfrase de caráter metafórico, que na legislação dos Estados modernos é necessário hoje um *habeas data*, um reconhecimento do direito do cidadão de dispor dos próprios dados pessoais, assim como ele tem o direito de dispor livremente do próprio corpo”.

dados pessoais na medida em que concede ao impetrante o direito de acesso e de retificação de “informações relativas à pessoa do impetrante” baseadas em bancos de dados públicos. Nota-se que, nesse dispositivo, a preocupação constitucional com as informações pessoais é expressa.

De acordo com Schertel Mendes (2018, p. 198), o *habeas data* constitui uma “garantia processual de proteção das liberdades e da personalidade frente ao tratamento de dados”. Tal entendimento ampara-se na leitura do acórdão do Supremo Tribunal Federal prolatado no julgamento do Recurso Extraordinário nº 673.707, bem como nos votos dos Ministros, onde se reconhece no *habeas data* um instrumento de tutela do direito fundamental à autodeterminação informativa, consolidando materialmente a proteção constitucional de dados pessoais¹³.

Por sua vez, ao referir-se à intimidade e à vida privada no inciso X, a CF/88 acabou por gerar controvérsia na diferenciação de ambos os conceitos. Para Mendes (2017, p. 280), a doutrina majoritária assenta não haver distinção entre os termos, embora haja quem defenda que o direito à intimidade integraria o direito à privacidade, mais amplo.

Adentra-se, a partir daqui, na compreensão da origem do direito do qual germina a tutela dos dados pessoais, qual seja o direito à privacidade, pois que se mostra relevante para a análise jurídica do direito fundamental à proteção de dados pessoais em face dos impactos do mundo digital na Sociedade da Informação.

O direito à privacidade tem como modelo precursor a defesa da privacidade na forma de um direito a ser deixado só, por meio do qual a reclusão periódica à vida privada é vista como uma necessidade de todo indivíduo. Essa reflexão teve início com a publicação do artigo *The right to privacy*, por Warren e Brandeis¹⁴ (1890, p. 205), que marcou uma nova concepção do direito à privacidade, vez que sua justificativa de tutela passou a residir na inviolabilidade da personalidade humana e não mais na propriedade privada.

De acordo com Mendes (2017, p. 280), o direito à privacidade tem por objeto os fatos relativos à pessoa em geral e às relações comerciais e profissionais que o indivíduo

¹³ Para que o *habeas data* proteja mais eficazmente os dados pessoais, segundo Schertel Mendes (2014, p. 174), “seria necessário simplificar os mecanismos de impetração da ação, bem como modificar a interpretação acerca das condições processuais dessa ação (interesse de agir e esgotamento das vias administrativas)”.

¹⁴ Doneda (2019) aponta inexistir unidade semântica do *right to privacy* norte-americano pois a expressão foi usada com fins diversos e distintos entre si, muito em razão da vasta amplitude das fontes normativas atinentes ao conceito. Essa multiplicidade de significados, típica ao pragmatismo de sistemas de *common law*, como o norte-americano, compõe a formação histórica do direito à privacidade.

não quer dar a conhecer ao público. Portanto, é concebido como uma liberdade negativa de resguardo contra interferências alheias, que visa manter um espaço reservado que esteja protegido da intromissão malquerida de terceiros e do Estado, do qual se exige abstenção.

Desenvolveu-se, assim, a teoria das três esferas da privacidade, subdivididas em dimensões progressivamente menores. Como explica Costa Jr. (2007, p. 29-30), a esfera de maior dimensão é a esfera da privacidade *stricto senso*, da vida particular, que congrega os comportamentos e acontecimentos que o indivíduo quer manter longe dos olhos do grande público. No interior da esfera da vida particular está a esfera da intimidade, da confiança, onde apenas participam as pessoas que o indivíduo confia e mantém certa intimidade. Por fim, ao centro, no núcleo, encontra-se a esfera do segredo, cuja proteção jurídica é maior por se referir àquela parcela da vida privada da qual participam poucos indivíduos mais próximos da pessoa¹⁵.

Historicamente, na esteira da preocupação com os limites a serem dados ao Estado diante das ameaças de vigilância abusiva dos indivíduos (MALHEIRO; VIGLIAR, 2020), o direito à privacidade se desenvolveu em paralelo aos efeitos causados na sociedade em virtude da formulação de novas tecnologias (câmera fotográfica, filmadora, rádio, televisão, computador, dispositivo móvel). Essas evoluções perpassaram não somente as formas de comunicação encontradas pelo ser humano, mas também a expansão da capacidade de acondicionamento de informações em locais cada vez menores (disquete, CD, DVD, pen-drive, disco rígido portátil, computação em nuvem) e o potencial de geração de informações possibilitado pelo cruzamento de dados (construção de perfis, publicidade comportamental direcionada, avaliação de crédito etc.).

A privacidade deixou de ser uma característica apenas de pessoas da mais alta classe social, preocupados sobretudo com sua honra e imagem públicas, e adentrou em

¹⁵ Entretanto, impõe-se observar, a teoria das esferas recebeu críticas diante da constatação da inexistência de uma relação necessária entre o grau de privacidade de certa informação e os danos causados por sua divulgação. Um exemplo desse descompasso é o potencial de a agregação de dados isolados possibilitar a construção de perfis completos de indivíduos sem ter havido a coleta de informações íntimas de seu exclusivo conhecimento, como demonstra Leonardi (2012, p. 60-61) ao descrever os ensinamentos pioneiros de Stefano Rodotà, o qual “já advertia havia tempo que a proteção da privacidade nesses casos decorria da dispersão dos dados pessoais. Ao serem centralizados e atualizados continuamente, certos dados permitem visualizar um dossiê completo do indivíduo: ‘Cada um dos dados, considerado em si, pode ser pouco ou nada significativo: ou melhor, pouco ou nada diz além da questão específica a que diretamente se refere. No momento em que se torna possível conhecer e relacionar toda a massa de informações relativas a uma determinada pessoa, do cruzamento dessas relações surge o perfil completo do sujeito considerado, que permite sua avaliação e seu controle por parte de quem dispõe do meio idôneo para efetuar tais operações”.

sua dimensão social positiva de proteção. São causas desse fenômeno: o aprimoramento das políticas públicas típicas do Estado de Bem-Estar Social - junto com a necessidade de armazenamento de dados pelo Estado para tais fins -, acompanhado por uma ampla demanda de direitos sociais, e o conseqüente aumento do fluxo de informações decorrente do desenvolvimento tecnológico.

Exemplo lapidar dos riscos causados à personalidade humana pelo aprimorado processamento e armazenamento de dados pessoais foi o julgamento histórico do Tribunal Constitucional alemão sobre uma lei de recenseamento de 1982 que, ao visar a coleta de dados dos cidadãos sobre a profissão, a moradia e o local de trabalho, fixava multa para quem não respondesse. O Tribunal, então, declarou nulo alguns dispositivos e fixou o conceito de livre controle da pessoa sobre a movimentação de suas informações na sociedade, reconhecendo o direito à autodeterminação informativa. Formulou-se, assim, a proteção de dados pessoais como um direito subjetivo fundamental cujo núcleo não poderia ser violado.

Com efeito, os conflitos de interesse se intensificaram a partir do florescimento de novos mecanismos tecnológicos, vez que as pessoas em sociedade passaram a vivenciar com mais frequência realidades ensejadoras de colisão de direitos. Os danos ilícitos, antes focados apenas no indivíduo, agora passam a ser também de natureza coletiva, vez que o tratamento massivo de informações atinge inúmeras pessoas. Não se tratava mais apenas de um direito negativo que exigia a abstenção do Estado na esfera individual, mas concebeu-se um direito positivo que garante o controle de informações pessoais para assegurar um espaço de autonomia da vontade que propicie o livre desenvolvimento da personalidade humana (MENDES, 2017, p. 282).

Doneda denomina tal processo de funcionalização da proteção da privacidade e entende que a proteção de dados pessoais é a sua continuação por outros meios. Para ele, o advento da sociedade pós-industrial proporcionou a necessidade de proteção de novos interesses jurídicos, não sendo mais suficiente tão só a tutela de natureza patrimonial.

Ao realizar essa continuidade, porém, a proteção de dados pessoais assume a tarefa de abordar uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias, especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais. Daí a necessidade de superar a ordem conceitual pela qual o direito à privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa (DONEDA, 2019, RB-1.1).

Schertel Mendes (2014, p. 29) se assemelha na compreensão do cenário de evolução descrito por Doneda. Segundo ela, o conceito de dados pessoais pode ser percebido de forma mais clara a partir da década de 1970 por meio de leis específicas e decisões judiciais de diversos países, bem como de tratados internacionais. O conteúdo do direito à privacidade foi alterado e passou a ser denominado privacidade informacional, autodeterminação informativa, proteção de dados pessoais, entre outros. Desse modo, conclui-se que a interpretação constitucional do inciso X do art. 5º da CF, portanto, abrange a proteção de atributos da personalidade humana, como a privacidade em sua dimensão de proteção de dados pessoais.

Destarte, é possível afirmar que a hermenêutica constitucional dos dispositivos atinentes à privacidade e às informações pessoais possibilita o reconhecimento da existência de um direito fundamental à proteção de dados pessoais. Essa tutela se complementa, no ordenamento jurídico brasileiro, por intermédio dos seguintes marcos legais e decretos regulamentares correspondentes, de forma exemplificativa:

- Código de Defesa do Consumidor (Lei 8.078/1990), que em seus artigos 43 e 44 trata dos dados integrantes dos cadastros de consumidores;
- Lei do *habeas data* (9.507/1997), que regulamenta o inciso LXXII do artigo 5º da CF e disciplina seu rito processual;
- Lei de Acesso à Informação (12.527/2011), que disciplina o direito constitucional de acesso à informação previsto no inciso XXXIII do artigo 5º, no inciso II do § 3º do artigo 37 e no § 2º do artigo 216 da CF;
- Lei do Cadastro Positivo de Crédito (12.414/2011), que regula um banco de dados com o histórico de crédito dos consumidores;
- Marco Civil da Internet - MCI (Lei 12.965/2014), que prevê expressamente o direito a proteção de dados pessoais como um princípio que permite o uso desses dados mediante o consentimento livre, expresso e informado de seu titular, e
- Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.709/2018), que regulamenta com maior profundidade a proteção de dados ao estabelecer um regime jurídico de princípios, definições, hipóteses lícitas de tratamento de dados e as sanções por sua violação, dispensando a necessidade de se adentrar em subjetivismos para a responsabilização por infrações à privacidade do titular de dados.

No entanto, a análise a ser efetuada no tópico seguinte revelará a insuficiência, para a eficácia da tutela dos dados pessoais, do reconhecimento do direito à proteção de dados pessoais como direito fundamental bem como dos instrumentos legais colacionados acima. Por certo, diante da ubiquidade da tecnologia da informação na sociedade, o tratamento massivo de dados demonstra que os direitos subjetivos do titular dos dados pessoais (direitos de informação, acesso, notificação, retificação, cancelamento e bloqueio), núcleo de tutela do regime jurídico instaurado pela LGPD, nem sempre são adequados e traduzem eficaz proteção da privacidade, como Schertel Mendes (2014, p. 46) anotou.

Para possibilitar o controle do titular acerca dos seus dados, foram estabelecidos, na maioria das legislações sobre o tema, direitos subjetivos, tais como os direitos de informação, acesso, retificação e cancelamento. Sua função principal era a de tornar efetivo o exercício dos princípios previstos nas normas. Embora esses direitos configurem significativo empoderamento do indivíduo, ver-se-á que o seu estabelecimento nem sempre é suficiente para garantir a adequada proteção de dados na sociedade da informação (SCHERTEL MENDES, 2014, p. 46, grifo nosso).

Nas conclusas palavras da autora (2014, p. 82), “percebe-se uma preocupação com a efetividade das normas atuais de proteção de dados pessoais”. Vê-se, desse modo, que o titular de dados pessoais se encontra vulnerável diante das inúmeras possibilidades de tratamento de seus dados pessoais de forma contrária ao consentimento dado, isto é, com finalidade não consentida, por exemplo.

Essa constatação permanece mesmo diante da entrada em vigor da LGPD, no dia 18 de setembro de 2020, com a parte das sanções administrativas previstas para vigorar a partir de 1º de agosto de 2021, consoante o art. 65, I-A da Lei (BOLSONARO..., 2020; VAINZOF, 2020). Como se verá nos tópicos seguintes, a conformação procedimental de hipóteses de tratamento, de condições para o controle dos dados pessoais por seu titular e a instituição de sanções administrativas com penalidades centradas no patrimônio, proporcionados pelos Marcos Legais existentes na ordem jurídica nacional, não são satisfatórias¹⁶. Assim, a fim de conferir maior proteção aos dados pessoais, há de se aventar acerca da existência de um mandado de criminalização advindo do dever objetivo de proteção da Constituição para tutelar penalmente os dados pessoais.

¹⁶ Zanatta (2015, p. 468-469) vai além ao afirmar que o direito é insuficiente para a garantia de direitos em um mundo digitalizado.

2 O MANDADO DE CRIMINALIZAÇÃO DECORRENTE DO DEVER CONSTITUCIONAL OBJETIVO DE PROTEÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Até aqui constatou-se a existência, em sede constitucional e mesmo que não de forma explícita, do direito fundamental à proteção de dados pessoais como acepção da garantia da inviolabilidade da privacidade que, por sua vez, pode ser instrumentalizada pelo *habeas data*. O direito fundamental à proteção de dados pessoais surge então a partir da hermenêutica do direito constitucional à privacidade (art. 5º, X, CF), da garantia do *habeas data* (art. 5º, LXXII, CF) e do princípio constitucional da dignidade humana (art. 1º, III, CF) e da igualdade substancial (art. 5º, CF).

Da garantia da inviolabilidade da intimidade e da privacidade extrai-se uma tutela ampla da personalidade que não teria sentido em si mesma caso excluísse de seu âmbito de proteção exatamente as situações em que a vida privada se sujeita a maior violação, como é o caso do processamento de dados pessoais. Nesse sentido, assevera Schertel Mendes (2014, p. 171):

Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e vida privada do homem médio do que os perigos ‘tradicionais’, que ensejaram o nascimento desse direito, como a hipótese de ser flagrado por paparazzi ou de ser notícia de jornais sensacionalistas.

Além disso, para a autora, o reconhecimento do direito fundamental à proteção de dados pessoais não é somente uma possibilidade, mas uma necessidade diretamente decorrente da exigência de efetividade dos fundamentos e princípios constitucionais do Estado Democrático de Direito na sociedade contemporânea da informação.

A relação entre a democracia e a premente proteção dos dados pessoais, nesse sentido, reside na amplitude de ações possibilitadas ao Estado e às empresas privadas em razão da posse de informações de todo tipo sobre os indivíduos. Elas vão desde a possibilidade da vigilância e do monitoramento do comportamento das pessoas¹⁷, sob os auspícios da proteção da soberania nacional, até às ávidas práticas comerciais de oferta de produtos e serviços, motor da economia de mercado.

A crescente utilização do tratamento de dados pessoais aumenta a atenção que deve ser despendida pelas autoridades públicas, pela academia e pela sociedade

¹⁷ Atualmente, há quem cogite um conceito para além da estrita vigilância nos moldes do Big Brother: o *dataveillance*, conforme Guardia (2020).

organizada às possíveis consequências prejudiciais à personalidade dos titulares. Ora, tal processamento de informações pessoais, característico da economia informacional da sociedade atual, gera elevado risco à privacidade em decorrência da repercussão à integridade de diversos direitos fundamentais. Exemplifica-se.

O direito à igualdade material é vilipendiado a partir do instante em que uma pessoa é impedida de participar de determinada atividade, evento ou processo porque apresenta certas características pessoais indesejadas pelos organizadores. A problemática está no fato de os organizadores terem tido acesso a tais informações pessoais sem o conhecimento do titular dos dados, que não agiu para que isso ocorresse. Ela é visível por meio do exemplo de filtragem de pessoas em um processo seletivo, como o ocorrido no recrutamento da Amazon que apresentou viés contra mulheres (AMAZON, 2018), ou em um programa governamental apenas por apresentar determinada cor de pele ou por residir em determinada região, sem justificativa específica e plausível¹⁸. Demonstra-se, aí, grave atentado ao princípio da igualdade material.

A violação ao livre exercício de profissão pode ser vista quando um candidato a emprego não é contratado por integrar cadastros corporativos clandestinos de pessoas que ajuizaram ações trabalhistas, as conhecidas “listas negras”¹⁹. Da mesma forma, as liberdades públicas de manifestação, de locomoção, de iniciativa empresarial etc. são transgredidas quando decisões automatizadas, calcadas em banco de dados, obstruem a oportunidade de pessoas participarem de iniciativas determinantes para suas vidas sem seu conhecimento acerca do processamento de dados realizado.

Assim, no contexto da configuração dos dados pessoais como extensão da personalidade humana que exige a tutela da privacidade individual, medidas mais efetivas devem ser adotadas. Isso porque, nos processos de coleta, armazenamento, utilização ou transferência de dados pessoais realizados atualmente, a presença de inúmeras possibilidades de infrações a normas fundamentais relativas a liberdades individuais - cujos exemplos concretos posteriormente se descreverá - é indubitável, mas não apenas. Como visto, o reconhecimento da proteção de dados pessoais como direito fundamental para o combate das violações ao direito subjetivo de tutela dos dados pessoais é

¹⁸ Para aprofundar na discriminação algorítmica passível de ocorrer nas relações de consumo, conferir Oliva (2021) e, especial no segmento de seguros, ver Junqueira (2020).

¹⁹ Vide decisões do TST acerca da ilegalidade de tal prática: RR 325/2004-091-09-00.7, julgado em 2-4-2008, Rel. Min. Maria de Assis Calsing, 4ª Turma, DJ 18-4-2008; RR 532/2003-091-09-00.0, julgado em 2-4-2008, Rel. Min. Maria de Assis Calsing, 4ª Turma, DJ 18-4-2008 (SCHERTEL MENDES, 2014, p. 162).

insuficiente, tornando-se necessário investigar a proteção decorrente da dimensão objetiva do direito fundamental à proteção de dados pessoais para salvaguardar com maior efetividade a privacidade individual.

Com efeito, o direito fundamental pode ser verificado sob as dimensões subjetiva e objetiva, não apenas como proibição de intervenção em direito alheio, mas também como proibição de proteção insuficiente. Registra-se que ambos os princípios de proibição têm origem na doutrina alemã sobre o postulado constitucional da proporcionalidade, cuja fonte reside no âmbito dos direitos fundamentais e, mais especificamente, na cláusula do devido processo legal expressa no art. 5º, LIV, da CF/88, conforme o magistério de Mendes (2017, p. 220; 223).

A dimensão subjetiva de um direito fundamental, relativa à origem dos estudos da doutrina do direito constitucional e recém vista acima, proporciona uma pretensão a um determinado comportamento capaz de modificar situações jurídicas. Manifesta-se também por meio do poder da vontade em produzir efeitos sobre vínculos jurídicos, em maior ou menor grau. Nessa ótica, o direito fundamental pode reclamar uma ação negativa ou positiva do indivíduo (MENDES, 2017, p. 165).

Já a dimensão objetiva do direito fundamental traduz uma diretriz para a atuação estatal, cujo bem que se visa tutelar pode constituir-se em valor a ser preservado por toda a ordem jurídica, cuja exigibilidade é capaz de restringir até o conteúdo e o alcance de direitos subjetivos individuais. Consoante o magistério de Mendes (2017, p. 168), o direito fundamental então é considerado como princípio básico da ordem constitucional, participe da essência do Estado Democrático de Direito e valor a ser protegido e conservado de maneira objetiva, devendo ser um norte para a ação dos poderes constituídos.

Conforme exemplifica o mesmo autor, o Estado pode então adotar medidas de prestação positiva até mesmo de ordem penal com o fim de proteger direitos fundamentais com maior efetividade. Segundo Mendes, cabe ressaltar que tal medida deve conformar-se com a liberdade de conformação do legislador, cuja discricionariedade na opção dos bens jurídicos a serem protegidos integra a natureza política da priorização de valores em situações de colisão de direitos e interesses envolvidos.

Os direitos fundamentais, assim, transcendem a perspectiva da garantia de posições individuais, para alcançar a estatura de normas que filtram os valores básicos da sociedade política, expandindo-os para todo o direito positivo (MENDES, 2017, p. 166).

No tocante a este trabalho, a ótica subjetiva do direito fundamental à proteção de dados pessoais constitui-se em direito de defesa que atribui uma esfera de liberdade e privacidade individual a qual não pode sofrer intervenção do poder estatal ou privado. Como exemplo, citam-se a hipótese de controle dos dados pessoais pelo seu titular, como ação positiva do sujeito, e as decorrentes obrigações e limitações, por não se tratar de direito absoluto. De outro lado, em caso de violação, esse direito subjetivo confere a possibilidade de adoção de ações ressarcitórias, de medidas preventivas, entre outras que exigem ação negativa do sujeito (SCHERTEL MENDES, 2014, p. 176).

Entretanto, como se viu, apenas a face subjetiva desse direito é insuficiente para a proteção efetiva da privacidade configurada na extensão da personalidade presente nos dados pessoais. Assim, a dimensão objetiva do direito fundamental à proteção de dados pessoais surge como alternativa de análise, bem como de proteção, e, desse modo, acarreta na necessidade da concretização, pelo Estado, de mecanismos de proteção do bem jurídico oriundos do dever de proteção exigido pela Carta de 1988, para além dos consequentes deveres de regulação e organização do exercício do direito de proteção de dados pessoais direcionado ao Estado-legislador²⁰. Esses deveres já possibilitaram a instituição de condições e procedimentos para a tutela de dados pessoais pela LGPD, que regulamentou direitos subjetivos de forma detalhada, como os direitos de informação, acesso, notificação, retificação, cancelamento e bloqueio.

Ocorre que, observou-se quão insatisfatória se deu na prática a proteção conferida por tais institutos em demais países, muito em razão da intensa dinâmica da economia de dados²¹, tão explorada pela Sociedade da Informação do século XXI (SCHERTEL MENDES, 2014, p. 46 e 82). No Brasil, apesar da entrada em vigor parcial da LGPD e do início da estruturação da Autoridade Nacional de Proteção de Dados – decreto regulamentador publicado pelo Executivo Federal e diretores indicados e aprovados pelo Senado -, órgão subordinado à Casa Civil e, ao que tudo indica, com potencial reduzido de fiscalização por questões técnicas e políticas, provavelmente não será diferente, uma vez que o núcleo duro do regime jurídico de proteção de dados pessoais e as correspondentes diretrizes normativas são de certa maneira já aplicáveis em decorrência

²⁰ A dimensão objetiva dos direitos fundamentais, conforme ensina Mendes (2017, p. 166), propicia um direito a prestação positiva estatal que “cobra a adoção de providências, quer materiais, quer jurídicas, de resguardo dos bens protegidos. Isso corrobora a assertiva de que a dimensão objetiva interfere na dimensão subjetiva dos direitos fundamentais, neste caso atribuindo-lhe reforço de efetividade”.

²¹ Sobre a temática, recomenda-se a leitura de Zanatta e Abramovay (2019).

do direito à proteção de dados pessoais expresso desde 2014 no vigente Marco Civil da Internet (Lei 12.965/2014)²².

Sendo assim, tendo em vista que a garantia efetiva da proteção constitucional de dados pessoais só é possível a partir da conformação e densificação da ação estatal, é necessário que o Estado-legislador concretize seu dever de proteção do bem jurídico tutelado pelo direito fundamental à proteção de dados pessoais. Segundo ensina Schertel Mendes (2014, p. 175), o bem jurídico salvaguardado por tal direito é duplo. De um lado, busca defender a integridade moral da pessoa como componente essencial da dignidade humana e, de outro, visa amparar as liberdades em sentido amplo (de comunicação, de trabalho, de locomoção, de iniciativa, de informação etc.).²³

Tais bens jurídicos, portanto, devem ser objeto de proteção para salvaguardar o direito fundamental à proteção de dados pessoais com maior efetividade por intermédio do mandado constitucional de criminalização, presente no título dos direitos e garantias fundamentais da Constituição de 1988, inciso XLI do art. 5º:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)

XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais;

Esse mandamento é entendido por Mendes (2017, p. 504) como um dever estatal genérico de tomar as providências necessárias à realização ou concretização dos direitos fundamentais e, como afirma Feldens (2012), tal mandado impõe a instituição de um sistema de proteção penal ao bem jurídico tutelado pelo direito fundamental.

Desse modo, é preciso apoiar-se no mandamento constitucional de criminalização de condutas atentatórias de direitos fundamentais para complementar a efetiva tutela de dados pessoais, ademais dos efeitos propiciados pelo Direito Civil e Administrativo no

²² Vide o exemplo da multa imposta ao Facebook no caso Cambridge Analytica pelo Departamento de Proteção e Defesa do Consumidor (DPDC) da Secretaria Nacional do Consumidor, do Ministério da Justiça, Em artigo com comentários à decisão, Frazão (2020) pontua: “Como se pode observar, também o DPDC, apesar de não aplicar a LGPD, mostrou claramente o seu interesse em dar eficácia aos dispositivos já existentes sobre a matéria, trazendo rica argumentação que adianta várias das discussões que são tratadas diretamente pela LGPD, tais como a finalidade específica do tratamento de dados, os limites e pressupostos do consentimento, bem como o alcance dos deveres de informação e monitoramento.”

²³ “Na Alemanha, o entendimento de que o direito à autodeterminação informativa visava exclusivamente à proteção da personalidade foi bastante criticado: hoje há um certo consenso na doutrina alemã de que a proteção de dados pessoais visa tanto a proteção da integridade moral e da personalidade, na dimensão interior do livre desenvolvimento do indivíduo (...), como a proteção do direito geral à liberdade e das liberdades específicas, na dimensão exterior do seu livre desenvolvimento (...)” (SCHERTEL MENDES, 2014, p. 175).

bojo do MCI e da LGPD. Pois de nada adianta a ordem jurídica plasmar o direito à proteção de dados pessoais, seja por meio da hermenêutica de dispositivos constitucionais, seja pelo regime jurídico cível infraconstitucional (SOUTO, 2020), se não conferir instrumentos de tutela que protejam efetivamente os titulares de dados pessoais de violações aos seus direitos fundamentais de liberdade, igualdade material, livre exercício da profissão, livre locomoção, livre iniciativa etc.

Então, há de se considerar a exigência jurídica de um mandamento constitucional de criminalização da violação dos dados pessoais traduzida na necessária tipificação penal de conduta atentatória ao direito fundamental de proteção de dados pessoais, também defendida por Tadeu (2011, p. 98). No entanto, antes de se aventar uma hipotética conduta apta a tutelar penalmente os dados pessoais, é preciso afirmar a constitucionalidade da criminalização da violação de dados pessoais tendo em vista a insuficiente atuação estatal para garantir a proteção do indivíduo contra os riscos à personalidade causados pelo tratamento de dados pessoais.

Objetiva-se, com isso, refutar de pronto eventual arguição de inconstitucionalidade de lei instauradora de tipo penal para tutelar os dados pessoais por excesso do Poder Legislativo. A justificativa reside na inexistência de violação ao postulado constitucional da proporcionalidade em sua dimensão de exigência de proibição de proteção insuficiente. Isso porque, como uma “metanorma que prescreve o modo de raciocínio e de argumentação relacionado às normas restritivas de direitos fundamentais”, segundo Novellino (2019, p. 336), o postulado da proporcionalidade impõe aos órgãos estatais o dever de tutelar os direitos fundamentais de forma adequada, suficiente e proporcional, proibindo uma proteção deficiente.

A proibição de proteção insuficiente impõe aos poderes públicos, portanto, a adoção de medidas adequadas e suficientes para garantir a proteção e promoção dos direitos fundamentais, sobretudo, daqueles que dependem de prestações materiais – e.g., direitos sociais prestacionais – e jurídicas – e.g., criminalização de condutas gravemente ofensivas – por parte do Estado. Na jurisprudência do Supremo Tribunal Federal referida face do princípio da proporcionalidade tem sido especialmente utilizada como imposição dirigida ao legislador quando do cumprimento dos “mandados constitucionais de criminalização” (NOVELINO, 2019, p. 340).

Com efeito, a verificação da proporcionalidade, da necessidade e da adequação do ato estatal tem origem na dogmática alemã, apresentada por Mendes (2017, p. 505), e tem estrutura diferenciada se comparada às proibições de intervenção ou excesso. Na hipótese

de eventual criação de lei penal, portanto, a análise de constitucionalidade deve considerar que o ato

(...) não será adequado quando não proteja o direito fundamental de maneira ótima; não será necessário na hipótese de existirem medidas alternativas que favoreçam ainda mais a realização do direito fundamental; e violará o subprincípio da proporcionalidade em sentido estrito se o grau de satisfação do fim legislativo é inferior ao grau em que não se realiza o direito fundamental de proteção (MENDES, 2017, p. 505).

Ora, a medida proposta por este trabalho não incorre em nenhuma das assertivas. A criminalização da violação de dados pessoais é adequada pois busca atingir o pretendido objetivo de cessação de condutas violadoras do direito fundamental à proteção de dados pessoais com maior rigor que o Direito Civil e Administrativo. A previsão de sanções penais se mostra mais gravosa e, portanto, apresenta maior potencial de coerção jurídica para inibição de comportamentos transgressores da privacidade.

Tal medida se revela necessária porquanto não há meios menos gravosos aos indivíduos que sejam efetivos na mesma medida da criminalização de conduta violadora da proteção de dados pessoais, como se verá pela exemplificação dos inúmeros e crescentes casos de violações de privacidade por meio do tratamento de dados pessoais.

Por sua vez, a adoção legislativa de conduta típica se revela proporcional em sentido estrito, vez que alcança o objetivo de equilíbrio entre o intuito visado pelo legislador ao criminalizar conduta violadora da privacidade de dados pessoais, qual seja a realização efetiva do direito fundamental de proteção de dados pessoais, e a necessária intervenção em direitos individuais.

De outro lado, caso se considerasse que já existem medidas cíveis e administrativas cabíveis suficientes para a proteção do direito fundamental à proteção de dados pessoais, constatar-se-ia a desproporcionalidade de eventual tipificação penal.

Identificado, portanto, o mandamento constitucional à criminalização de condutas atentatórias do direito fundamental à proteção de dados pessoais e a sua proporcionalidade, passa-se a tratar de sua concretização por meio da instituição eventual de um tipo penal. Tal ação é requerida em virtude não apenas da exigência do princípio da proibição de proteção insuficiente, mas também em razão do constante crescimento de fatos que se amoldariam a uma conduta violadora do direito fundamental aqui tratado, guardadas as devidas circunstâncias e adaptações.

3 A TUTELA PENAL A PARTIR DO REGIME JURÍDICO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Tendo identificado razões para sustentar a proporcionalidade da criminalização do tratamento indevido de dados pessoais, importa averiguar o atendimento dos pressupostos mínimos do Direito Penal, qual é o bem jurídico a ser tutelado, os atuais crimes existentes que não alcançam tal conduta, o âmbito de proteção do direito fundamental à proteção de dados pessoais bem como suas principais ramificações de proteção infraconstitucional, incluído o regime jurídico da LGPD. Busca-se, com isso, preencher os requisitos jurídicos de razoabilidade para instituir uma tutela penal específica e colher conceitos que delinearão a formatação de um tipo penal para maior proteção da privacidade do titular de dados pessoais²⁴.

Na esfera penal, não há dúvida de que o bem jurídico em geral a ser tutelado por eventual tipo penal que criminalize o tratamento indevido de dados pessoais é a privacidade, dimensão da personalidade humana cuja proteção é exigida pela CF/88. Entende-se privacidade aqui conforme o conceito de Westin (1967, p. 7), para quem ela se constitui como controle, pelo titular dos dados pessoais, das informações sobre si, isto é, como faculdade de determinar quando, como e em que medida tais dados serão comunicados a outrem.

Os crimes atualmente existentes no Código Penal (CP) brasileiro tutelam outros bens jurídicos, no entanto, insta nomear aqueles que lateralmente referem-se ao contexto do tratamento de dados pessoais, isto é, os crimes que visam proteger o sigilo das informações e a integridade dos computadores. São eles: violação de comunicações (art. 151, CP), divulgação de segredo pessoal ou profissional (art. 153, 154 CP) e invasão de dispositivo informático (art. 154-A, CP)²⁵.

No caso tratado por este artigo, quer-se proteger o titular de dados pessoais de quaisquer usos de suas informações que transgridam as normas de proteção da LGPD ou que extrapolem a finalidade do uso consentida pelo titular. Dessa forma, em consonância

²⁴ Sobre esse assunto, cf. CRUZ; NAVARRO, 2020.

²⁵ Em dezembro/2019, o Brasil foi convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. A Convenção trata de crimes relacionados a infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, relacionadas com computadores, com conteúdo (pornografia infantil) e infrações relacionadas com a violação do direito de autor e direitos conexos. Desde julho/2020 a matéria encontra-se em tramitação no Congresso Nacional a fim de que, caso seja aprovada, o Brasil possa aderir ao referido instrumento internacional (BRASIL, 2020).

com o que foi dito alhures, a tutela da privacidade como bem jurídico protege a integridade moral da pessoa e as suas liberdades fundamentais.

Para uma correta criminalização de conduta violadora da privacidade, em sua dimensão dos dados pessoais, importa conhecer o âmbito de proteção específico do direito fundamental à proteção de dados pessoais tomado do precursor trabalho de Schertel Mendes (2014, p. 174), amparado na doutrina alemã. Para ela, esse direito regula a ordem de informação e comunicação, multidimensional por essência, com o objetivo de equilibrar os inúmeros interesses em conflito no tocante aos usos de dados e na proteção dos direitos da personalidade e de participação dos titulares das informações nos processos de tratamento.

Para a autora, o objeto protegido por esse direito fundamental, ao contrário do que se possa imaginar, não é a informação pela informação mas, sobretudo, o processo de tratamento das informações, conforme explica:

A relevância jurídica reside menos nos dados em si, mas no **processo de coleta, armazenamento, utilização ou transferência, a partir do qual são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins**. Assim, entra em ação a proteção constitucional se a informação for usada para uma finalidade que cause riscos aos cidadãos, ou para fins considerados ilícitos a priori (como é o caso, por exemplo, de bancos de dados criados para fins discriminatórios). Assim, somente uma análise do contexto do uso das informações (ou das hipóteses previstas para a sua utilização), do conteúdo da informação, da finalidade de sua utilização e dos riscos envolvidos para o cidadão pode determinar a legitimidade de uma ação de tratamento de dados ou de informações pessoais (SCHERTEL MENDES, 2014, p. 175, grifo nosso).

Desse modo, no âmbito desse direito se constata a relevância da proteção jurídica dos elementos da finalidade do tratamento de dados pessoais e do conteúdo das informações pessoais utilizadas no contexto de cada uso. Não por acaso, esses aspectos foram regulados pela LGPD e, portanto, busca-se adequar a tutela penal para a proteção efetiva do âmbito desse direito fundamental embasando-se nos princípios e definições instituídos por esse regime jurídico, em análise semelhante à conduzida por Carvalho (2020).

Por meio dos incisos do seu art. 5º, a LGPD estipulou conceitos importantes como o de dado pessoal (“informação relacionada a pessoa natural identificada ou identificável), 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”), titular (“pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”), consentimento (“manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade adequada”), tratamento (“toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão...”) e agentes de tratamento (“o controlador e o operador”).

Foram elencadas hipóteses legais de tratamento de dados pessoais e definidas sanções civis e administrativas aplicáveis, nos termos do art. 5º da LGPD, ao controlador (“pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”) ou ao operador (“pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”)²⁶. Tais sanções objetivam inibir o tratamento de dados feito em desconformidade com a legislação, o que inclui, para os fins desse trabalho, aquele realizado com finalidade não consentida pelo titular da informação e aquele que não forneça a segurança esperada pelo titular dos dados, considerada a forma do tratamento, seu resultado, os riscos esperados do tratamento e as técnicas disponíveis à época, segundo o art. 46 da LGPD.

No art. 6º, a Lei estipulou que as atividades de tratamento de dados pessoais deverão observar os princípios da boa-fé, da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização e da prestação de contas. Para o que interessa a este trabalho, importa descrever o significado dos princípios da finalidade, da adequação, da necessidade e da segurança, bem como exemplos de violações.

Finalidade, nos termos da Lei (art. 6º, I), é a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. Segundo Cots e Oliveira (2019, p. 80), seriam transgressões a esse princípio as hipóteses de informar que a coleta de dados seria voltada para o faturamento de produto ou serviço, mas usar os dados para campanhas de marketing, outra seria avisar que o compartilhamento de dados se dará com a empresa X, mas compartilhá-los com a empresa W e outro exemplo seria informar que os dados não serão copiados, porém realizar a cópia deles.

²⁶ Acerca da exposição a eventuais responsabilidades criminais do controlador e do operador, cf. VALENTINI; HADDAD, 2019 e SANDRIN; SILVA, 2020.

Por sua vez, o princípio da adequação (art. 6º, II) busca compatibilizar o procedimento de tratamento a sua finalidade consentida pelo titular. O princípio da necessidade (art. 6º, III) estipula que a finalidade do tratamento consentida pelo titular deve nortear e ser o limite da qualidade, da abrangência e do volume dos dados que serão usados. Para Teixeira e Armelin (2019, p. 47), a finalidade, a adequação e a necessidade formam o conjunto principiológico do mínimo essencial que precisa ser observado para se buscar qual é a menor quantidade de dados pessoais necessária para que se chegue ao fim pretendido de maneira adequada.

Por fim, o princípio da segurança (art. 6º, VII) traduz a “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”. Tal princípio enfatiza a necessária proteção das informações pessoais contra ataques externos de furto de dados e posterior chantagem, por exemplo, abarcando as práticas ilícitas típicas da sociedade digital, nos termos utilizados por Zanellato (2002).

Desse modo, vistos tais conceitos para a compreensão da descrição da conduta consistente no tratamento indevido de dados pessoais, impõe-se elencar alguns casos que envolveram a violação da privacidade de titulares de dados pessoais, tendo ou não repercussão na esfera judicial ou administrativa. Os exemplos de casos ilustram a já citada recorrência de fatos ensejadores da necessidade de haver uma proteção normativa mais efetiva do titular de dados pessoais na Sociedade da Informação hiperconectada do século XXI. Eles abrangem, dentre aqueles que tiveram grande repercussão mundial, fatos noticiados pela imprensa, acusações de órgãos públicos, ações de governos, imposição de multas por órgãos públicos, entre outros.

Um marco histórico acerca da relação entre a privacidade dos dados pessoais e a liberdade necessária à democracia foi o conhecimento do público acerca do amplo acesso do governo dos Estados Unidos a informações pessoais de seus cidadãos e a comunicações privadas de chefes de Estado de outros países, revelado a nível mundial por meio de documentos secretos vazados para a imprensa pelo ex-servidor da agência de espionagem norte-americana Edward Snowden (GREENWALD, 2013a, 2013b; GREENWALD; KAZ; CASADO, 2013).

O acesso do governo dos Estados Unidos a essas informações teria se dado por meio da infraestrutura das operadoras de telecomunicação atuantes no País, ferramental que também possibilita a identificação do trajeto de suspeitos de crimes no âmbito de

investigações policiais, como ocorreu no Brasil nas investigações do caso Marielle (LAVADO, 2019).

Outros casos relacionados às telecomunicações no Brasil envolveram o mapeamento de dados de navegação de usuários na internet, supostamente sem o seu consentimento, para a criação de perfil e posterior venda a anunciantes (CASEMIRO; XAVIER, 2014) e o “hackeamento” de mensagens de autoridades políticas, do Poder Judiciário e do Ministério Público, e posterior divulgação pela imprensa, propiciado por vulnerabilidades das redes telefônicas (COMO..., 2019).

Colhe-se dos fatos noticiados, cada vez mais frequentes, que as violações de privacidade dos dados pessoais retratam, exemplificativamente:

- O vazamento de dados pessoais por ausência de controle interno de organizações que detêm as informações, por exemplo, cuja divulgação não fora consentida pelos titulares (GAVIOLI, 2019; NETSHOES..., 2019; COELHO, 2018a; URUPÁ, 2019; ANDRADE; HENRIQUE, 2019);
- O compartilhamento em desacordo com os termos do consentimento dado ou a venda ilícita dos dados pessoais para outro agente de mercado (JUIZ..., 2015; COELHO, 2018b; COX, 2020; GOOGLE..., 2011);
- A coleta de dados pessoais por meios e dispositivos diversos, sem autorização (ERNESTO, 2018; COMO..., 2018 LIXEIRA..., 2013; POMPEU, 2019), etc.

É possível, portanto, aliado ao já identificado dever constitucional de proteção dos dados pessoais, depreender a necessidade de maior proteção normativa à privacidade dos indivíduos por meio da tutela penal diante da observação de casos de diversos matizes envolvendo o uso de dados pessoais em desconformidade com o consentimento dado pelo titular ou cuja forma de consentimento, prescrita para ser específica e destacada em razão de o uso visar a um fim específico – como prevê a LGPD no art. 11 para o tratamento de dados pessoais sensíveis -, não fora observada.

Para ilustrar a conduta cuja tipificação penal será proposta com o intuito de a proscreever e de penalizar seu autor com maior rigor²⁷, insta destacar, em razão de figurar como fato motivador deste trabalho, o polêmico caso de compartilhamento indevido de dados pessoais envolvendo a maior rede social do mundo, o Facebook (FB), a empresa

²⁷ Não foi encontrado nenhum projeto de lei criminalizando o compartilhamento indevido de dados pessoais, apesar de Gondim (2019) ter relatado o intuito oral feito por dois parlamentares para inserir mecanismos de responsabilização criminal na LGPD.

britânica de pesquisas Global Science Research (GSR), comandada pelo pesquisador Aleksander Kogan, e a então consultoria de marketing político Cambridge Analytica (CA) (GRANVILLE, 2018).

Esse caso, amplamente noticiado e com repercussões jurídicas ainda em andamento em inúmeros países (SCORSIM, 2018; FACEBOOK..., 2020), servirá de suporte fático exemplar à tipificação penal que será proposta. Pois, como Farias, Otto e Souto (2019, p. 13) demonstraram, as medidas judiciais implementadas visaram apenas a indenizações específicas. Tais consequências são desproporcionais para dar azo à "nefasta repercussão para a sociedade" da falta de controle sobre o tratamento de dados pessoais.

A partir de março de 2018, a imprensa mundial passou a noticiar o uso de dados pessoais de 87 milhões de usuários do FB para a compilação de perfis psicológicos que foram usados na campanha de marketing digital do então candidato Donald Trump pela consultoria CA (FACEBOOK..., 2018). Da análise de reportagens (CAPELAS, 2018; ENTENDA..., 2018; SAIBA..., 2018), entrevistas (ROMANI, 2020; FACEBOOK, 2018b), documentários (AMER; NOUJAIM, 2019, on-line; HOBACK, 2013, on-line), dos fatos contidos no processo administrativo²⁸ que resultou na multa de R\$ 6.6 milhões imposta pela Secretaria Nacional do Consumidor ao FB em decorrência dos cerca de 443 mil brasileiros afetados (MJSP..., 2019), e para o que interessa a este trabalho, importa explicitar duas questões acerca do trajeto percorrido pelos dados pessoais: a forma do consentimento para seu tratamento e a finalidade para a qual o tratamento fora autorizado pelo titular (ESCÂNDALO..., 2018).

A primeira questão envolve o fato de a forma de consentimento para tratamento de dados pessoais sensíveis²⁹ de usuários do FB, de seus amigos e de amigos de amigos não ter sido destacada e específica, mas integrava, à época do caso, a configuração padrão do perfil do usuário recém cadastrado na plataforma (*opt-in*), violando os incisos VII, VIII e IX do art. 7º do MCI, vigente em solo brasileiro à época dos fatos.

Em manifestação no bojo do processo administrativo supracitado, o FB informou que, à época da aplicação do *quiz thisisyourdigitallife*, promovido pelo pesquisador Kogan, da GSR, e que possibilitou a coleta dos dados pessoais dos usuários do FB, a

²⁸ Processo nº 08012.000723/2018-19, cf. BRASIL, 2019.

²⁹ “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”, nos termos da LGPD.

política da plataforma permitia³⁰, por padrão, que o consentimento geral dado pelo usuário, por meio do aceite dos termos e condições de uso (*opt-in*) necessário para a criação de conta na plataforma ou para a participação no *quiz* do aplicativo, para que o FB compartilhasse seus dados com aplicativos parceiros abrangia os dados pessoais de seus amigos, quais sejam as informações presentes no perfil do indivíduo, algumas consideradas dados pessoais sensíveis (nome, gênero, data de nascimento, cidade natal e atual, estado civil, fotos, vídeos, educação – escolas frequentadas - páginas curtidas, local de trabalho, listas de amigos, atividades, interesses e atualizações de status) (BRASIL, 2019, p. 4, 23)³¹.

A respeito desse ponto, insta colacionar trecho esclarecedor da nota técnica que fundamentou a imposição da multa pelo Ministério da Justiça (BRASIL, 2019, p. 14):

Isso colocado, no presente caso, a simples adoção de um sistema de opt-out, em vez de um sistema de opt-in, tem implicações significativas. Afinal de contas, num sistema de opt-in, a quantidade de potenciais afetados no presente caso teria se limitado a oitenta e quatro usuários ou a um quantitativo não muito superior a isso (justamente aqueles usuários brasileiros que subscreveram o aplicativo *thisisyourdigitallife*), enquanto o sistema de opt-out implicou em um quantitativo superior a quatrocentos e quarenta mil usuários com seus dados expostos a tal aplicativo. Afinal de contas, é inverossímil acreditar que, num sistema em que sejam adotadas configurações-padrão de opt-in, os amigos de alguém que passasse a usar um aplicativo respondessem afirmativamente a cada solicitação de compartilhamento de dados que esse aplicativo fizesse a esses amigos. Ainda, é de se esperar que, caso esse fosse o modelo de negócios adotado pelas Representadas, a plataforma Facebook dificilmente teria a dimensão e porte (em capital, investimento e em capilaridade e quantidade de usuários) que possui atualmente.

³⁰ O que foi alterado entre 2014 e 2015 conforme a síntese das alegações do Facebook relatadas na Nota Técnica nº 32/2019/CGCTSA/DPDC/SENACON/MJ: “que foram ainda introduzidas mudanças na Plataforma Facebook, a partir de 30 de abril de 2014, com o objetivo de restringir os dados que aplicativos como o Dr. Aleksandr eram capazes de acessar” (BRASIL, 2019, p. 3) e “que essa política de dados foi atualizada em 2015, com a finalidade de tornar mais transparentes os mecanismos de controle de privacidade disponibilizados ao usuário pela plataforma” (BRASIL, 2019, p. 4).

³¹ Colhe-se a seguinte conduta das considerações finais da Nota Técnica nº 32/2019/CGCTSA/DPDC/SENACON/MJ (BRASIL, 2019, p. 26): “os Representados, pela adoção de um modelo de negócios que implicava em um padrão de configuração (decorrente de um *nudge*) de compartilhamento automático de dados de amigos (ou amigos de amigos etc.) de usuários com os aplicativos utilizados por esses últimos, deveriam ter um cuidado muito maior na gestão desses dados, uma vez que o modelo de consentimento adotado teve implicações relevantes para o número de pessoas com dados expostos (o qual é certamente muito maior do que se fosse adotado um modelo de opt-in para tal compartilhamento de tais dados). Neste particular, deve ser ponderado que tal lógica fez parte (pelo menos dentro do período em que se deram as condutas apuradas) do modelo de negócios da plataforma e, como tal, as Representadas também devem arcar com os riscos daí decorrentes quanto à proteção dos direitos de personalidade e da privacidade de seus usuários. Ainda quanto aos fatos em análise, as Representadas falharam em oferecer a proteção correspondente”

Assim, em razão de a grande maioria dos usuários sequer abrir os termos para leitura, havia um consentimento tácito do usuário para que não apenas seus dados fossem compartilhados, mas também o de seus amigos³². Ocorre que esse compartilhamento com os desenvolvedores do aplicativo abrangia dados pessoais sensíveis de terceiros, cujo consentimento para tratamento requer condições especiais, o que não fazia parte das políticas do FB³³. Constata-se, portanto, a transgressão do FB às normas de proteção de dados pessoais relativas à forma específica de consentimento necessária para o tratamento de dados pessoais sensíveis (art. 11, I, da LGPD – não vigente à época dos fatos; art. 7º, VII, VIII e IX, do MCI).

A segunda questão retrata a finalidade do tratamento de dados pessoais, sensíveis ou não, objeto de consentimento pelo titular das informações, vez que se considera a definição de consentimento da LGPD³⁴. Sabe-se que o compartilhamento de dados pessoais de usuários do FB à GSR de Kogan, por meio do aceite prévio do usuário do FB ao responder o *quiz*, foi autorizado pelo FB apenas para fins acadêmicos. Contudo, conforme os fatos amplamente veiculados e contrariamente à finalidade consentida pelos usuários do FB para tratamento de seus dados pessoais, de seus amigos e de amigos de amigos pelo aplicativo *thisisyourdigitallife*, a GSR comercializou os dados pessoais de milhares de usuários com a CA, a qual, por sua vez, utilizou-os para aplicar um método de perfilamento de indivíduos com o fim de influenciar eleitores não só nos Estados Unidos, mas também no México, na Malásia, na Austrália e na África do Sul (SUSPEITOS..., 2018).

Desta feita, porque desconforme com a finalidade consentida para o uso dos dados, observa-se o uso ilícito que foi feito pelo pesquisador Kogan, da GSR, e pela consultoria CA dos dados pessoais de usuários do FB, de seus amigos e de amigos de amigos, e até do FB caso fosse comprovado seu conhecimento acerca da comercialização dos dados pela GSR à CA. Portanto, as duas questões objeto de destaque para os fins deste trabalho, quais sejam a forma do consentimento e a finalidade para a qual o tratamento fora autorizado, retratam a violação das normas que prescrevem uma forma de consentimento específica em razão da sensibilidade das informações pessoais e das

³² Almeida e Almeida (2016) demonstram os efeitos deletérios da falta de leitura dos termos de uso.

³³ Nota Técnica nº 32/2019/CGCTSA/DPDC/SENACON/MJ, cf. BRASIL, 2019. Trechos da Nota (p. 7 e 21) atestam que o Facebook permitiu que terceiros utilizassem dados pessoais sensíveis dos consumidores sem a autorização específica e destacada requerida pelo MCI e hoje também pela LGPD.

³⁴ “Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”, conforme o art. 5º, XII da LGPD.

normas que autorizam o tratamento de dados pessoais, sensíveis ou não, para uma finalidade determinada mediante o consentimento do titular, falhas atestadas também por Farias, Otto e Souto (2019, p. 9).

Por conseguinte, em consonância com o que tem sido afirmado, mostra-se imperioso efetivar uma proteção normativa de maior grau jurídico à privacidade do titular de dados pessoais, sobretudo diante da proporção do caso analisado - exemplo significativo que foi detalhado³⁵ - e da frequência da veiculação de casos de compartilhamento indevido nos serviços integrantes dos modelos de negócios de empresas que exploram a crescente e permanente conectividade entre as pessoas na sociedade da informação do século XXI (TIM..., 2018; GOMES, 2018)³⁶. A prática de tais modelos abarca, e tem como base e referência, os serviços e produtos providos pelas gigantes mundiais da indústria tecnológica e do mercado digital propiciado pela exploração das funcionalidades das redes sociais (Google, Facebook, Twitter, Apple, Amazon etc.) (CAPELAS; WOLF, 2020; DANCE; LAFORGIA; CONFESSORE, 2018).

Assim, diante das constatações fáticas dos casos de violação de privacidade do titular de dados pessoais acima observados, sugere-se a criação de um tipo penal cujo *caput* reproduza a conduta de “fornecer, transmitir, compartilhar ou transferir dados pessoais, sob a forma de tratamento do art. 7º, I, da Lei 13.709 de 2018, de forma onerosa ou não, sem o consentimento livre, expresso, informado, destacado e específico do titular, ou em desconformidade com a finalidade de tratamento objeto do consentimento dado pelo titular”, com previsão de pena de reclusão de dois anos a cinco anos.

Do mesmo modo, é de se aventar o acréscimo da seguinte conduta equiparada na forma de um parágrafo: “incide na mesma conduta do *caput* o receptor ou o destinatário dos dados pessoais que tem conhecimento que o compartilhamento foi feito sem o consentimento livre, expresso, informado, destacado e específico do titular, ou em desconformidade com a finalidade de tratamento objeto do consentimento dado pelo titular”. É de se ressaltar novamente que os tipos penais em vigor no Brasil não abarcam

³⁵ Se tais fatos ocorreram com a maior rede social do mundo, mesmo sob rígidos controles internos e sob observação de órgãos públicos de controle de diversos países, indaga-se o que já pode ter ocorrido, o que está a acontecer ou o que certamente acontecerá em organizações de menor abrangência, se comparadas ao Facebook.

³⁶ Em resposta a crítica pública do CEO da Apple, Tim Cook, o CEO do Facebook, Mark Zuckerberg, assim se pronunciou: “Se você deseja criar um serviço que ajude a conectar todos no mundo, há muitas pessoas que não podem pagar. E um modelo apoiado por publicidade é o único modo racional”. ‘Isso não significa que não estamos focados em servir pessoas’, afirmou. Zuckerberg disse ainda que o modelo do uso de dados privados como forma de monetização é ‘a única forma possível de manter a plataforma funcionando’ (TIM..., 2018).

as referidas condutas, que terminam por não sofrer a punição necessária por parte do direito para dissuadir os sujeitos de sua prática.

Os sujeitos ativo e passivo desse crime, no Direito Penal brasileiro, só podem ser pessoas naturais, já que a pessoa jurídica, como ente abstrato que é, não possui capacidade penal, visto ser desprovida de vontade natural de ação e de capacidade de culpabilidade (BITENCOURT, 2018, p. 313), salvo os casos de delitos ambientais específicos. Sendo assim, em meio a um esforço de uniformização da interpretação da legislação referente à proteção de dados pessoais, a análise eventual de autoria da referida conduta poderia se voltar às pessoas naturais que se amoldam à figura do controlador³⁷ ou do operador, observadas as definições do art. 5º da LGPD, e a verificação do sujeito passivo se adstringiria ao titular dos dados pessoais.

De acordo com o redação do tipo sugerido, condutas como as desenvolvidas pelo Facebook, por meio de seus funcionários – controlador ou operadores – e pelo pesquisador Kogan seriam sancionadas, uma vez que não houve consentimento livre, expresso, informado, destacado e específico do titular para que seus dados pessoais sensíveis fossem utilizados para fins de propaganda eleitoral personalizada no Facebook, como ocorreu na campanha presidencial estadunidense de 2016, mas apenas para fins de pesquisa acadêmica.

Da mesma forma, seria sancionada a conduta hipotética de determinado controlador ou operador dos dados pessoais do usuário de um navegador web que comercializasse, sem o consentimento ou em desconformidade com a finalidade do uso dos dados autorizada pelo titular, os dados pessoais com fornecedores de produtos de varejo para direcionamento de conteúdos adequados ao interesse dos clientes demonstrado pelas evidências de navegação rastreadas por cookies no navegador web, por exemplo. Assim, juntamente com a intenção de cometer o delito (dolo), observa-se que o consentimento³⁸ e a finalidade do uso dos dados pessoais traduzem os elementos determinantes da configuração do tipo penal.

³⁷ Convém destacar que a ANPD considera que a pessoa natural só poderá ser controladora, nos termos da LGPD, “nas situações em que é a responsável pelas principais decisões referentes ao tratamento de dados pessoais. Nessa hipótese, a pessoa natural age de forma independente e em nome próprio – e não de forma subordinada a uma pessoa jurídica ou como membro de um órgão desta. É o que ocorre, por exemplo, com os empresários individuais, os profissionais liberais (como advogados, contadores e médicos) e os responsáveis pelas serventias extrajudiciais” (BRASIL, 2021, p. 10).

³⁸ Tendo como pano de fundo o caso aqui relatado envolvendo o Facebook e a Cambridge Analytica, Bezerra e Furtado (2020, p. 8) concluem que “o compartilhamento de informações do perfil digital (*profiling*) do consumidor criado a partir da coleta e do tratamento de seus dados (*data mining*) pode gerar

A criminalização dessa conduta na forma da redação sugerida advém em razão da exigência do princípio da proibição de proteção insuficiente, em especial em razão do déficit normativo da proteção dos dados pessoais na seara penal. Para que eventual formulação de crime respeite as diretrizes constitucionais de *lege ferenda*, é preciso observar, para os fins deste trabalho, os seguintes princípios do Direito Penal: a ofensividade, a intervenção mínima e a tipicidade.

A redação sugerida para a conduta é passível de intervenção penal em razão da elevada ofensividade ao bem jurídico que se visa tutelar, pois que há perigo de dano concreto, real e efetivo à privacidade do titular de dados pessoais quando o tratamento de tais informações é realizado em desconformidade com a manifestação livre, expressa e obrigatoriamente informada, destacada e específica do titular que consentiu com o uso dos dados para uma finalidade determinada, nos termos da definição de “consentimento” dada pelo inciso XII do art. 5º da LGPD. A tipicidade, traduzida na “conformidade do fato praticado pelo agente com a moldura abstratamente descrita na lei penal” (BITENCOURT, 2018, p. 356), encontra-se na redação proposta, vez que a conduta típica deve ser a mais precisa possível.

Por fim, a intervenção mínima como princípio está presente na medida em que se utiliza do Direito Penal como *ultima ratio* do sistema normativo, orientando e limitando o poder incriminador do Estado, para proteger efetivamente a privacidade do titular de dados pessoais (BITENCOURT, 2018, p. 56). Tal princípio se liga semanticamente a outros dois princípios primordiais para o objeto desse trabalho, vez que fundamentam a necessidade da intervenção do Direito Penal na tutela da privacidade dos dados pessoais, quais sejam: a fragmentariedade e a subsidiariedade.

A fragmentariedade consiste em um princípio norteador da seletividade de bem jurídico essencial à coexistência humana cuja proteção então receberá a intervenção grave do Direito Penal - pois que proporciona constrição à liberdade como pena. Tal intervenção se faz necessária diante da necessidade de proteger o bem jurídico – no caso deste trabalho a privacidade dos dados pessoais - contra “condutas tendentes à produção de danos mais graves e relevantes”, consoante Pacelli e Callegari (2020, p. 81). Desta feita, atesta-se a fragmentariedade da criminalização de conduta atentatória ao direito fundamental de proteção de dados pessoais.

limitações à utilização de serviços, causar-lhe estímulo ao consumismo e até mesmo afetar o livre exercício de sua cidadania”. Para eles, a utilidade ao consumidor do tratamento de dados pessoais está na necessária e adequada informação de todos os riscos e implicações da atividade ao titular.

Por sua vez, o princípio da subsidiariedade se faz presente nessa incriminação legal quando resta ao Direito Penal intervir para a efetiva proteção do bem jurídico violado³⁹, vez que a proteção conferida por demais ramos do Direito se mostra insuficiente para uma tutela adequada e eficaz (BITENCOURT, 2018, p. 57). Assim, o Direito Penal termina por defender o bem jurídico de eventual violação de forma subsidiária, como última alternativa, assemelhando-se, em certo sentido, ao princípio da intervenção mínima.

É nesse sentido que se reafirma a incapacidade de o Direito Civil e Administrativo tutelar, de maneira integral e segura, a privacidade dos dados pessoais, bem jurídico tão relevante para a vida do indivíduo e da sociedade. Desse modo, é necessário que se empregue a tipificação penal da conduta suprarreferida para que o direito fundamental à proteção de dados pessoais seja assegurado de forma mais efetiva diante dos desafios vividos pela sociedade hiperconectada dos tempos atuais, sendo certa sua insuficiência para abarcar todas as condutas lesivas a esse direito fundamental.

CONCLUSÃO

Em arremate, viu-se neste trabalho que falar de dados pessoais é falar da pessoa humana. Os dados sobre um indivíduo (nome, idade, profissão, estado civil, endereço, gostos...) traduzem clara extensão da personalidade humana visto que, na operacionalização dos serviços de muitas organizações, uma pessoa termina por ser tratada como o conjunto de suas informações cadastrais e específicas. Esses processamentos de informações têm se intensificado cada vez mais em razão da exponencial evolução tecnológica que tem transformado o modo como as pessoas se relacionam com os objetos.

Assim, tendo em vista a premente preservação da autonomia do indivíduo e da dignidade humana, o tratamento dos dados pessoais deve necessariamente envolver condicionantes e limites que protejam a liberdade dos titulares de dados pessoais. No entanto, as tutelas cível e administrativa que sustentam coercitivamente tais limitações sob pena de sanções pecuniárias têm se mostrado insuficientes diante do crescente

³⁹ Ressalta-se que o § 2º do art. 52 da LGPD não deixa dúvida acerca da possibilidade de o Direito Penal vir a tutelar a privacidade mesmo diante das sanções administrativas que tal Marco Legal instituiu, pois essas não substituem a aplicação de sanções administrativas, civis ou penais do Código de Defesa do Consumidor ou de outra norma específica.

aumento do número de casos de violação da privacidade por meio do tratamento indevido dessas informações, isto é, feito sem o consentimento do titular ou em desconformidade com a finalidade do uso objeto do consentimento.

Verificou-se, desde o escândalo revelado pelo ex-agente da CIA, Edward Snowden, uma série de casos polêmicos relativos, principalmente, ao compartilhamento ou à comercialização indevida de informações pessoais. Com a existência de legislações específicas sobre o assunto, os fatos que retratam violações à privacidade dos dados avolumam-se a nível mundial, uma vez que eles hoje são o principal insumo econômico transacionado em quase todos os setores da indústria, do comércio e dos serviços.

Desse modo, atestou-se a imperiosa necessidade de se empreender a inserção da tutela penal ao aparato jurídico da proteção dos dados pessoais, considerados como elementos centrais à consecução desse objetivo a salvaguarda do consentimento e da finalidade do tratamento de dados pessoais. Isso explica a redação do tipo penal proposto para se inibir a desconsideração do consentimento, ou sequer de sua colheita, e a infração à regra permissiva, consentida pelo titular, para uso dos dados para fins determinados. Por exemplo, admite-se a coleta de dados para tratamento que possibilite a participação em consulta médica, enquanto o que ocorre, em verdade, é a venda de tais informações a planos de saúde locais para formatação de ofertas e prospecção de clientes.

O consentimento referido, como proposto, deve ser livre, expresso, informado, destacado e específico. Isso porque ele se constitui em instrumento apto a prover o equilíbrio de forças entre as organizações e os indivíduos, os quais podem apresentar vulnerabilidades cognitivas de ordem fática, técnica e jurídica. Informar ao titular acerca dos riscos e implicações abrangidas no tratamento de seus dados concede-lhe a oportunidade do exercício de sua autodeterminação informativa.

Da mesma forma, o tipo sugerido procura atender aos ditames dos princípios da finalidade e da adequação ao impor ao tratamento de dados a observância estrita à finalidade do uso consentida pelo titular para propósitos, no dizer do legislador, legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com tais fins. Essa compatibilidade é um elemento fundamental a ser protegido pelo tipo penal proposto, o qual não abarca, em hipótese alguma, todas as condutas ofensivas ao bem jurídico da privacidade.

Desse modo, busca-se elevar o nível jurídico de proteção dos dados pessoais a fim de obstar práticas e condutas que buscam burlar o conhecimento, de fato, do titular acerca do tratamento que será engendrado pelo controlador ou pelo operador com o intuito de

auferir o maior proveito possível de tais informações. Espera-se que, com tal criminalização, em razão dos riscos reputacionais e financeiros, as plataformas de produtos e serviços passem a dispor de forma separada e mais clara ao titular quais serão os fins e os riscos do consentimento, expurgando as solitárias, e repugnantes, opções de aceites definitivos de todas as regras de uso e a implementação de configurações padrão que importem em devassa à privacidade do usuário sem seu conhecimento destacado, conforme se deu no caso do FB, que foi obrigado a alterar suas políticas de privacidade após o escândalo da CA em decorrência do poder fiscalizatório das autoridades norte-americanas.

Nota-se, portanto, a necessidade de se instituir uma tutela jurídica mais efetiva, qual seja a penal. Nesse intento, ao observar o postulado da proporcionalidade, deve-se buscar o equilíbrio dos valores constitucionais quando da instituição de um tipo penal, mesmo que se procure o efeito simbólico da criminalização, e não o efetivo encarceramento, a fim de inibir os indivíduos do cometimento de tais condutas violadoras da privacidade do titular de dados pessoais.

REFERÊNCIAS

ALMEIDA, Juliana E. de; ALMEIDA, Daniel E. Vasconcelos. A ditadura do algoritmo e a proteção da pessoa humana: uma análise do controle do SI eletrônico. **Revista de Direito Privado**, v. 69, p. 29-43, set. 2016.

AMAZON desiste de ferramenta secreta de recrutamento que mostrou viés contra mulheres. **Época**, 10 out. 2018. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2018/10/amazon-desiste-de-ferramenta-secreta-de-recrutamento-que-mostrou-vies-contramulheres.html>. Acesso em: 15 jun. 2021.

AMER, Karim; NOUJAIM, Jehane. Privacidade Hackeada (1h54 min). **Netflix**, 24 jul. 2019. Disponível em: <https://www.netflix.com/br/title/80117542>. Acesso em: 11 ago. 2020.

ANDRADE, Vitor Morais de; HENRIQUE, Lygia Maria M. Molina. Vazamento de dados: uma preocupação da Lei Geral de Proteção de Dados. **Migalhas**, 21 mar. 2019. Disponível em: <https://www.migalhas.com.br/depeso/298452/vazamento-de-dados-uma-preocupacao-da-lei-geral-de-protecao-de-dados>. Acesso em: 18 out. 2020.

BEZERRA, Daniel Teixeira; FURTADO, Gabriel Rocha. Privacidade, consentimento informado e proteção de dados do consumidor na internet [artigo eletrônico]. **Revista de Direito do Consumidor**, v. 128, p. 205-225, mar./abr. 2020.

BIONI, B. R.; RIELLI, M. M.; ZANATTA, R. A. F. Petição de Amicus Curiae na ADI 6.387. **Associação Data Privacy Brasil de Pesquisa**, 5 abr. 2020. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbr_amicuscuria_stf_ibge.pdf. Acesso em: 18 jun. 2020.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral** 1. 24. ed. São Paulo: Saraiva Educação, 2018.

BOLSONARO sanciona e LGPD entra em vigência nesta sexta-feira. **Valor Econômico**, 17 set. 2020. Disponível em: <https://valor.globo.com/empresas/noticia/2020/09/17/bolsonaro-sanciona-e-lgpd-entra-em-vigencia-nesta-sexta-feira.ghtml>. Acesso em: 3 nov. 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília: Autoridade Nacional de Proteção de Dados; Governo Federal, maio 2021. 23 p. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado>. Acesso em: 3 jul. 2021.

BRASIL é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. **Secretaria-Geral da Presidência da República**, Relações Internacionais, 24 jul. 2020. Disponível em: <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contraa-criminalidade-cibernetica>. Acesso em: 3 jul. 2021.

BRASIL. **Constituição Federal**, de 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 maio 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet (MCI). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 11 ago. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 jan. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. Processo Nº 08012.000723/2018-19. Nota Técnica nº 32/2019/CGCTSA/DPDC/SENACON/MJ. **Departamento de Proteção e Defesa do Consumidor (DPDC) - Secretaria Nacional do Consumidor (SENACON)**, 27 dez. 2019. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/01/SEI_08012.000723_2018_19-1-1.pdf. Acesso em: 11 ago. 2020.

CALABRICH, Bruno F. de C. Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais. **Revista de Direito e as Novas Tecnologias**, v. 8, jul./set. 2020.

CAPELAS, Bruno. Facebook perde US\$ 128 bi em valor de mercado e vê conta de escândalos chegar. **O Estado de São Paulo**, 25 jul. 2018. Disponível em: <https://link.estadao.com.br/noticias/empresas,acoes-do-facebook-caem-20-apos-queda-em-crescimento-de-usuarios,70002415365>. Acesso em: 11 ago. 2020.

CAPELAS, Bruno; WOLF, Giovanna. Gigantes de tecnologia são postas em xeque em depoimento histórico nos EUA. **O Estado de São Paulo**, 29 jul. 2020. Disponível em: <https://link.estadao.com.br/noticias/empresas,gigantes-de-tecnologia-sao-postas-em-xeque-em-depoimento-historico-nos-eua,70003380480>. Acesso em: 11 ago. 2020.

CARVALHO, Claudia da Costa B. de. O crime de apropriação indébita digital e a conservação ilícita de dados, de acordo com as normas da LGPD. **Revista de Direito e as Novas Tecnologias**, v. 6, p. 127-139, jan./mar. 2020.

CASEMIRO, Luciana; XAVIER, Luiza. Oi é multada em R\$ 3,5 milhões por invasão de privacidade feita por Velox. **O Globo**, 23 jul. 2014. Disponível em: <https://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505>. Acesso em: 10 ago. 2020.

CASTELLS, Manuel. **A sociedade em rede**: a era da informação, economia, sociedade e cultura. 8. ed. São Paulo: Paz e Terra, 2005.

COELHO, Gabriela. MP-DF pede a condenação de banco por vazamento de dados pessoais. **Conjur**, 31 jul. 2018a. Disponível em: <https://www.conjur.com.br/2018-jul-31/mp-df-condenacao-banco-vazamento-dados-pessoais>. Acesso em: 18 out. 2020.

COELHO, Gabriela. MP-DF acusa empresa pública de vender dados pessoais de brasileiros. **Conjur**, 31 maio 2018b. Disponível em: <https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros>. Acesso em: 18 out. 2020.

COMO Alexa, a assistente virtual da Amazon, gravou e compartilhou mensagem privada de casal. **G1**; **BBC**, 29 maio 2018. Disponível em: (<https://g1.globo.com/economia/tecnologia/noticia/como-alexa-a-assistente-virtual-da-amazon-gravou-e-compartilhou-mensagem-privada-de-casal.ghtml>). Acesso em: 18 out. 2020.

COMO agiram os suspeitos de invadir o celular de Moro, segundo investigação. **BBC Brasil**, 24 jul. 2019. Disponível em: <https://www.bbc.com/portuguese/brasil-49103904>. Acesso em: 10 ago. 2020.

COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade**. 4. ed. São Paulo: Revista dos Tribunais, 2007.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. São Paulo: Thomson Reuters, 2019.

COX, Joseph. Documentos vazados expõem o mercado secreto para seus dados de navegação. Trad. por Marina Schnoor. **Vice**, 29 jan. 2020. Disponível em: https://www.vice.com/pt_br/article/qjdkq7/documentos-vazados-expoem-o-mercado-secreto-para-seus-dados-de-navegacao. Acesso em: 18 out. 2020.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CRUZ, Fernanda Paula Sousa; NAVARRO, Jenifer Ponce. A LGPD e a responsabilidade penal. **Jus Navigandi**, maio 2020. Disponível em: <https://jus.com.br/artigos/81849/algpd-e-a-responsabilidade-penal>. Acesso em: 9 set. 2020.

DAMASCENO, Paulo Victor Medeiros. **A invasão do dispositivo informático e a tutela penal da privacidade**. 2014. 64 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal do Ceará (UFC), Fortaleza, 2014.

DANCE, Gabriel J. X.; LAFORGIA, Michael; CONFESSORE, Nicholas. Facebook abriu privacidade de dados de usuários para gigantes da tecnologia (*The New York Times*). **O Estado de São Paulo**, 19 dez. 2018. Disponível em: <https://link.estadao.com.br/noticias/empresas,facebook-abriu-privacidade-de-dados-de-usuarios-para-gigantes-da-tecnologia,70002652334>. Acesso em: 11 ago. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da Lei geral de proteção de dados. São Paulo: Thomson Reuters Brasil, 2019.

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades (BBC). **G1 Globo**, 20 mar. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 11 ago. 2020.

ERNESTO, Marcelo. Drogaria Araujo é multada em quase R\$ 8 milhões por pedir CPF de clientes. **Estado de Minas**, 6 dez. 2018. Disponível em: https://www.em.com.br/app/noticia/economia/2018/12/06/internas_economia,1011120/drogaria-araujo-e-multada-em-quase-r-8-milhoes-por-pedir-cpf-de-clien.shtml. Acesso em: 18 out. 2020.

ESCÂNDALO do Facebook: entenda como dados pessoais foram obtidos por empresa de marketing político. **O Globo**, com agências internacionais, 20 mar. 2018. Disponível em: <https://oglobo.globo.com/economia/escandalo-do-facebook-entenda-como-dados-pessoais-foram-obtidos-por-empresa-de-marketing-politico-22507080>. Acesso em: 11 ago. 2020.

ESTRADA, Manuel Martín Pino. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. **Revista de Direito do Trabalho**, v. 172, p. 35-54, nov./dez. 2016.

FACEBOOK revela que dados de 87 milhões foram usados por consultoria. **O Estado de São Paulo**, 4 mar. 2018. Disponível: <https://link.estadao.com.br/noticias/empresas,facebook-diz-que-87-milhoes-de-usuarios-tiveram-dados-usados-por-cambridge-analytica,70002254468>. Acesso em: 11 ago. 2020.

FACEBOOK sabia que dados poderiam ser vendidos, diz Aleksandr Kogan. **UOL**, 23 abr. 2018b. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/04/23/facebook-sabia-que-dados-poderiam-ser-vendidos-diz-aleksandr-kogan.htm>. Acesso em: 11 ago. 2020.

FACEBOOK pode ser multado em US\$ 348 bi na Austrália por violação de privacidade. **O Estado de São Paulo**, 9 mar. 2020. Disponível em: <https://link.estadao.com.br/noticias/empresas,facebook-pode-ser-multado-em-us-348-bi-na-australia-por-violacao-de-privacidade,70003225632>. Acesso em: 11 ago. 2020.

FARIAS, Gabrielle Graça de; OTTO, Samira; SOUTO, Gabriel Araújo. Caso Facebook e Cambridge Analytica: o GDPR e a nova Lei Brasileira (13.709/2018) [artigo eletrônico]. **Revista de Direito e as Novas Tecnologias**, v. 4, jul./set. 2019.

FELDENS, Luciano. **Direitos fundamentais e direito penal: a constituição penal**. 2 ed. Porto Alegre: Livraria do Advogado, 2012.

FERNANDES, Elora Raad; OLIVEIRA, Jordan V. de. Quanto valem seus dados? O caso Google Opinion Rewards. **Revista de Direito e as Novas Tecnologias**, v. 7, abr./jun. 2020.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de**

São Paulo, n. 88, p. 439-459, jan./dez. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 3 mar. 2020.

FORTES, Vinícius Borges. **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**. 2015. 225 f. Tese (Doutorado em Direito) -Universidade Estácio de Sá, Rio de Janeiro, 2015.

FRAZÃO, Ana. Proteção de dados e expectativas para 2020. **Jota**, 12 fev. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/protecao-de-dados-e-expectativas-para-2020-12022020>. Acesso em: 5 set. 2020.

GAVIOLI, Allan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. **InfoMoney**, São Paulo, 10 out. 2019. Disponível em: <https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/>. Acesso em: 18 out. 2020.

GOMES, Helton S. Gigantes da internet sabem por onde você anda, que lugares frequenta e com quem fala; entenda. **G1 Globo**, 12 abr. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/gigantes-da-internet-sabem-por-onde-voce-anda-que-lugares-frequenta-e-com-quem-fala-entenda.ghtml>. Acesso em: 11 ago. 2020.

GONDIM, Abnor. Deputados querem responsabilidade criminal na LGPD. **Tele.Síntese**, 13 ago. 2019. <https://www.telesintese.com.br/deputados-querem-responsabilidade-criminal-na-lgpd/>. Acesso em: 9 set. 2020.

GOOGLE é multada por coleta indevida de dados. **Conjur**, 22 mar. 2011. Disponível em: <https://www.conjur.com.br/2011-mar-22/franca-multa-google-100-mil-euros-coleta-indevida-dados>. Acesso em: 18 out. 2020.

GRANVILLE, Kevin. Como a Cambridge Analytica recolheu dados do Facebook. **Folha de São Paulo**, 21 mar. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/como-a-cambridge-analytica-recolheu-dados-do-facebook.shtml>. Acesso em: 11 ago. 2020.

GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. **The Guardian – US News**, 6 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. Acesso em: 10 ago. 2020.

GREENWALD, Glenn. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. **The Guardian – US News**, 31 jul. 2013. Disponível em: <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>. Acesso em: 10 ago. 2020.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. EUA espionaram milhões de e-mails e ligações de brasileiros. **O Globo**, 6 jul. 2013. Disponível em:

<https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em: 10 ago. 2020.

GUARDIA, Andrés Felipe T. S. De Surveillance a Dataveillance: enfoque a partir da noção jurídica de tratamento de dados. **Revista dos Tribunais**, v. 1012, p. 135-151, fev. 2020.

HISSA, C. B.; LIMA, Ana Paula M. C. de L.; SALDANHA, P. M. (Coords.). **Direito Digital: debates contemporâneos**. São Paulo: Revista dos Tribunais, 2019.

HOBACK, Cullen. Sujeito a termos e condições (58 min). **Daily Motion**, 12 jul. 2013. Disponível em: <https://www.dailymotion.com/video/x3okve4>. Acesso em: 11 ago. 2020.

JUIZ determina suspensão de site que vende dados pessoais de brasileiros. **ConJur**, 30 jul. 2015. Disponível em: <https://www.conjur.com.br/2015-jul-30/juiz-manda-suspender-site-vende-dados-pessoais-brasileiros>. Acesso em: 18 out. 2020.

JUNQUEIRA, Thiago. **Tratamento de dados pessoais e discriminação algorítmica nos seguros**. São Paulo: Revista dos Tribunais, 2020.

LAVADO, Thiago. Investigação hi-tech: como a polícia fuçou buscas e localização de celular para chegar aos suspeitos de matar Marielle. **G1 – Globo.com**, 12 mar. 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/03/12/investigacao-hi-tech-como-a-policia-fucou-buscas-e-localizacao-de-celular-para-chegar-aos-suspeitos-de-matar-marielle.ghtml>. Acesso em 10 ago. 2020.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.

LIXEIRA conectada deixa ruas de Londres após coletar dados móveis. **G1**, 12 ago. 2013. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/08/lixeira-conectada-deixa-ruas-de-londres-apos-coletar-dados-moveis.html>. Acesso em: 18 out. 2020.

LUCCA, Newton de.; SIMÃO FILHO, Adalberto; LIMA, Cíntia R. P. de (Coords.). **Direito & Internet III**. Marco Civil da Internet. Lei Nº 12.965/ 2014. São Paulo: Quartier Latin, 2015.

MALHEIRO, Emerson P.; VIGLIAR, José Marcelo M. A execução da atividade do estado no acompanhamento do mercado e as suas consequências nas pessoas na sociedade da informação. **Revista dos Tribunais**, v. 1.019, p. 57-71, set. 2020.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). **Direito Digital: direito privado e internet**. 2. ed. São Paulo: Editora Foco, 2019.

MATTIUZZO, Marcela. Propaganda online e privacidade - o varejo de dados pessoais na perspectiva antitruste. **Revista do IBRAC – Direito da Concorrência, Consumo e Comércio Internacional**, v. 26, p. 295-314, jul./dez. 2014.

MATTIUZZO, Marcela. Discriminação algorítmica: reflexões no contexto da Lei Geral de Proteção de Dados Pessoais. In: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo;

MENDES, Laura Schertel. **Lei Geral de Proteção de Dados (Lei nº 13.709/2018):** a caminho da efetividade: contribuições para a implementação da LGPD [livro eletrônico]. Brasília: Revista dos Tribunais, 2020. p. 7.1- 7.4.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 12. ed. São Paulo: Saraiva, 2017.

MJSP multa Facebook em R\$ 6,6 milhões. **Ministério da Justiça e Segurança Pública**, 30 dez. 2019. Disponível em: <https://www.novo.justica.gov.br/news/mjssp-multa-facebook-em-r-6-6-milhoes>. Acesso em: 11 ago. 2020.

NETSHOES terá de pagar R\$ 500 mil por vazamento de dados de 2 milhões de clientes. **G1**, Brasília, 5 fev. 2019. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml>. Acesso em: 18 out. 2020.

NOGUEIRA, Hendri. **A utilização de dados pessoais no meio digital e a (im)possibilidade de lesão ao direito à privacidade**. 2019. 85 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade do Sul de Santa Catarina (UNISUL), Florianópolis, 2019.

NOVELINO, Marcelo. **Curso de direito constitucional**. 14. ed. Salvador: Ed. JusPodivm, 2019.

OLIVA, Milena Donato. Discriminação algorítmica nas relações de consumo. **Migalhas**, 23. fev. 2021. Disponível em: <https://www.migalhas.com.br/depeso/340680/discriminacao-algoritmica-nas-relacoes-de-consumo>. Acesso em: 15 jun. 2021.

OLIVEIRA, Tainá Cristina de. **Privacidade na internet à luz do Direito Penal**. 2012. 134 f. Trabalho de Conclusão de Curso (Graduação em Direito Penal) – Centro de Ciências Sociais Aplicadas da Universidade Estadual do Norte do Paraná (UENP), Jacarezinho–PR, 2012.

PASSI, Renata C. Z. Q.; TEIXEIRA, Tarcisio. Privacidade na internet: a formação de bancos de dados e a transformação das pessoas em mercadorias. **Revista dos Tribunais**, v. 990, p. 109-125, abr. 2018.

POMPEU, Ana. MJ instaura processo contra Google Brasil por violação de privacidade. **ConJur**, 7 fev. 2019. Disponível em: <https://www.conjur.com.br/2019-fev-07/ministerio-abre-processo-google-violacao-privacidade>. Acesso em: 18 out. 2020.

PINHEIRO, Patricia Peck. A janela indiscreta das aplicações digitais: vazamentos de dados escancaram a falta de garantia de segurança na internet. **Revista dos Tribunais**, São Paulo, ano 108, vol. 1007, p. 363-367, set. 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Elaboratori elettronici e controllo sociale**. Bologna: Il Mulino, 1973.

RODRÍGUEZ, Víctor Gabriel. **Tutela penal da intimidade**: perspectivas da atuação penal na sociedade da informação. São Paulo: Atlas, 2008

ROMANI, Bruno. ‘As pessoas foram enganadas para dar algo valioso: seus dados’, diz Brittany Kaiser. **O Estado de São Paulo**, 19 abr. 2020. Disponível em: <https://link.estadao.com.br/noticias/cultura-digital,as-pessoas-foram-enganadas-para-dar-algo-valioso-seus-dados-diz-brittany-kaiser,70003275070>. Acesso em: 11 ago. 2020

SAIBA quem é o psicólogo por trás da polêmica do uso de dados do Facebook (Bloomberg). **O Globo**, 20 mar. 2018. Disponível em: <https://oglobo.globo.com/economia/saiba-quem-o-psicologo-por-tras-da-polemica-do-uso-de-dados-do-facebook-22507501>. Acesso em: 11 ago. 2020.

SANDRIN, Pedro J. P.; SILVA, Julia X. R. da. Possíveis reflexos penais da Lei Geral de Proteção de Dados. **Migalhas**, 28 fev. 2020. Disponível em: <https://www.migalhas.com.br/depeso/320959/possiveis-reflexos-penais-da-lei-geral-de-protecao-de-dados>. Acesso em: 7 set. 2020.

SANTOS, Daniel Leonhardt dos. **Crimes de informática e bem jurídico-penal**: contributo à compreensão da ofensividade em direito penal. 2014. 146 f. Dissertação (Mestrado em Ciências Criminais) - Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS, Porto Alegre, 2014.

SAUAIA, Hugo Moreira Lima. **A proteção dos dados pessoais no Brasil**. Rio de Janeiro: Lumen Juris, 2018.

SCHERTEL MENDES, Laura Ferreira. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

SCHERTEL MENDES, Laura Ferreira. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/655/905>. Acesso em: 30 ago. 2020.

SCHERTEL MENDES, Laura Ferreira. A encruzilhada da proteção de dados no Brasil e o caso do IBGE, **Jota**, 23 abr. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020>. Acesso em: 11 ago. 2020.

SCORSIM, Ericson M. Coleta ilegal de dados pessoais na plataforma do Facebook: o impacto global do fato e a regulação setorial em cada país. **Migalhas**, 5 abr. 2018. Disponível em: <https://www.migalhas.com.br/depeso/277671/coleta-ilegal-de-dados-pessoais-na-plataforma-do-facebook-o-impacto-global-do-fato-e-a-regulacao-setorial-em-cada-pais>. Acesso em 11 ago. 2020.

SILVA, Carlos Bruno Ferreira da. **Proteção de dados e cooperação transnacional**: teoria e prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes, 2014.

SILVA, César Dario Mariano da. **Tutela penal da intimidade**. Curitiba: Juruá, 2015.

SIQUEIRA JR., Paulo Hamilton. Direitos humanos e cidadania digital. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015. t. 1.

SOUTO, Gabriel Araújo. Vazamento de dados no setor privado brasileiro: a gestão do risco como parâmetro para a responsabilidade empresarial. **Revista de Direito e as Novas Tecnologias**, v. 7, abr./jun. 2020.

STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. **Supremo Tribunal Federal – imprensa - notícias STF**, 07 maio 2020. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1>. Acesso em: 19 jun. 2021.

SUSPEITOS de usar dados vazados do Facebook são flagrados em vídeo dizendo que consultoria trapaceia em eleições, diz TV. **G1 Globo**, 19 mar. 2018. Disponível em: <https://g1.globo.com/mundo/noticia/suspeitos-de-usar-dados-vazados-do-facebook-sao-flagrados-em-video-dizendo-que-consultoria-trapaceia-em-eleicoes-diz-tv.ghtml>. Acesso em: 11 ago. 2020.

TADEU, Silney Alves. Um novo direito fundamental: algumas reflexões sobre a proteção da pessoa e o uso informatizado de seus dados pessoais. **Revista de Direito do Consumidor**, v. 79, p. 83-100, jul./set. 2011.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dado pessoais**: comentada artigo por artigo. Salvador: Ed. Juspodivm, 2019.

TIM Cook critica uso de dados pessoais como 'armas' por empresas de tecnologia. **O Estado de São Paulo**, 24 out. 2018. Disponível em: <https://link.estadao.com.br/noticias/empresas,tim-cook-critica-o-complexo-industrial-de-dados-criado-por-empresas,70002561578>. Acesso em: 11 ago. 2020.

URUPÁ, Marcos. Intervozes aciona Vivo na justiça por vazamento de dados pessoais. **TeleTime**, 7 jan. 2019. Disponível em: <https://teletime.com.br/07/01/2020/intervozes-aciona-vivo-na-justica-por-vazamento-de-dados-pessoais/>. Acesso em: 18 out. 2020.

VAINZOF, Rony. LGPD em vigor: o que muda? **Thomson Reuters Brasil**, 18 set. 2020. Disponível em: <https://www.thomsonreuters.com.br/pt/juridico/blog/lgpd-em-vigor-o-que-muda.html>. Acesso em: 5 nov. 2020.

VALENTINI, R.; HADDAD, L. A lei geral de proteção de dados e os seus possíveis reflexos penais. **Portal Migalhas**, 30 out. 2019. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI313882,91041-A+lei+geral+de+protecao+de+dados+e+os+seus+possiveis+reflexos+penais>. Acesso em: 28 dez. 2019.

WARREN, Samuel; BRANDEIS, Louis. *The right to privacy*. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em:

<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 14 jun. 2020.

WESTIN, Alan. **Privacy and freedom**. Nova York: Atheneum, 1967.

ZANATTA, Rafael A. F. A Proteção de Dados Pessoais entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. *In*: LUCCA, Newton de.; SIMÃO FILHO, Adalberto; LIMA, Cíntia R. P. de (Coords.). **Direito & Internet III. Marco Civil da Internet. Lei Nº 12.965/ 2014**. São Paulo: Quartier Latin, 2015. t. 1. p. 447-470.

ZANATTA, Rafael A. F.; ABRAMOVAY, Ricardo. Dados, vícios e concorrência: repensando o jogo das economias digitais. **Estudos Avançados**, São Paulo, v. 33, n. 96, p. 421-446, maio/ago. 2019. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142019000200421&lng=en&nrm=iso. Acesso em: 11 jan. 2020.

ZANELLATO, Marco Antonio. Condutas ilícitas na sociedade digital. **Revista de Direito do Consumidor**, v. 44, p. 206-261, out./dez. 2002.