UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

PROTEÇÃO DE DADOS PESSOAIS COMO FUNDAMENTO DO ESTADO DEMOCRÁTICO DE DIREITO

ARY GOMES DA MOTTA NETO

RIO DE JANEIRO

2023

PROTEÇÃO DE DADOS PESSOAIS COMO FUNDAMENTO DO ESTADO DEMOCRÁTICO DE DIREITO

Projeto de Monografia apresentado à Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Dr. Daniel Mitidieri

RIO DE JANEIRO

2023

CIP - Catalogação na Publicação

M921p

Motta Neto, Ary Gomes da
Proteção de dados pessoais como fundamento do Estado Democrático de Direito / Ary Gomes da Motta Neto. -- Rio de Janeiro, 2023.
82 f.

Orientador: Daniel Mitidieri.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2023.

1. Direito Constitucional. 2. Direito Digital. 3. Proteção de Dados Pessoais. I. Mitidieri, Daniel, orient. II. Titulo.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

PROTEÇÃO DE DADOS PESSOAIS COMO FUNDAMENTO DO ESTADO DEMOCRÁTICO DE DIREITO

Projeto de Monografia apresentado à Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Dr. Daniel Mitidieri

Data da aprovação _____/_____/_____

BANCA EXAMINADORA:

_____

Orientador

_____

Membro da Banca

_____

Membro da Banca

RIO DE JANEIRO

2023

AGRADECIMENTOS

Primeiramente, agradeço a meus pais, por serem meus amigos ao longo de desse início de trajetória acadêmico-profissional que é a graduação. Sem todo o apoio que que sempre me deram, tenho certeza de que esse percurso seria incomparavelmente mais tortuoso e, talvez nem estivesse apresentando um trabalho de conclusão de curso a esse momento. Palavras nunca serão o bastante para expressar a gratidão, o carinho e o amor que tenho por vocês. Ainda no âmbito familiar, também agradeço à minha tia Luise Motta, que praticamente coorientou essa pesquisa, pois sem sua ajuda, essa monografia não teria a clareza conceitual e, na medida do possível, a elegância e conformidade à estrutura que terminou por ter. Mesmo sendo de outra área, ela me mostrou como os limites existem de forma diferente para grandes professores e, em seu caso, imortais de suas academias. No âmbito institucional da FND-UFRJ, agradeço a meu orientador, prof. Daniel Mitidieri, por gentilmente ter aceitado assumir a orientação desse trabalho e aprová-lo para defesa. Também agradeço aos grandes professores que tive a felicidade de encontrar e que despertaram meu entusiasmo e carinho pelas ciências jurídicas: o prof. Carlos Bolonha, que no começo do curso mostrou a riqueza do que é, foi e pode ser o Estado; a prof.ª Renata Versiani, que sempre expôs de forma otimista os desafios de concretizar em ser o dever-ser e a fazer parecer simples a sistemática processual trabalhista; o prof. Emiliano Brunet, que ao lecionar sobre políticas públicas abriu a janela para um novo e vibrante paradigma deontológico do direito; o prof. Marilson Santana, que ensinou a ética e estatuto da advocacia para além das normas, lendo capítulos do livro que é a sua vida como jurista para mostrar os desafios e satisfações da advocacia; por fim, mas absolutamente longe de menos importante, aos queridos professores e irmãos, Nilo e Lorenzo Pompílio, para os quais o magistério é indissociável do companheirismo, da sinceridade e da retidão, tendo sempre feito questão de mostrar o lado humano do direito nas áreas em que atuam (direito penal e civil, respectivamente) e como todo o esforço e cansaço do estudo e da prática jurídica florescem em grandeza e enriquecimento do espírito. Cito apenas esses professores por serem alguns dos que mais me marcaram, mas deixo meus sinceros agradecimentos a muitos outros que contribuíram imensamente nessa jornada e dos quais guardo lembranças de verdadeira admiração e carinho. Por fim, agradeço à instituição FND-UFRJ por ter me propiciado um espaço rico em conhecimento e espero estar à altura da honraria do título de bacharel dessa grandiosa trigésima centenária instituição.

"O cientista inventa uma flor que parece
A razão mais segura pra ninguém saber
De outra flor que tortura, pois é, pra quê?"
(Pois é pra quê? – Sidney Miller)

"Não basta um século para fazer a pétala
Que um só minuto faz
Ou não
Mas
A vida muda
A vida muda o morto em multidão"
(Dentro da noite veloz - Ferreira Gullar)

RESUMO

Os celulares consolidaram-se como computadores de bolso e a internet passou a moldar o estilo de vida do indivíduo, assumindo papel que já fora das instituições religiosas (medievo), do monarca (modernidade) e do parlamento (contemporaneidade). As fundações jurídicas, políticas e filosóficas sob as quais se ergue o Estado Democrático de Direito sofrem grave erosão devido à falta de tutela efetiva dos dados pessoais. A presente monografia busca entender o que é a proteção de dados pessoais enquanto direito fundamental usando a metodologia proposta por Alexy em sua Teoria dos Direitos Fundamentais. Dessa forma, busca-se compreender os aspectos de um direito fundamental em três dimensões: empírica, normativa e analítica. O objetivo desse trabalho é delimitar a moldura jurídica do direito fundamental à proteção de dados pessoais, garantindo seu adequado sopesamento com outras normas no ordenamento brasileiro. Foram obtidos como resultados que esse direito é composto parcialmente pelos direitos de defesa e, de forma plena, por direitos a prestações normativas e fáticas. Concluímos assim que as competências de direito privado e os princípios da Lei Geral de Dados Pessoais (LGPD) são a essência desse direito fundamental, determinando, respectivamente, direitos subjetivos e o novo paradigma de liberdade digital.

Palavras-chave: direito constitucional; proteção de dados pessoais; direito digital; direito civil.

ABSTRACT

Cellphones estabilished themselves as portable computers and the internet started do shape the lifestyle from persons, taking the place that once was from religious institutions (medievalism), monarchy (modernity) and from parliamentarism (contemporaneity). The legal, political and philosophycal foundations upon which stands the Democratic Rule of Law suffer serious erosion due to the absence of effective data protection. The present monograph seeks to understand what is the fundamental right to personal data protection employing Alexy's methodology from his Theory of Fundamental Rights. Thus, it seeks to understand the aspects of a fundamental rights according to three dimensions: empirical, normative and analitical. The objective of this work is to line-off the legal frame of the fundamental right to data protection, assuring it's adequate weighting against other norms from the brazilian legal system. It was taken as results that this right is composed by defence rights partially and, fully, by rights to normative and factual provisions. Thus, we concluded that the competences of private right and the principles of the Personal Data Protection General Law (LGPD) are the essence of this fundamental right, defining, respectively, personal rights and a new paradigm of digital freedom.

.

Keywords: Constitutional Law; Personal Data Protection; Digital Law; Civil Law.

SUMÁRIO

INTRODUÇÃO

Em 2007 a Apple lança o primeiro smartphone e os celulares consolidam-se como computadores de bolso. Aparelhos antes analógicos são digitalizados e conectados à rede, assim como a vida do indivíduo. Sua rotina, locais que visita, trabalhos, gostos, preferências e opiniões são registrados por esses aparelhos. A internet passa a moldar o estilo de vida do indivíduo, assumindo papel que já fora das instituições religiosas (medievo), do monarca (modernidade) e do parlamento (contemporaneidade). A essência do indivíduo foi capturada pela internet e convertida em dados pessoais. Em 2013, a empresa *Cambridge Analytica* usa dados pessoais e algoritmos do *Facebook* para manipular a opinião de milhões de pessoas nos EUA e influenciar o resultado das eleições presidenciais (BERGHEL, 2018). Nesse mesmo ano, Edward Snowden, analista da Agência de Segurança Nacional (NSA, em inglês) dos EUA vaza informações demonstrando que a agência realizava espionagem em massa ao redor de todo o globo. O cidadão médio ouve, pela primeira vez a expressão "*big data*", modalidade pela qual a imensa quantidade de dados era armazenada e tratada a fim de se obter informações úteis. Nem mesmo chefes de Estado, como a então presidente Dilma Rousseff e a chanceler Angela Merkel, ficaram imunes à vigilância da NSA, assim como empresas, por exemplo a Petrobrás (BBC, 2013). Em 2018, Jamal Khashoggi, jornalista saudita crítico ao regime de seu país e radicado nos EUA em autoexílio, é brutalmente assassinado e esquartejado por um grupo de assassinos na embaixada saudita, em Istanbul, Turquia. Acredita-se que o assassinato foi ordenado pelo príncipe saudita, Mohammed bin Salman a quem Khashoggi fazia duras críticas (ANISTIA INTERNACIONAL, 2021). Em especial, dados da inteligência americana apontam que o assassinato do jornalista saudita foi planejado com base em ataques cibernéticos realizados a celulares de pessoas próximas ao jornalista. A partir dessas invasões, tiveram acesso a diversas conversas e puderem prever o dia e momento em que Khashoggi visitaria a embaixada, assassinando-o em espaço de jurisdição saudita, afinal, ele não voltaria ao país por saber do risco de vida que corria (ANISTIA INTERNACIONAL, 2021). Não só a liberdade e a própria vida dos indivíduos estavam em xeque, como também a própria soberania dos estados-nações, mas houve uma resposta.

Ainda em 2018, o Senado dos Estados Unidos investiga a manipulação das eleições pela empresa *Cambridge Analytica*, colhendo testemunho do próprio presidente do *Facebook* (rede social na qual a manipulação ocorreu de fato), Mark Zuckerberg (WASHINGTON POST, 2018). No mesmo ano entra em vigor o Regulamento Geral sobre Dados Pessoais na Europa, como resposta dos Estados democráticos a esse novo perigo, em busca de regular o mercado de dados pessoais e proteger os cidadãos. Na Europa, o ativista sueco Max Schrems apresenta processo contra o *Facebook* perante o Tribunal de Justiça da União Europeia (TJUE). Resumidamente, alega que a transferência dos dados pessoais da Europa aos EUA, onde estão os servidores da empresa, culminaria na disponibilidade de todos os dados às agências de inteligência dos EUA, como a NSA (TJUE, 2020). O resultado do julgamento é favorável à pretensão de Schrems, invalidando acordo de transferência de dados, que é reformulado em 2016 e invalidado novamente em 2020. Em breve síntese, o TJUE entende que não existem limitações legais às agências de inteligência norte-americanas em virtude da política da Guerra ao Terror e, como estas colhiam os dados diretamente do cabo submarino de internet que liga os dois continentes, não há possibilidade de controle judicial ou limitação (TJUE, 2020).

Enquanto isso, talvez a tônica dos debates sobre proteção de dados pessoais seja principalmente a privacidade no que tange à perturbação pelo marketing e a estelionatos decorrentes de vazamentos de dados pessoais. Um dos casos de maior repercussão foi o da rede de hotéis Marriott (ICO, 2020), no qual criminosos tiveram acesso ao banco de dados da rede hoteleira. Enquanto isso, Julian Assange, fundador do WikiLeaks, permanece preso por ter vazado informações que denunciavam crimes de guerra dos EUA no Iraque (ANISTIA INTERNACIONAL, 2021) e Edward Snowden permanece na Rússia, inicialmente como asilado político (THE GUARDIAN, 2013), mas desde 2022, já como cidadão russo (AP NEWS 2022). A questão da proteção de dados transcende o mero aspecto consumerista e é efetivo desafio constitucional. As fundações jurídicas, políticas e filosóficas sob as quais se erige o Estado Democrático de Direito sofrem grave erosão devido à falta de tutela efetiva dos dados pessoais. As liberdades, os direitos humanos e o próprio direito à vida são vilipendiados em um ambiente imaterial, a internet, que contém um mapa preciso do mundo real, da rotina dos indivíduos, de seus medos, seus desejos e de sua individualidade. Assim como a ordem controladora imposta pelas instituições religiosas no medievo permitia facilmente identificar dissidentes e inflamar as massas para queimá-los em fogueiras; como a propaganda nazista e a

rígida definição de um estilo de vida com base nas decisões do partido nacional-socialista permitiram aglutinar amplos setores sociais desesperados com a fome e o desemprego para incendiar casas, assassinar opositores e garantir a hegemonia de um projeto político que almejava o genocídio de minorias; a internet, por meio do uso indiscriminado dos dados pessoais, permite que grupos econômicos privados e setores políticos também dirijam as massas para provocar a cisão da sociedade e a consolidação de seu projeto político, mesmo que esse seja contrário ao Estado Democrático de Direito e ao antropocentrismo, expresso pela Declaração Universal dos Direitos Humanos. Por essas questões é imprescindível discutir como a privacidade é um fator central da sociedade e entender o que significa a proteção de dados pessoais nesse contexto, assim como de que forma ela deve ser consolidada como um dos fundamentos do Estado Democrático de Direito, isto é, como um direito fundamental.

CONSIDERAÇÕES INICIAIS (APONTAMENTOS METODOLÓGICOS)

A presente pesquisa foi estruturada conforme a Teoria Geral dos Direitos Fundamentais de Robert Alexy (ALEXY, 2015), obra publicada originalmente em 1986 e complementada em 2002. Essa teoria é composta por diversos níveis, que podem ser, resumidamente, divididos em um primeiro nível estrutural e um segundo, procedimental, o qual ramifica-se em, ao menos, mais dois subníveis.

No primeiro nível, são determinados objeto e natureza da teoria conforme três dimensões: "ela é em primeiro lugar, uma teoria dos direitos fundamentais da Constituição alemã; em segundo lugar, uma teoria jurídica; e, por fim, uma teoria geral" (ALEXY, 2015). A primeira dessas dimensões, determina que o objeto deve ser uma norma específica, que no caso de Alexy é a Constituição alemã e, na presente pesquisa, é o direito constitucional brasileiro à proteção de dados pessoais. A segunda dessas dimensões mescla objeto e natureza, mas, como o objeto já está bem definido pela primeira, se destaca que a natureza da teoria é jurídica, descartando concepções filosóficas ou sociológicas, determinando o campo científico das fontes e da pesquisa. Por fim, no âmbito de ser uma teoria geral, há uma diferenciação entre a presente pesquisa e o método de Alexy. Enquanto o autor alemão apresenta uma teoria que abrange todo o sistema constitucional alemão, caracterizando-se em sua natureza como uma teoria integradora (ALEXY, 2015) e cujo objetivo é apresentar "um sistema de enunciados gerais de direitos fundamentais, corretos ou verdadeiros, ordenados da forma mais clara possível" (ALEXY, 2015), por outro lado, a presente pesquisa é mais específica, tendo como ponto focal o direito fundamental à proteção de dados pessoais. Considerando-o, porém como parte de um sistema no qual ao mesmo tempo que influencia o todo, também é influenciado por ele. Assim, ainda pretende-se analisar o todo, porém pela perspectiva do direito fundamental à proteção de dados pessoais.

Atingindo o segundo nível (procedimental), são apresentadas três dimensões: empírica, normativa e analítica. A primeira delas, a dimensão empírica, é aquela caracterizada pela "cognição do direito positivo válido" (ALEXY, 2015), que é composta não somente pelo direito legislativo (Constituição e leis), mas também pelo que o autor denomina como "direito judicial" (jurisprudência) e pelo direito prático (a materialidade do direito). Cabe ressaltar que, devido à abertura semântica intrínseca dos direitos fundamentais, esses três aspectos têm especial relevância, pois, a mera análise semântica do texto legal é insuficiente (ALEXY, 2015). A segunda, delas, a dimensão normativa, é aquela relacionada ao silogismo entre a aplicação da norma abstrata e o caso concreto. É a dimensão natural da prática jurídica, que depende da "fundamentação racional dos juízos de valor" (ALEXY, 2015) e produz normas complementares, garantindo sua efetivação no caso concreto, sem que o resultado seja uma interpretação meramente subjetiva de uma questão axiológica aberta (ALEXY, 2015). Esse procedimento é marcado por uma crítica valorativa, que trata tanto do problema da complementação (lacunas legais), quanto do problema da fundamentação (sopesamento de direitos enraizados em valores distintos). Para fins de adequação à presente pesquisa a jurisprudência será analisada na dimensão normativa, de forma que sejam apresentadas a crítica valorativa e a fundamentação de alguns tribunais de especial relevância para o tema. Por fim, a terceira dimensão (analítica) "diz respeito à dissecção sistemático-conceitual do direito vigente" (ALEXY, 2015), que por sua vez é fragmentada em quatro espectros: conceitos elementares, construções jurídicas, estrutura do sistema jurídico e fundamentação na aplicação dos direitos fundamentais:

> "O espectro de tal dimensão estende-se desde a análise de **conceitos elementares** (por exemplo, do conceito de norma, de direito subjetivo, de liberdade e de igualdade), passando por **construções jurídicas** (por exemplo, pela relação entre o suporte fático dos direitos fundamentais e suas restrições e pelo efeito perante terceiros), até o **exame da estrutura do sistema jurídico** (por exemplo, da assim chamada irradiação dos direitos fundamentais) e da **fundamentação no âmbito dos direitos fundamentais** (por exemplo, do sopesamento)" (ALEXY, 2015, grifos nossos).

Segundo Alexy, "se a ciência jurídica quiser cumprir sua tarefa prática de forma racional, deve ela combinar essas três dimensões" (ALEXY, 2015). Destaque-se que há a determinação de uma finalidade prática e de um meio para atingi-la, a racionalidade. Assim, deve-se partir da dimensão empírica (o conhecimento do direito), progredindo para a dimensão normativa nos casos em que a etapa anterior for insuficiente e, por fim, recorrendo à dimensão analítica como

instrumento garantidor de “clareza conceitual, ausência de contradição e coerência” (ALEXY, 2015). Portanto, as três dimensões são necessárias para que seja apresentada uma teoria jurídica sobre direitos fundamentais.

Novamente, para fins de adaptação à presente pesquisa, será feita uma pequena alteração, sem grande prejuízo à estrutura da teoria: conceitos elementares e construções jurídicas serão abordadas em conjunto, assim como a estrutura do sistema jurídico e a fundamentação no âmbito dos direitos fundamentais também serão abordadas juntas. Por mera opção de estilo, é mais conveniente abordar uma ou mais construções jurídicas relativas a um conjunto de conceitos basilares antes de apresentar outros conceitos do que cindir essa relação de coesão interna em prol de uma clareza na estrutura geral. Dessa forma, buscando elaborar estudo acerca do direito fundamental à proteção de dados, este objeto será analisado pela perspectiva das dimensões empírica, normativa e analítica propostas por Alexy.

DIMENSÃO EMPÍRICA

A constitucionalização do direito à proteção de dados pessoais

A Constituição da República Federativa do Brasil prevê grau especial de proteção aos direitos individuais, previstos principalmente em seu art. 5º, como uma de suas cláusulas pétreas. Segundo o eminente ministro do Supremo Tribunal Federal, Luis Roberto Barroso, "a proteção especial dada às normas amparadas por cláusulas pétreas sobreleva seu *status* político ou sua carga valorativa, com importantes repercussões hermenêuticas" (BARROSO, 2010) e, nesse contexto, insere-se a proteção aos dados pessoais, que está prevista no inciso XXIX do referido art. 5º. Barroso também explicita que o status de cláusula pétrea não implica em uma hierarquia normativa interna da Constituição, devendo ser interpretado estritamente como vedações ao legislador ordinário e ao poder constituinte derivado, tendo todas as normas constitucionais igual hierarquia (BARROSO, 2010).

Além de consubstanciar-se em cláusula pétrea, o direito a proteção de dados pessoais existe como um direito fundamental autônomo, tendo sido inserido no rol do art. 5º por meio da Emenda Constitucional nº 115 de 10 de fevereiro de 2022. O processo teve início no Senado Federal, com a apresentação de PEC pelo Senador Eduardo Gomes, subscrita por mais 29 senadores às mesas do Senado Federal e da Câmara de Deputados Federal em 12 de março de 2019. A justificação no projeto apresentado pelos senadores aborda assuntos importantes, sendo destacada a necessidade de constitucionalização do direito à proteção de dados por duas razões: (1) a necessidade fática de maior proteção no mundo cibernético, ambiente em acelerado desenvolvimento e que, em âmbito constitucional, ainda era uma lacuna (apesar de já existir legislação ordinária sobre o assunto); (2) a necessidade política de centralização da competência legislativa, a fim de garantir uma legislação nacional uniforme. Quanto ao segundo aspecto, destaca-se o receio advindo do trâmite de projetos de lei em nível estadual e municipal que replicavam a LGPD, havendo, no entanto, a possibilidade de alterações (até de conceitos essenciais, como a definição de dado pessoal) que poderiam levar a uma indesejada

pulverização da regulamentação do tema (BRASIL, 2019a). Assim, surgiu a PEC de apenas três artigos, um incluindo a proteção de dados pessoais como inciso XXII-A do art. 5º da CRFB, outro incluindo-a como competência legislativa privativa da União, na forma de inciso XXX ao art. 22 da CRFB e, um último artigo, prevendo a vigência da PEC a partir da publicação. A relatoria da PEC na Comissão de Constituição e Justiça coube à então senadora Simone Tebet, que, em seu relatório, afirma já existir tutela da proteção de dados em âmbito constitucional, por meio da conjugação dos artigos dos artigos 1º, III; 3º, I e IV, 5º, X, XII e LXXII. Também realiza breve análise de direito comparado, observa legislações europeias, norte-americanas e sul-americanas, concluindo em favor da PEC e indicando a ausência de impedimentos constitucionais a ela (BRASIL, 2019b). Em reunião da CCJ, o senador Rodrigo Pacheco propõe alteração textual que é convertida e aprovada como emenda nº 1-CCJ (de redação) à PEC, que substituía a criação do inciso XXII-A por uma nova redação do inciso XXII, incluindo-se, ao final, o texto integral do então proposto inciso XXII-A (BRASIL, 2019c).

Enviada à Câmara Federal, o projeto foi aprovado sem óbices pela CCJ e enviado ao plenário, sendo criada comissão especial para a PEC. A relatoria coube ao deputado federal Orlando Silva, que relata a realização de seis audiências públicas na Câmara, marcadas por ilustres presenças, das quais, cabem alguns recortes do relatório para ilustrar as discussões. A respeito da autonomia do direito à proteção de dados pessoais, a professora de direito, pesquisadora e especialista legal em proteção de dados, Laura Schertel, argumenta a favor de um direito autônomo, visto que, diferente do sigilo de comunicações, a proteção de dados é um direito coletivo e implica em mais do que mero não agir do Estado. Essa posição praticamente não tem discordâncias, porém, algumas vozes como a de Christina Aires, advogada especialista da Confederação Nacional da Indústria, discordam, porém não quanto à criação de um direito autônomo ou complementação de outro já existente, mas quanto à própria inclusão da proteção de dados dentro do catálogo de diretos fundamentais. Com relação à questão da competência legislativa, há ampla maioria de manifestações em favor da competência privativa da União (15 manifestações favoráveis, 4 contrárias e 3 que não abordaram o tema), como a do professor Danilo Doneda, ao afirmar que a fragmentação fragilizaria a proteção em razão do trânsito dos dados ou de seu titular (fatores elementares e inevitáveis da situação) e de Gileno Barreto, Diretor Jurídico de Governança e Gestão do SERPRO, que argumenta pelo aspecto

mercadológico, exemplificando que, na Europa, a possibilidade de complementação do GDPR trouxe impactos econômicos negativos aos países que exerceram essa faculdade.

O relator, deputado federal Orlando Silva, apresenta voto aprofundado: aborda a conceituação da proteção de dados pessoais como direito fundamental; sua diferenciação de outros direitos fundamentais já existentes (conceituação como direito autônomo); justifica a competência legislativa privativa da União; e apresenta alterações ao texto da PEC nº 17 de 2019. Inicialmente, afirma que a temática tem grande relevância econômica, considerando-se a existente economia de dados e a configuração da civilização em "sociedade da informação". Afirma que o poder constituinte originário brasileiro já considerava o direito à vida privada e à intimidade como direitos fundamentais, assim como o direito ao sigilo de comunicações, sendo os três, expressões da liberdade de expressão e de pensamento. Por essa razão, caracterizam-se como liberdades individuais (BRASIL, 2019d). Prossegue:

> "O direito à proteção de dados pessoais reúne as características principais dos direitos fundamentais. É um direito universal, aplicável a toda e qualquer pessoa e é um direito inalienável ou indisponível, o que impede o titular aliená-lo ou tornar impossível o seu exercício. O direito à proteção de dados também deve ser entendido como um direito essencial à formação da personalidade. Portanto, essencial à dignidade da pessoa e dela indissociável. **Por fim, o direito à proteção de dados pessoais possui caráter fundamental porque vincula as ações e atividades do Poder Público e do setor privado, tornando-os parâmetros de organização administrativa e de limitação dos Poderes Públicos, assim como das empresas com relação à forma de viver dos cidadãos**. Dessa forma, a fundamentalização do direito à proteção de dados é não apenas possível, como indispensável para a autodeterminação informativa limitando as possibilidades e as formas de ação do indivíduo nos tempos atuais" (BRASIL, 2019d).

Também acolhe a argumentação da professora Laura Schertel, afirmando que o direito à proteção de dados pessoais difere do direito ao sigilo de comunicação por ser um direito coletivo e um direito positivo, enquanto o outro é um direito individual e negativo. Para além dessas diferenças, ressalta que a finalidade do direito à proteção de dados é a igualdade, isto é, a não-discriminação, enquanto o sigilo das comunicações tem como objetivo o "uso tranquilo da propriedade" (BRASIL, 2019d). Com base nesses argumentos, propõe que o direito à proteção de dados pessoais seja inserido no rol do artigo 5º como um direito autônomo, com

inciso próprio e sem vinculação a qualquer outro, isto é, como o inciso XXIX (ao invés de ser mera nova redação do inciso XII ou de ser numerado como inciso XII-A, propostas suscitadas no Senado Federal). Com relação à competência legislativa privativa da União, afirma que, a adoção de uma postura diversa culminaria em um "risco sistêmico à segurança jurídica, aos investidores, ao fluxo e ao tratamento de dados em geral, com consequências deletérias para todos os agentes envolvidos e cidadãos" (BRASIL, 2019d). Também entende no mesmo sentido quanto ao mercado e à fiscalização:

> "Na União Europeia, por exemplo, um dos objetivos expressos do Regulamento 2016/679 é justamente promover a harmonização e evitar que diferenças nos níveis de direitos à proteção de dados possam representar obstáculos ao livre fluxo de dados, distorcer a competição ou dificultar a atuação da autoridade responsável pela fiscalização das atividades de tratamento de dados" (BRASIL, 2019d).

Ressalta que a LGPD possuí eficácia expressa em todos os entes da federação e que outorga à ANPD o poder central de interpretação da legislação de proteção de dados e de produção de normas infralegais que visem a conformar (ou efetivar) a LGPD. Dessa forma, fundamenta a pertinência de que seja positivada a competência legislativa privativa da União para garantir validade, eficácia e coesão sistemática quanto ao papel central dessa autarquia federal. Anteriormente, em audiência pública, foi questionado se tal decisão não prejudicaria áreas sensíveis, que requerem regulação com observância das peculiaridades regionais ou locais, em especial no âmbito do Direito do Consumidor. Quanto a esses questionamentos, assevera que a competência privativa da União sobre a proteção de dados pessoais tem incidência distinta da consumerista e de outras competências concorrentes, sem que uma anule a outra. Nesse sentido, cita o caso da competência privativa sobre legislação de telecomunicações, que não interfere na regulação e tutela consumerista desse âmbito. Por fim, entende que a própria ANPD também terá de articular-se com outras autoridades reguladoras públicas para fiscalizar eficientemente setores específicos (conforme postula a própria LGPD). Por essas razões, afirma que não prospera o temor de sufocamento do pacto federativo ou da própria democracia. Por fim, acrescenta mais um artigo, prevendo a competência de exercício da regulação e fiscalização da "competência material para organizar e fiscalizar a proteção e o tratamento de dados pessoais" (BRASIL, 2019d), por meio de uma agência reguladora (autarquia). Essa última alteração tem em vista garantir a legitimidade da ANPD, mas é

inespecífica para que possa abarcar uma eventual mudança futura na autarquia ou em seu nome e, de forma geral, concluí o microssistema constitucional de proteção de dados pessoais sem que a ANPD seja desconsiderada.. Em síntese, o substitutivo do relator à PEC nº 17 de 2019 do Senado acresce os incisos XXIX, XXVI e XXX, respectivamente, aos arts. 5º, 21 e 22, que, nessa ordem, listam (1) os direitos fundamentais individuais, (2) as competências materiais da União e (3) as competências legislativas privativas da União, incluindo a proteção de dados pessoais nesses três catálogos da Constituição Federal. Aprovado na Câmara Federal, o projeto volta a tramitar no Senado, sendo aprovado sem novas alterações e, por fim, sendo convertido na Emenda Constitucional 115 pelas mesas da Câmara Federal e do Senado, em sessão conjunta do Congresso Nacional, na data de 17 de fevereiro de 2022.

A Lei Geral de Proteção de Dados Pessoais

Princípios

Em caráter anterior ao da Emenda Constitucional 115, já existia previsão legal ordinária acerca da proteção de dados pessoais. Trata-se da Lei 13.709, também denominada Lei Geral de Proteção Dados Pessoais, promulgada em 14 de agosto de 2018. Inicialmente, observa-se que a LGPD conta com quatro tipos de princípios: (1) aqueles gerais, que incidem sobre todo o diploma legal; (2) aqueles relativos à atividade de tratamento de dados; (3) aqueles relacionados à titularidade de dados; e (4) aqueles quanto à atuação da ANPD.

O primeiro conjunto (princípios gerais), expresso principalmente pelo art. 2º (fundamentos da lei) inclui, expressamente, o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação de comunicação e de opinião; o desenvolvimento econômico e tecnológico e a inovação; a livre-iniciativa; a livre concorrência e a defesa do consumidor; os direitos humanos e o exercício da cidadania pelas pessoas naturais (LGPD, art. 2º, I-VII). O art. 1º, paralelamente, afirma que os objetivos da lei são a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural (LGPD, art. 1º). Cabe ressaltar que enquanto objetivos são normas programáticas, fundamentos são normas principiológicas.

Segundo aspecto são os princípios relacionados à atividade de tratamento de dados que incluem, especificamente: a boa-fé, a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não-discriminação e a responsabilização e prestação de contas (LGPD, art. 6º, *caput* e incisos I a X). Abordando de forma específica esses princípios, primeiramente, os princípios da finalidade, adequação e

necessidade “são umbilicalmente conexos, formando, juntamente com a transparência, o cerne dessa norma jurídica” (MALDONADO; BLUM, 2020). A finalidade é a fundamentação da coleta de dados pessoais conforme uma das hipóteses legais de tratamento. Já a adequação reflete a compatibilização do uso que é feito dos dados pessoais com a finalidade que justifica sua coleta. Por exemplo, dados coletados para o acompanhamento da saúde não podem ser usados, sem consentimento específico, para formar perfis de consumo farmacêutico (MALDONADO; BLUM, 2020). A necessidade, também conhecida como princípio da minimização de dados, prevê que a coleta de dados pessoais deve ser restrita ao mínimo necessário para o adequado tratamento de dados conforme a finalidade aplicada. Além disso, a necessidade também abrange a ponderação entre potenciais riscos e benefícios aos direitos dos titulares em razão do tratamento de dados, razão pela qual um risco muito acentuado pode reduzir ou até mesmo vedar o tratamento de dados (MALDONADO; BLUM, 2020). O princípio do livre acesso versa sobre direito potestativo do titular de dados pessoais de requerer, sem custos, informações claras sobre: seus dados pessoais armazenados, sua integridade, tratamento, finalidade e compartilhamento (MALDONADO; BLUM, 2020). O princípio da qualidade dos dados prevê que os agentes de tratamento têm a obrigação de zelar pela precisão dos dados armazenados e, da mesma forma, de coletar e armazenar apenas dados pertinentes à finalidade aplicada. Destaca-se também que o titular possui presunção de vulnerabilidade técnica e informacional, razões pelas quais as informações devem ser prestadas de forma acessível (MALDONADO; BLUM, 2020). Em sequência, o princípio da segurança dispõe sobre outro dever dos agentes de tratamento: empregar medidas aptas a prevenir acidentes ou incidentes com dados pessoais, nominalmente, a destruição, perda, alteração e comunicação ou difusão, em todos os casos, ilícitas (LGPD, art. 6º, VII). Complementarmente, o princípio da prevenção postula que devem ser adotadas medidas de segurança visando à prevenção da ocorrência de ilícitos com dados pessoais (LGPD, art. 6º, VIII), criando responsabilidade não somente pelo dano, como também pela negligência quanto à regular adoção de medidas de segurança. O princípio da não-discriminação, por sua vez, impõe que é defeso adotar finalidade voltada à discriminação ilícita ou abusiva (LGPD, art. 6º, IX). Ressalta-se de toda forma, que nem toda “discriminação” é ilícita, como é comumente realizada pela criação de perfis de consumidor e de marketing direcionado. Por essa razão a “discriminação” é caracterizada como “ilícita ou abusiva” para os fins do art. 6º, IX da LGPD. Por fim, o princípio da responsabilização e prestação de contas (LGPD, art. 6º, X), trata da responsabilidade dos agentes de tratamento em manter a conformidade do tratamento com a Lei, com as determinações da ANPD e com a legítima expectativa (MALDONADO; BLUM, 2020).

Terceiro aspecto são os princípios relacionados à titularidade dos dados pessoais, que é vinculada aos "direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei" (LGPD, art. 17). *A priori*, se observa que os conceitos possuem dupla fundamentação: constitucional, por força da expressão "direitos fundamentais", e como ei ordinária (a própria LGPD). Quarto aspecto é o de princípios relacionados à atividade da ANPD, que ao criar normas deve conjugar os princípios do tratamento e os direitos dos titulares com a mínima intervenção, nos termos do art. 170 da Constituição Federal (LGPD, art. 55-J, §1º), isto é, "a ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social" (CRFB, art. 170).

Objeto

O art. 5º, I define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (LGPD, art. 5º, I). Portanto, a LGPD adota um conceito expansionista, segundo o qual a informação que tem potencial de identificar uma pessoa natural também é um dado pessoal (MALDONADO; BLUM, 2020) e inclui, expressamente, a formação de perfis comportamentais (LGPD, art. 12, §2º). Já o dado anonimizado (LGPD, art. 5º, III), que não é protegido pela LGPD (LGPD, art. 12, *caput*), é aquele absolutamente incapaz de identificar o sujeito ao qual se refere. Incapacidade caracterizada pela abstenção do controlador em reverter o processo (LGPD, art. 12, *caput*) ou pela impossibilidade de reversão por meios razoáveis, considerando fatores objetivos, como tecnologias disponíveis, custo e tempo (LGPD, art. 12, *caput* e §1º). Visando maior segurança jurídica, cabe à ANPD dispor sobre padrões e técnicas de anonimização, assim como verificar a segurança deles (LGPD, art. 12, §3º). Complementarmente, a pseudoanonimização é procedimento intermediário, como a criptografia de um banco de dados e armazenamento, em separado da "chave" de descriptografia (LGPD, art. 13, §4º). Note-se que a pseudoanonimização tem objetivo de segurança ao invés de desvincular dado e titular. A LGPD cria regramento especial, e mais

rígido, quanto aos dados pessoais sensíveis, definidos como aqueles que “possam trazer algum tipo de discriminação” (MALDONADO; BLUM, 2020), sendo determinados pela lei como aqueles 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” (LGPD, art. 5º, II).

O acúmulo de dados pessoais forma um banco de dados (LGPD, art. 5º, IV). Destaca-se, a princípio, que banco de dados e base de dados não se confundem. Bancos de dados se referem a qualquer conjunto de dados pessoais e são objetos da LGPD, já a base de dados recebe tutela pelo direito autoral, conforme o art. 7º, XIII da Lei 9.610/98 e faz referência ao resultado da atividade intelectual (via desenvolvimento de software, por exemplo) voltada à organização de conjunto de dados para atender a determinado objetivo (MALDONADO; BLUM, 2020; LIMA, 2004). O que interessa à presente pesquisa é o mesmo que à LGPD: os bancos de dados. Para que os dados pessoais tenham valor, eles são “tratados”, isto é, submetidos a operações que transformem informações fragmentadas em um conjunto agregado e útil à finalidade almejada. A LGPD elenca essas operações expressamente como a “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração” (LGPD, art. 5º, X). Tratamento de dados pessoais que recebe abordagem especial é a anonimização, processo que transforma um dado pessoal em um dado anonimizado, conforme abordado anteriormente. Também existe previsão legal de “tratamento irregular de dados pessoais”, que é aquele realizado em desconformidade com a legislação ou aquém dos padrões de segurança esperados pelo titular (LGPD, art. 44, *caput*). Com o propósito de caracterizar essa situação, são indicadas três circunstâncias relevantes: o modo do tratamento (LGPD, art. 44, I), resultado e riscos esperados (LGPD, art. 44, II) e as técnicas de tratamento disponíveis à época da infração (LGPD, art. 44, III).

O tratamento de dados pessoais é permitido em apenas dez hipóteses, as bases legais de tratamento, que têm grande relevância para a temática e estão expressas em rol taxativo dos incisos I a X do art. 7º da LGPD. A primeira hipótese, é o tratamento mediante o consentimento do titular (LGPD, art. 7º, I), devendo o controlador oportunizar ao titular meio gratuito e facilitado para revogar o consentimento, produzindo efeitos *ex tunc* até que sejam definitivamente eliminados (LGPD, art. 8º, §5º). Tal consentimento tem definição expressa na LGPD, reputando requisitos que, caso não seguidos, culminam em vício insanável da base legal e consequente vedação ao tratamento de dados (LGPD, art. 8º, §3º). O art. 5º, XII define-o como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (LGPD, art. 5º, XII). Notadamente, é uma definição rica em elementos. Inicialmente, é uma manifestação inequívoca, o que implica que o consentimento deve ser explícito, fator que diferencia a base legal "consentimento" de "legítimo interesse", por exemplo. Essa manifestação também não precisa, necessariamente, ser textual (LGPD, art. 8º), podendo ser o simples clique em uma opção de "concordo". Ainda nessa seara, a cláusula de consentimento deve estar destacada das demais (LGPD, art. 8º, §1º), seja por meios textuais ou gráficos (MALDONADO; BLUM, 2020). Em sequência, essa manifestação deve ser livre, ficando, portanto, vedado que um contrato estipule tratamento de dados com finalidade diversa da obrigação principal e não seja possível ao contratante recusar esse tratamento adicional (MALDONADO; BLUM, 2020). A manifestação também deve ser informada, de forma que "o consentimento deve ser apresentado ao titular de uma forma que o distinga visivelmente de outros assuntos, de modo inteligível, de fácil acesso e em uma linguagem clara e simples" (MALDONADO; BLUM, 2020), característica vinculada diretamente à presunção de vulnerabilidade técnico-informacional do titular. Por fim, existe previsão legal processual, incumbindo ao controlador o *onus probandi* de obtenção do consentimento conforme todos os requisitos legais, devendo manter registro comprobatório de todas as operações.

Prosseguindo às demais hipóteses, a segunda delas é o "cumprimento de obrigação legal ou regulatória pelo controlador" (LGPD, art. 7º, II), podendo se acrescentar justificativas ligadas ao direito internacional e a boas práticas, contanto que exista prévio estudo dos riscos e elaboração de relatório de impacto a respeito (MALDONADO; BLUM, 2020). Terceira base legal aplica-se apenas quando o controlador compuser a administração pública, caso no qual o

tratamento e uso compartilhado de dados pessoais pode ser realizado sem consentimento quando o objetivo for a "execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres" (LGPD, art. 7º, III). A quarta base legal também tem restrição quanto ao controlador dos dados, aplicando-se apenas a órgão de pesquisa, tendo como finalidade a realização de estudos e, ainda assim, priorizando a anonimização dos dados pessoais tratados (LGPD, art. 7º, IV). A quinta base é o tratamento de dados para cumprimento de obrigação contratual em que titular e controlador sejam partes, assim como em âmbito pré-contratual, hipótese a qual é necessária provocação do titular (LGPD, art. 7º, V). Como exemplo da hipótese pré-contratual, Lima exemplifica com o pedido de crédito a instituição financeira, que implicará em levantamento de dados financeiros do requerente em caráter antecedente à celebração do contrato (MALDONADO; BLUM, 2020). Sexta base legal é o tratamento "para o exercício regular de direitos em processo judicial, administrativo ou arbitral" (LGPD, art. 7º, VI). Sétima base legal de tratamento de dados é a "proteção da vida ou da incolumidade física do titular ou de terceiro" (LGPD, art. 7º, VII). Lima aponta que é uma hipótese muito restrita e cita o tratamento de dados de geolocalização para localização de vítimas de sequestro e sobreviventes sob escombros como exemplos (MALDONADO; BLUM, 2020). Oitava hipótese é "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (LGPD, art. 7º, VIII). Portanto, profissionais da área da saúde, serviços de saúde e entidades membros do Sistema Nacional de Vigilância Sanitária (SNVS) podem realizar o tratamento de dados pessoais sem consentimento, contudo, limitados estritamente à finalidade de tutela da saúde (MALDONADO; BLUM, 2020). Nona hipótese é o tratamento "necessário para atender aos legítimos interesses do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (LGPD, art. 7º, IX). O legítimo interesse do controlador é conceito aberto, que conta com rol exemplificativo no art. 10º da LGPD. A primeira hipótese é de "apoio e promoção de atividades do controlador" (LGPD, art. 10, I), considerando-se principalmente o marketing direto, destinado a clientes atuais, inclusive com tratamento individualizado pela gestão de preferências (MALDONADO; BLUM, 2020). A segunda hipótese exemplificativa é o tratamento com fim de proteger o titular ou de prestar serviços que o beneficiem, caso, por exemplo, do tratamento de dados para prevenção à fraude (MALDONADO; BLUM, 2020). Todavia, existem critérios e obrigações concretas para a aplicação dessa base legal. Conforme o *caput* do art. 10º, é necessário que existam finalidades legítimas (propósitos legítimos, específicos, explícitos e informados ao titular) e da existência de uma situação concreta, isto é,

de um vínculo real entre controlador e titular (MALDONADO; BLUM, 2020). Os dados tratados com essa finalidade também devem seguir o princípio da necessidade, sendo reduzidos aos estritamente necessário (LGPD, art. 10º, §1º), e da transparência (LGPD, art. 10º, §2º). Também é facultado à autoridade de dados solicitar a qualquer momento relatório de impacto quanto aos dados pessoais tratados conforme esta base legal (LGPD, art. 10º, §3º). Décima e última base legal é a proteção do crédito, considerando-se também a legislação específica (LGPD, art. 7º, X). Por fim, há previsão para o tratamento de dados pessoais públicos, isto é, dados publicamente acessíveis, estabelecendo-se que, nesses casos, vigoram os princípios da boa-fé e da finalidade, conforme o interesse público que fundamenta a disponibilização dos dados (LGPD, art. 7º, §3º). Também podem ser livremente tratados aqueles dados pessoais publicizados pelo próprio titular, cabendo o exercício dos direitos do titular e demais disposições da lei (LGPD, art. 7º, §4º).

Existe regulação especial para os dados pessoais sensíveis (LGPD, art. 11, *caput*) e para o tratamento de dados pessoais gerais que possam revelar dados pessoais sensíveis (LGPD, art. 11º, §1º). Destaca-se que o consentimento para tratamento de dados pessoais sensíveis e a finalidade desse tratamento devem ser especialmente explícitos, determinados, claros, compreensíveis e acessíveis ao titular dos dados pessoais (MALDONADO; BLUM, 2020). Por outro lado, é possível o tratamento de dados sensíveis sem consentimento do titular, contanto que indispensável ao atendimento de uma das finalidades previstas nas alíneas “a” a “g” do art. 11, II da LGPD. Ademais, é imposta a obrigação de publicizar a dispensa ao consentimento para tratamento de dados pessoais sensíveis nas hipóteses das alíneas “a” e “b” (respectivamente, cumprimento de obrigação regulatória e execução de política pública), conforme o art. 11º, §2º da LGPD. Caso seja realizado tratamento de dados pessoais para estudos de saúde (dados sensíveis), o órgão de pesquisa poderá ter acesso aos bancos de dados pessoais, contudo, deverá seguir critérios especiais de segurança, previstos no art. 13 da LGPD.

Outro relevante objeto das políticas regulatórias da LGPD é a transferência internacional de dados (definido pelo art. 5º, XV da LGPD), que pode ter como objetivo o tratamento ou o

mero armazenamento de dados pessoais no estrangeiro. Tem especial relevância pela "vibrante economia baseada em dados, sem fronteiras físicas, que necessitam de trânsito desburocrático para que não se criem entraves desnecessários em situações comuns existentes na vida de qualquer indivíduo" (MALDONADO; BLUM, 2020). São indicadas nove condições alternativas para a transferência internacional de dados (incisos I a IX do art. 33 da LGPD) que, resumidamente, englobam a manutenção do grau de proteção da LGPD, a cooperação jurídica internacional, a proteção à vida e à incolumidade física, execução de política pública (com obrigação de publicidade), cumprimento de obrigação legal ou regulatória do controlador, autorização da ANPD, exercício de direitos em âmbito judicial, arbitral ou administrativo e consentimento específico, informado e destacado do titular para execução de contrato ou pré-contrato.

Igualmente regulado é o término do tratamento de dados (LGPD, art. 15), estabelecendo quatro termos resolutivos para vedar que a atividade seja perpétua. Primeiro deles é o esgotamento da utilidade dos dados quanto à finalidade do tratamento, por alcançar-se a finalidade ou pela perda de pertinência dos dados para tal (LGPD, art. 15, I). Segundo é o fim do período de tratamento preestabelecido (LGPD, art. 15, II). Terceiro é o pedido do titular, inclusive por revogação do consentimento (LGPD, art. 15, III) e quarto é por determinação da ANPD como penalidade, por violação à LGPD (LGPD, art. 15, IV). Concluído o tratamento, proceder-se-á obrigatoriamente à eliminação dos dados pessoais, conforme as possibilidades técnicas (LGPD, art. 16). Contudo, ainda após o término do tratamento de dados é permitido que eles sejam armazenados para cumprimento de obrigação legal ou regulatória do controlador (LGPD, art. 16, I); para estudos por órgãos de pesquisa, preferencialmente anonimizados (LGPD, art. 16, II); para transferência a terceiros, respeitada a LGPD (LGPD, art. 16, III) e; para uso exclusivo do controlador, devendo ser anonimizados (LGPD, art. 16, IV).

Concluindo a análise do objeto da LGPD, o art. 4º determina hipóteses de não incidência da LGPD, subdivididas em quatro grupos, conforme os incisos I, II e III. O primeiro deles, versa unicamente sobre o tratamento de dados por pessoa natural para fins exclusivamente

particulares e sem fim econômico (inciso I), contemplando, por exemplo, o compartilhamento da própria geolocalização com amigos ou armazenamento de lista de endereços de amigos (MALDONADO; BLUM, 2020). O segundo grupo (inciso II) abrange fins exclusivamente jornalísticos e artísticos (alínea “a”) e fins acadêmicos (alínea “b”). Tendo o primeiro caso como fundamento a liberdade de expressão e o segundo o desenvolvimento econômico, tecnológico e a inovação (MALDONADO; BLUM, 2020). O terceiro grupo (inciso III) agrega hipóteses de ordem de segurança interna, externa, integridade político-administrativa e processual penal (incisos “a”, “b”, “c” e “d”). Por fim, o quarto grupo (inciso IV) contempla a hipótese em que é realizado apenas tratamento de dados no Brasil exclusivamente de titulares de um único país estrangeiro com nível de proteção de dados similar ao brasileiro por controlador desse mesmo país. Lembrando que a LGPD também não incide sobre os dados anonimizados, conquanto que não sejam ou não possam ser revertidos em dados pessoais, conforme o art. 12 da LGPD.

Sujeitos

O titular dos dados pessoais é a pessoa natural à qual os dados se referem (LGPD, art. 5º, V), vinculando o conceito de titular de dados com o conceito de personalidade civil (MALDONADO; BLUM, 2020). Dessa forma, é vedada a titularidade de dados pessoais por pessoas jurídicas, sejam elas públicas ou privadas (MALDONADO; BLUM, 2020).

Os direitos expressos do titular estão previstos nos arts. 18 a 22 da LGPD, que podem ser “exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento” (LGPD, art. 18, §3º), sem custos e conforme prazos de regulamento específico (LGPD, art. 18, §5º). Por outro lado, a resposta por parte do controlador é obrigatória, ainda que para informar não ser controlador dos dados pessoais em questão (LGPD, art. 18, §4º, I) ou informar tanto a impossibilidade material de atender a demanda quanto a inexistência de obrigação legal para tal (LGPD, art. 18, §4º, II).

Os direitos do titular materializam-se como: confirmação da existência do tratamento (LGPD, art. 18, I); acesso aos dados (LGPD, art. 18, II); correção dos dados, visando manter sua qualidade (LGPD, art. 18, III c/c art. 6º, V); "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade" (LGPD, art. 18, IV); portabilidade dos dados a outro controlador, conforme regulamentação da ANPD (LGPD, art. 18, V), salvo quanto a dados anonimizados (LGPD, art. 18, §7º); eliminação de dados tratados sob a base legal do consentimento (LGPD, art. 18, VI); informações quanto aos controladores com os quais os dados foram compartilhados (LGPD, art. 18, VII); requisitar informações sobre o não fornecimento de consentimento e impactos negativos (LGPD, art. 18, VIII); revogação do consentimento (LGPD, art. 18, IX); "peticionar em relação a seus dados contra o controlador perante a autoridade nacional" (LGPD, art. 18, §1º) e perante órgãos de defesa do consumidor (LGPD, art. 18, §8º); oposição ao tratamento de dados sem consentimento e sem conformidade com as relativas hipóteses legais (LGPD, art. 18, §2º); uniformização dos efeitos de requerimento perante um controlador quanto aos demais com os quais este tenha compartilhado os dados, por ação do controlador que recebeu a requisição (LGPD, art. 18, §6º); revisão de decisões automatizadas com impactos sobre seus interesses (LGPD, art. 20, *caput*); esclarecimento de critérios e procedimentos da decisão automatizada (LGPD, art. 20, §1º) ou de realização de auditoria pela ANPD quando houver recusa sob justificativa de segredo comercial e industrial (LGPD, art. 20, §2º); vedação ao tratamento de dados pessoais referentes ao exercício regular de direitos como titular de dados (LGPD, art. 21); judicialização individual ou coletiva visando à defesa de direitos da titularidade de dados pessoais (LGPD, art. 22).

No polo oposto ao do titular, estão os agentes de tratamento: operador e controlador de dados pessoais (art. 5º, IX da LGPD). Controlador é pessoa física ou jurídica que possuí interesse (econômico, jurídico, político etc.) no resultado do tratamento de dados pessoais, ainda que para alienação. Operador é a pessoa física ou jurídica diversa do controlador e que presta um serviço a ele (o tratamento de dados), sem interesse nos dados pessoais em si. A diferenciação pode ser complexa, especialmente porque o controlador pode permitir menor ou maior discricionariedade ao operador para realizar o tratamento, contudo, um dos fatores mais marcantes para a diferença é quem toma a decisão inicial de realizar o tratamento de dados

pessoais, assim como quem define quais dados serão tratados, estes são poderes que marcam a figura do controlador (MALDONADO; BLUM, 2020). A previsão desses dois sujeitos está nos incisos VI e VII do art. 5º da LGPD. Ademais, apesar de atuar sob as ordens do controlador, também cabe ao operador, ao seguir essas instruções, observar as normas atinentes à atividade de tratamento (LGPD, art. 39). Por fim, o operador responde solidariamente ao controlador sempre que causar danos ao titular em virtude do descumprimento de ordens do controlador (LGPD, art. 42, §1º, I).

No mesmo âmbito, também há a determinação da figura do encarregado. É obrigatório que os controladores de dados indiquem um encarregado, sendo facultativo aos operadores. O encarregado tem papel centralizador com relação a todo o ciclo de tratamento dos dados. É o encarregado a quem os titulares podem se dirigir para requerer informações ou providências, cabendo a ele cumpri-las (LGPD, art. 41, §2º, I). Também é o encarregado o legitimado para receber solicitações de informações e providências pela ANPD (LGPD, art. 41, §2º, II) e que deve zelar para que o tratamento de dados seja realizado em conformidade com as normas aplicáveis (LGPD, art. 41, §2º, III e IV).

A existência de direitos dos titulares de dados pressupõe a existência de deveres dos agentes de tratamento, como o dever de manter registro de todas as operações de tratamento, em especial, daquelas fundamentadas em legítimo interesse (LGPD, art. 37, caput). Da mesma forma, o dever de apresentar, sempre que solicitado pela ANPD, relatório de impacto à proteção de dados pessoais em virtude de suas próprias operações de tratamento, inclusive de dados sensíveis, descrevendo ao menos os tipos de dados coletados, metodologia de coleta e de segurança e análise quanto às medidas, salvaguardas e mecanismos de mitigação de risco adotados (LGPD, art. 38, caput e parágrafo único). Outrossim, é estipulado que os agentes de tratamento têm o dever de adotar medidas de segurança em âmbito técnico e administrativo (LGPD, art. 46, caput), desde a concepção do produto ou serviço (LGPD, art. 46, §2º) até depois do término do tratamento (LGPD, art. 47), sendo reservada competência à ANPD para definir padrões técnicos mínimos. Ocorrido eventual incidente de segurança, o controlador também

tem a obrigação de informar o ocorrido, em prazo razoável, à ANPD e aos titulares dos dados afetados quando existir risco ou dano relevante (LGPD, art. 48, caput). A referida notificação, por sua vez, tem alguns requisitos de conteúdo (LGPD, art. 48, §1º e seus incisos): descrição dos dados afetados (inciso I); informações sobre os titulares envolvidos (inciso II); medidas técnicas e de segurança utilizadas (inciso III); riscos do incidente (inciso IV); eventuais motivos para demora da notificação (inciso V) e; medidas adotadas ou previstas para reverter ou mitigar o dano (inciso VI).

Em acréscimo a estes dois atores, também há a ANPD, autarquia de natureza especial, com autonomia técnica, decisória e patrimônio próprio (LGPD, art. 55-A), também denominada como "agência reguladora". De forma mais ampla, a ANPD, em sua totalidade, possui amplo rol de competências, exercendo poder de polícia no âmbito da LGPD, centralizando procedimentos administrativos para apuração de irregularidades e definindo padrões mínimos para procedimentos de tratamento de dados pessoais visando a garantia da conformidade com a lei (LGPD, art. 55 e seguintes). Além de competências quanto à elaboração de normas, políticas públicas, cooperação interna e externa, dentre outras competências (LGPD, art. 55-J, I a XXIV).

Informada quanto a eventual incidente de vazamento de dados, a ANPD, inicialmente, tem o dever de mensurar a gravidade do incidente (LGPD, art. 48, §2º), considerando medidas comprovadamente adotadas para tornar os dados afetados ininteligíveis a terceiros, conforme tecnicamente possível (LGPD, art. 48, §3º). Também cabe à agência, quando julgar necessário para tutelar os dados pessoais dos titulares, "determinar ao controlador a adoção de previdências" (LGPD, art. 48, §2º). Em rol exemplificativo, são listadas duas medidas: "ampla divulgação do fato em meios de comunicação" (LGPD, art. 48, §2º, I) e "medidas para reverter ou mitigar os efeitos do incidente" (LGPD, art. 48, §2º, II).

Também se explicitam algumas regras processuais, como quanto à composição do polo passivo, determinando que há responsabilidade solidária entre controlador e operador quando o último descumprir ordens do primeiro e ocorrer dano ao titular (LGPD, art. 41, §1º, I), assim como entre controladores, quando houver dano e os dados forem tratados diretamente por mais de um controlador (LGPD, art. 41, §1º, II). Nas disposições finais da LGPD, ainda é estipulado que, independentemente de instrumento privado, o responsável por escritório (ou congênere) de empresa estrangeira no Brasil é legitimado a receber notificações e intimações de todos os atos previstos na LGPD (LGPD, art. 61). Assim, busca-se imprimir celeridade e efetividade aos procedimentos da ANPD, mesmo contra empresa estrangeira. Ademais, é prevista a possibilidade de inversão do ônus da prova em favor do titular de dados sempre que houver hipossuficiência para produzir provas ou quando sua produção for excessivamente onerosa ao titular (LGPD, art. 41, §2º). Também é possível a proposição de ação coletiva quando existir dano coletivo (LGPD, art. 41, §3º) e há o direito de ação regressiva do agente de tratamento que reparar o dano quanto aos demais corresponsáveis (LGPD, art. 41, §4º). Ainda nessa seara são previstas três hipóteses de exclusão da responsabilidade: o agente não ter realizado o tratamento dos dados em questão (LGPD, art. 43, I), o agente não ter violado a legislação de proteção de dados (LGPD, art. 43, II) e o dano ser exclusivamente por culpa do titular ou de terceiro (LGPD, art. 43, III).

Último tópico a ser abordado é a responsabilidade civil dos agentes de tratamento. Inicialmente, controlador e operador podem ser responsáveis, sempre que causarem dano a titular por violação da LGPD (LGPD, art. 42, caput). Configurando-se relação de consumo, também há previsão expressa pela aplicação da responsabilidade objetiva e das demais normas quanto à responsabilidade de direito do consumidor (LGPD, art. 45). De forma cumulativa, também é prevista a aplicação de sanções administrativas pela ANPD (LGPD, art. 52, caput), elencadas em rol taxativo com oito sanções: “advertência com indicação de prazo para adoção de medidas corretivas” (LGPD, art. 52, I); publicização da infração após ser apurada e confirmada (LGPD, art. 52, IV); multa diária, até o limite da multa simples (LGPD, art. 52, III); multa simples, de até 2% do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil,

conforme seu último exercício, excluídos os tributos e limitada a 50 milhões de reais (LGPD, art. 52, II), podendo considerar-se o faturamento total (e não apenas nacional) quando o valor não for apresentado ou for apresentado de informa incompleta ou não for inequívoco e idôneo (LGPD, art. 52, §4º); suspensão parcial do banco de dados afetado por até 6 meses, prorrogáveis em períodos iguais até a regularização do tratamento (LGPD, art. 52, X); suspensão do tratamento de dados a que se refere a infração pelo período de 6 meses, prorrogáveis por igual período (LGPD, art. 52, XI) e; "proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados" (LGPD, art. 52, XII). Sendo os valores das multas destinados ao Fundo de Defesa de Interesses Difusos, previsto nas Leis 7.347/85 e 9.009/95 (LGPD, art. 52, §5º). Essas sanções podem ser divididas conforme dois critérios, sendo o primeiro deles a aplicabilidade a órgãos públicos, caso no qual as multas simples (art. 52, II) e diária (art. 52, III) são as únicas que não são aplicáveis (LGPD, art. 48, §3º), sem prejuízo de incidência das Leis 8.112/90 (regime jurídico dos servidores públicos civis da União, autarquias e fundações públicas federais), 8.429/92 (improbidade administrativa) e 12.527/11 (LAI), conforme o §3º do art. 48 da LGPD. Segundo critério é o de reincidência na mesma infração. Segundo esse critério, as sanções mais severas (relacionadas a suspensões ou proibições, previstas nos incisos X e XI do art. 52 da LGPD), só podem ser aplicadas em caso de reincidência específica quanto ao mesmo caso concreto e já tendo sido imposta ao menos uma das sanções menos severas (LGPD, art. 52, §6º e I). Ressalte-se que se o controlador for submetido a outro órgão ou entidade com poder sancionatório, este também deve ser ouvido antes da imposição de uma sanção mais severa (LGPD, art. 52, §6º, II). Também merece destaque que essas sanções podem ser cumuladas com sanções administrativas, civis ou penais do Código de Defesa do Consumidor, a Lei 8.078 e de legislação específica (LGPD, art. 52, §2º).

Evidentemente a aplicação de sanção é precedida de procedimento administrativo com respeito à ampla defesa, que pode ser gradativa, isolada ou cumulativa, conforme o caso concreto (LGPD, art. 52, §1º) e que terá como critérios de dosimetria: "gravidade e natureza das infrações e dos direitos pessoais afetados" (inciso I); "boa-fé do infrator" (inciso II); "vantagem auferida ou pretendida pelo infrator" (inciso III); "condição econômica do infrator" (inciso IV); "reincidência" (inciso V); "grau do dano" (inciso VI); "cooperação do infrator" (Inciso VII); adoção de medidas para reverter ou mitigar os efeitos do incidente (inciso VIII);

“adoção de políticas de boas práticas e governança” (inciso IX); “pronta adoção de medidas corretivas” (inciso X) e; proporcionalidade entre infração e sanção (inciso XI). Quanto à multa diária, está deverá ser proporcional à gravidade e ao dano, devendo a intimação que a comunica descrever a obrigação imposta, prazo estipulado para seu cumprimento (que deve ser razoável) e seu valor diário, sendo facultado à ANPD acrescentar outras informações (LGPD, art. 54, *caput* e § único). Além desses critérios gerais, também foi reservada competência à ANPD para dispor de forma mais minuciosa sobre regulamento de dosimetria das sanções de multa (LGPD, art. 53, *caput*).

Antecedentes da LGPD

O prof. Danilo Doneda leciona que existem objetos de tutela constitucional que já tangenciavam a proteção constitucional aos dados pessoais antes de sua inclusão no rol do art. 5º da Constituição Federal dentro do próprio art. 5º: a inviolabilidade da intimidade e da vida privada (inciso X), de comunicações em geral e de dados (inciso XII) e do domicílio (inciso XI). Também já previa a ação de *habeas data* (art. 5º, LXXII), cujo propósito é o acesso e retificação de dados pessoais em bancos de dados da administração pública. Também reflete acerca de uma proteção de dados pessoais “primitiva” em âmbito legal, a qual denomina como período “pré-constitucional” de proteção da privacidade (DONEDA, 2020).

O CDC, elaborado em 1990, conta com previsões específicas quanto a bancos de dados. Contudo, limita-se a uma proteção baseada no *Fair Credit Reporting Act* de 1970, dos EUA (DONEDA, 2020). Os artigos 43 e 44 do diploma legal tratam do assunto, prevendo os direitos do consumidor de ter ciência da abertura de ficha de cadastro sobre si, dos dados registrados serem acessíveis e corretos (sob pena de detenção ou multa, conforme os arts. 72 e 73 do CDC), assim como de que não sejam armazenadas informações negativas sobre si por mais de cinco anos e que não sejam mantidos registros de dívidas prescritas. Há também a definição da natureza jurídica dos bancos de dados sobre consumidores como de direito público e a previsão

de publicação de lista de reclamações quanto a fornecedores de forma pública e regular (art. 43, §4 e art. 44, *caput*). Por fim, há previsão específica de exclusão do registro do consumidor em inadimplência nos casos de repactuação de dívidas em situação de superendividamento conforme data estipulada em plano de pagamento homologado na conciliação (104-A a 104-C do CDC, inclusos pela Lei 14.181 de 2021). No mesmo âmbito da tutela de bancos de dados, existe o *credit scoring*, cuja tutela foi pormenorizada pela Lei do Cadastro Positivo (Lei 12.414 de 2021).

Já em âmbito constitucional, o *habeas data* também tem relações com a proteção de dados pessoais. Doneda destaca que o *habeas data* é um instituto jurídico predominantemente brasileiro, mas que se espalhou pela América do Sul em virtude de um contexto político em comum: a redemocratização das nações sul-americanas em momento de superação da onda de ditaduras militares iniciada em 1964. Em especial, destaca-se o papel da informação na ditadura brasileira e nas ditaduras da América do Sul, durante as quais, nas palavras de Luis Roberto Barroso:

> "os órgãos de segurança mergulharam em terreno pantanoso de perseguições a adversários, operando frequentemente nas fronteiras da marginalidade. A chamada comunidade de informações passou a constituir um poder paralelo e agressivo, que, por vezes, sobrepunha-se ao poder político institucional, valendo-se de meios ilícitos para fins condenáveis" (BARROSO, 1998. *In*: DONEDA, 2020).

Doneda também indica que parte da doutrina entende que o *habeas data* tem inspiração no direito dos EUA, como é o caso do e. Ministro do STF, Alexandre de Moraes. Moraes aponta que a referência é o *Freedom of Infomation Act* de 1974, assim como sua reforma de 1978 e, ao abordar a finalidade do *habeas data* traz interessantes referências das doutrinas brasileira e portuguesa, que conta com dispositivo similar em sua Constituição (MORAES, 2018). Primeiramente, cita Michel Temer, que afirma que o *habeas data* "é fruto de uma experiência constitucional anterior, em que o governo arquivava, a seu critério e sigilosamente, dados referentes à convicção filosófica, política, religiosa e de conduta pessoal dos indivíduos" (TEMER, 1995. *In*: MORAES, 2018). Em sequência, resgata lição de Canotilho e Vital

Moreira: “no âmbito normativo do direito à identidade pessoal inclui-se o direito de acesso à informação sobre a identificação civil a fim de o titular do direito tomar conhecimento dos dados de identificação e poder exigir a sua rectificação ou actualização” (CANOTILHO; VITAL, 1991. *In*: MORAES, 2018).

Da primeira citação temos o *habeas data* como aspecto estruturante do Estado, impactando em seu *modus operandi*, e, da segunda, temos o *habeas data* como parte do feixe de direitos vinculados diretamente à dignidade humana, ambas questões relevantes a nível constitucional e com impactos sobre a compreensão do direito constitucional de proteção de dados pessoais. Moraes também ensina que a ação de *habeas data* pode ter, como objeto, dados de pessoas físicas ou jurídicas (sujeitos de legitimidade ativa) armazenados pelo poder público ou pessoa privada em exercício de função pública ou de interesse público (sujeitos de legitimidade passiva; destaque-se, quanto ao interesse público, como exemplo, o caso dos bancos de dados de *credit scoring*, citados anteriormente, que por força do art. 43, §4 do CDC possuem natureza jurídica de direito público). Também destaca a dupla finalidade do *habeas data*, composta pelo acesso e retificação, que pode ser atingida de forma consecutiva ou isolada (caso de não ser necessária retificação ou de já se ter o acesso e buscar-se apenas a retificação). Discorre sobre a competência de foro quanto ao sujeito e à matéria, assim como quanto ao cabimento, destacando o requisito de denegação pela via administrativa, e, por fim, da controvérsia quanto ao objeto ser protegido por sigilo, caso no qual filia-se ao entendimento de que isso não deve impedir o acesso do titular (MORAES, 2018).

Em complementação ao remédio constitucional do *habeas data*, ressalta-se que sua fundamentação reside no inciso XXXIII do art. 5º da CRFB:

> “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado” (CRFB, art, 5º, XXXIII).

Esse direito tem como decorrência infraconstitucional a Lei 12.527 de 2011 (Lei de Acesso à Informação ou, simplesmente, LAI). A LAI, logo de princípio tem algumas similaridades notáveis com a LGPD, dentre elas, a definição de “informação pessoal” como referente à pessoa identificada ou identificável (art. 4º, IV); os conceitos de “tratamento de

informação" (art. 4º, V), de qualidade dos dados (art. 4º, VII, VIII e IX) e, por fim; o direito do particular de acessar informações a seu respeito e de que estas sejam mantidas em segurança (art. 6º). A LAI, no entanto, diferencia-se da LGPD por alguns fatores: por uma incidência mais restrita quanto ao sujeito passivo, limitando-se às relações Estado-cidadão, conforme o art. 1º (a LGPD também trata de relações puramente privadas), e por uma incidência mais ampla quanto ao sujeito passivo e ao objeto, incluindo-se, por um lado, pessoas jurídicas (art. 10, *caput*) e, por outro, somando-se as informações de interesse público[1] (art. 10, *caput* e §1º) às informações pessoais como dados acessíveis ao requerente.

Outra lei ordinária de grande relevância quanto ao assunto é o Marco Civil da Internet (MCI), sendo, provavelmente, a Lei mais próxima à LGPD. Sancionada em 2014, foi a primeira tentativa na legislação brasileira de regular o mundo virtual de forma sistemática (intervenções pontuais e setoriais já haviam sido feitas, como nos casos da LAI, do CDC e da Lei Carolina Dieckmann). Chiara Spadaccini Teffé e Maria Celina Bodin afirmam que, segundo o MCI: "a internet brasileira se encontra alicerçada em um tripé axiológico formado pelos princípios da neutralidade da rede, da privacidade e da liberdade de expressão, que estão ligados entre si" (TEFFÉ; MORAES, 2017), conforme o art. 3º do MCI. Entendem que a neutralidade se refere à ausência de filtragem ou qualquer intervenção nos dados enviados e recebidos. Já a privacidade, como a vedação à circulação indiscriminada de informações pessoais, tendo em vista, especialmente, evitar que se exerça controle ilegítimo sobre o indivíduo. Por fim, a liberdade de expressão, em sua concepção comum, é reforçada como condição *sine qua non* do uso da internet no Brasil (TEFFÉ; MORAES, 2017).

A Lei tem como sujeitos passivos, aos quais são impostos deveres e limitações os provedores de conexão à internet e de aplicações, conforme indicado em alguns artigos da Lei, como no art. 7º, XI e no art. 11, *caput* (resumidamente, os primeiros são os que oferecem serviço de acesso à internet, como o 4G, e os segundos oferecem serviços dentro da internet,

[1] Isto é, aquelas voltadas à fiscalização cidadã do Estado, cujo exercício pode ser efetivado pela Ação Popular (art. 5º, LXXII da CRFB e Lei 4.717).

armazenando em seus servidores dados dos clientes ou usuários, por exemplo, qualquer serviço de e-mail). Já o polo ativo é composto pelos "usuários de serviços da internet" e, apesar da conjugação entre "acesso à internet" e "exercício da cidadania" (arts. 2º, II; 7º, *caput*; 24, IX; 26, *caput*), não há determinação expressa de que apenas pessoas físicas são consideradas como usuários. De toda forma, o MCI estipula rol de direitos dos titulares no art. 7º, composto por treze incisos, sendo o último deles uma cláusula de aplicação da proteção do consumidor às relações de consumo na internet. Os demais direitos podem ser resumidos à inviolabilidade da privacidade, das informações em tráfego e daquelas armazenadas (I, II e III), ao acesso à informação clara sobre o serviço prestado, assim como sobre o tratamento, armazenamento e proteção de dados pessoais (VI e VIII) e a ininterrupção da qualidade do acesso à internet (IV). Uma das inovações dessa lei foi a previsão de responsabilização dos provedores por danos causados por terceiros, buscando garantir segurança jurídica a uma situação que já era atual devido a ofensas em redes sociais, a exemplo da Ação Cível 990.10.126.564-8 de 2010, na qual o piloto Rubens Barrichello processa o provedor Orkut por ter se negado a retirar do ar 91 comunidades e 348 perfis falsos cujo propósito era ofender o piloto, culminando em condenação ao pagamento de indenização por danos morais em 200 mil reais e à indisponibilidade dos referidos conteúdos (TEFFÉ; MORAES, 2017).

Todavia, o otimismo inicial logo é dissipado ao se analisar o sistema de regulação criado pelo MCI, cujo núcleo está em seu art. 19:

> "Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário" (MCI, art. 19).

Anderson Schreiber apresenta importante interpretação crítica dessa disposição, afirmando que, em primeiro lugar, a ressalva ao início do *caput* já causa certo estranhamento, uma vez que responsabilidade civil pressupõe um abuso de direito (da liberdade de expressão)

e a causação de dano a terceiro. Em seguida, ao vincular a remoção de conteúdo ofensivo ao pré-requisito do recebimento de ordem judicial, cria uma redundância legal cujo único efeito é retardar a tutela efetiva dos direitos do ofendido (por exemplo, a remoção de conteúdo ofensivo). Explica que, naturalmente, a possibilidade de ingressar com uma ação judicial sempre existiu e que a violação de ordem judicial é crime de desobediência, conforme o Código Penal. Além disso, o requisito de que a ordem seja específica também abre margem de interpretação para que a tutela efetiva dos direitos do indivíduo seja cumprida apenas parcialmente e seja necessário provocar o judiciário repetidamente até que seja concluída. Por fim, segundo o MCI, a responsabilidade por indenização de danos só é cabível se, após todo o processo judicial, publicação de sentença e notificação do provedor, este não executar as ordens específicas, o que, na prática, faz com que danos já cometidos não sejam reparados (SCHREIBER, 2015).

Schreiber considera ainda mais grave que ao se observar a jurisprudência anterior há notório retrocesso do MCI na tutela do tema. Explica que os tribunais já vinham incorporando a técnica do *notice and take-down*, transplantada de legislação dos EUA, o *Digital Millenium Copyright Act*, que previa procedimento denominado pelo autor como "responsabilidade *ex-post*". Nesses casos, como forma de garantir uma tutela rápida, eficaz e conceder estímulos aos provedores para que cumprissem atividade fiscalizatória em suas redes, estes estariam obrigados a remover conteúdo ofensivo assim que notificados pelo titular e, cumprindo a requisição, não teriam responsabilidade sobre os danos já provocados. Assim, a "responsabilidade *ex-post*" é caracterizada por incidir apenas a partir do momento em que o responsável é notificado pelo ofendido, isto é, após o dano já existir. Ressalta, todavia, que era necessária maior regulação legal, uma vez que o transplante do "*notice and take-down*" foi feito sem trazer consigo a sistemática que o envolve (requisitos específicos da notificação e uma contra-notificação ao "usuário-ofensor", por exemplo). Também ressalta que, mesmo antes desse aporte, a jurisprudência brasileira já adotava mecanismos da legislação pátria para garantir essa tutela: caracterizada relação de consumidor entre usuário e o provedor, aplicava-se a tese de prestação de serviço defeituoso; assim como, na esfera cível, chegou a ser adotado entendimento pelo STJ de que a atividade dos provedores é atividade de risco, conforme o art. 927, parágrafo único do Código Civil, isto é a aplicação da responsabilidade objetiva a esses casos (SCHREIBER, 2015). Para concluir o tema, resta destacar que Schreiber ainda enfrenta

questão no âmago da problemática, quanto à caracterização das empresas provedoras, que se consideram meras "gestoras" das plataformas. Porém, para Schreiber, elas são "juridicamente proprietárias da marca, do endereço eletrônico, do espaço publicitário e de tudo o mais que compõe a rede social" (SCHREIBER, 2015) e, portanto, devem ser civilmente responsabilizadas pelos danos causados em seu espaço virtual.

Considerações materiais sobre proteção de dados pessoais

Ao longo da abordagem acerca da legislação pertinente ao tema, foram abordados alguns aspectos concretos com relação ao tema da proteção de dados pessoais, especialmente as ofensas proferidas, de forma pública, no ambiente virtual e o vigilantismo das ditaduras sul-americanas. Em sequência, estes serão aprofundados apenas pela perspectiva concreta, tendo em vista uma melhor compreensão sobre o que esses direitos efetivamente versam.

Simson Garfinkel aborda a evolução da relação entre sistemas de informática e a privacidade. Lembra inicialmente que, nos idos dos anos 80, a grande preocupação era que a tecnologia concretizasse a distopia orwelliana de vigilância estatal, em detalhes, de todo o cotidiano dos cidadãos. Contudo, com o passar do tempo, as preocupações mudaram. O autor exemplifica com o caso dos cartões de crédito, cujas reclamações não são por registrarem todo uso. Reclama-se justamente quando uma transação não é registrada (GARFINKEL, 2000). Ainda mais atualmente, com a difusão das redes sociais, a própria figura de um sistema externo que armazena os dados vem sendo substituída pelos próprios indivíduos, que voluntariamente registram (e oferecem aos servidores de terceiros) detalhes de suas vidas e de seu cotidiano. Assim, o temor de perda da privacidade foi substituído pelo entusiasmo da conexão. Garfinkel indica que, ao contrário dessa expectativa de controle, um problema que se tornou frequente foi o roubo de identidade, isto é, o acesso indevido a dados pessoais e seu uso por um criminoso.

O caso mais emblemático desse tipo de prática é o roubo de dados relacionados a cartões de crédito, quando o cartão é usado para realizar diversas compras, culminando em grandes transtornos ao verdadeiro proprietário. Isto porque, conforme Garfinkel afirma, de forma concisa, há uma grande confiança das instituições nos bancos de dados, inclusive para identificar pessoas de forma granular, sendo que não há garantia de que os bancos de dados tenham informações corretas (GARFINKEL, 2000). Nesse sentido, apresenta exemplo que desvia dos casos corriqueiramente comentados, de que a identificação por papiloscopia (biometria, especialmente dos dedos) apenas vincula um dedo a um dado. Dessa forma, a simples substituição de um dado por outro, com a troca de seu "rótulo", isto é, a identificação do dedo ao qual o dado se refere, culmina em um erro no banco de dados e em um erro quanto à identificação de um indivíduo, seja para um banco ou seja para uma investigação policial. De forma direta, o autor afirma: "as técnicas não identificam pessoas, elas identificam corpos" (GARFINKEL, 2000, tradução nossa). Mitnick reconhece o outro lado da mesma moeda: "a maior parte das informações aparentemente inúteis sob a posse de uma empresa são valorizadas por um engenheiro social agressor, porque elas cumprem um papel vital em seu esforço de vestir-se com uma capa de credibilidade (MITNICK; SIMON, 2002); "tais quais peças de um quebra-cabeça, cada peça de informação pode ser irrelevante por si só. Contudo, quando as peças são juntadas, emerge uma imagem clara" (MITNICK; SIMON, 2002, tradução nossa) e, exemplificando:

> "apenas porque alguém ligando ou um visitante conhece o nome de algumas pessoas da empresa, ou conhece alguns jargões e procedimentos da empresa, não significa que ele é quem diz ser. E isto definitivamente não o caracteriza como uma pessoa autorizada a receber informação interna, ou a acessar o sistema ou rede de computadores" (MITNICK; SIMON, 2002, tradução nossa).

Em sua obra, "The Art of Deception", Mitnick apresenta diversos casos de como criminosos muitas vezes colocados como "hackers", são na verdade engenheiros sociais, que atingem seus objetivos principalmente por explorar pessoas ao invés de desafiar sistemas de segurança eletrônicos (*firewalls*, criptografia etc.). Mitnick apresenta situações em que uma pessoa pode fingir ser outra para obter informações internas menos relevantes e, progressivamente ganhar maior credibilidade em suas enganações ao ponto de fazer-se parecer

ter credenciais para acessar informações sigilosas (e conseguir). Em uma de suas histórias exemplificativas, uma recrutadora é contratada para buscar talentos com experiência e de dentro dos quadros de uma outra empresa. Em um primeiro telefonema, busca o contato do setor de transporte, fingindo ser uma funcionária que necessita do serviço, mas também pede e recebe o telefone de outros setores, dentre os quais o financeiro. Em uma segunda ligação, para o setor financeiro, finge ser uma funcionária com dúvidas quanto ao preenchimento de um formulário, pedindo e conseguindo o código do "*cost center*" de um dos escritórios da empresa. Em uma terceira ligação, para outro setor, finge ser uma funcionária da empresa e ter ligado por engano, aproveitando para perguntar para onde deveria ligar para obter uma nova cópia impressa do "*business directory*" (que tem contatos e cargos de todos os funcionários), recebendo o telefone do setor de publicações. Por fim, realiza a quarta e última ligação, para o setor de publicações, fingindo ser uma funcionária que requisita uma cópia do "*business directory*" para um novo consultor da empresa, indicando uma caixa postal para a qual o documento deveria ser enviado, também tendo sucesso, e ao receber, surpreende-se por também conter a estrutura hierárquica da empresa detalhada, facilitando seu trabalho (MITNICK; SIMON, 2002).

Esse é apenas um dos casos que Mitnick aborda em sua obra para discutir a segurança informacional de empresas, apresentando *modus operandi* específicos que requerem medidas ajustadas, mas que, nas palavras do autor, podem ser resumidas, de forma geral, às três citações apresentadas incialmente. Contudo, se Mitnick fala em um "manto de credibilidade" e em "enganação", é possível entender que esta nada mais é do que a perspectiva do farsante, enquanto, pela perspectiva da vítima (ou da pessoa enganada), o que ocorre, retomando a discussão suscitada por Garfinkel, é um erro de identificação. Contextualizando com um caso mais convencional de proteção de dados pessoais, também é observável a mesma lógica de tomar um caminho mais longo e mais inusitado, mas que, ao mesmo tempo, é consideravelmente menos tortuoso. Trata-se do caso do incidente de segurança da *British Airways*, que culminou em multa da autoridade de dados inglesa, o ICO, à empresa em 2018. Nesse caso, um hacker consegue se conectar, na condição de administrador (isto é, sem nenhuma restrição de acesso), ao banco de dados geral da empresa e obter informações sobre cartões de crédito de clientes (número, código de segurança, data de validade e senha em especial). Contudo, o que chama a atenção é que o criminoso obtém acesso infiltrando-se, inicialmente, no sistema de uma empresa terceirizada que prestava serviços de manejo de

bagagens em aeroportos para a companhia aérea. Esse sistema, aparentemente de menor risco, tinha um grau de segurança deficitário, que foi facilmente invadido pelo hacker, conseguindo acessá-lo depois como administrador e, em sequência, acessar o sistema da tomadora de serviços (ICO, 2020). Essa discussão torna mais nítido o conceito adotado pela LGPD de dado anonimizado, uma vez que o avanço da tecnologia pode permitir que mais informações "inúteis" consigam ser processadas e chegar a um resultado que transforme um dado anonimizado em um dado pessoal.

Retomando as reflexões de Garfinkel, este aponta quatro hipóteses para o tão comentado "erro de identificação": erro do sistema, erro humano, fraude (alteração intencional) e vigilantismo estatal (MITNICK; SIMON, 2002). Abordemos as quatro possibilidades citadas. A primeira delas é o erro da tecnologia, tendo como bom exemplo a campanha "tire meu rosto da sua mira", organizada pela Coalizão Direitos na Rede e que produziu o miniguia "reconhecimento facial: e quando a máquina erra?". Afirma-se que, em operação realizada em 2019 no Estádio do Maracanã, no Rio de Janeiro, o emprego de câmeras ligadas a programa de reconhecimento facial resultou em onze identificações de supostos criminosos, que foram detidos. Contudo, desses onze apenas quatro foram identificações corretas e os sete demais foram falsos positivos (COALIZÃO DIREITOS NA REDE, 2022). Na Bahia, em 2019, ocorreram 903 identificações por reconhecimento facial, das quais apenas 34 foram confirmadas e foram expedidos mandados de prisão (3,6% de aproveitamento); na cidade de Detroit, EUA, um chefe de polícia afirmou em 2020 que a taxa de acerto do reconhecimento facial foi em torno de 4%. O mesmo em Londres, Inglaterra, quando em 2019 a Universidade de Essex divulgou estudo apontando uma taxa de acerto de 9%, em média (COALIZÃO DIREITOS NA REDE, 2022). Também cumpre destacar que o erro de identificação na área criminal não é um novo problema, causado pela tecnologia que agrega bancos de dados e inteligência artificial para realizar reconhecimento de biometria facial. O reconhecimento fotográfico, quando uma pessoa (vítima ou testemunha) reconhece o suposto criminoso por fotografia, por exemplo, já causava problemas quanto ao erro de identificação antes disso.

Quanto à identificação fotográfica, o STJ reconhece em sua jurisprudência que se trata de uma evidência, ao invés de uma prova, ou seja, sem poder, por si só, de vincular uma pessoa à autoria do fato ilícito. Destaca que o reconhecimento fotográfico (ou mesmo pessoal) é afetado pela memória humana, que pode ser falha ou imprecisa (HC 639.792/RS, 2021). Garfinkel também destaca que algumas tecnologias de reconhecimento às quais se atribuí grande confiança usam parâmetros que podem ter variações. Notório exemplo é o uso de inteligência artificial para reconhecimento pela retina do olho, que tende a não funcionar em mulheres grávidas devido a uma alteração natural da retina durante a gravidez. Nesse caso, além da possibilidade de erro, há um risco severo de intrusão na vida do indivíduo, uma vez que as informações podem ser usadas para discriminação (GARFINKEL, 2000), como é vedado, por exemplo, pela Lei 9.029/95 que proíbe perguntas a esse respeito e a exigência de atestado negativo de gravidez em entrevista de emprego. Todavia, o principal objetivo da discussão sobre erro de identificação é demonstrar que um erro quanto à identificação do corpo pode causar sérios embaraços ao indivíduo. Portanto, se a identificação do corpo já causa sérios problemas, imagina-se quando o referencial é um conjunto de informações sobre o comportamento de uma pessoa no mundo virtual.

O erro humano, segunda hipótese de Garfinkel, por sua vez, pode ocorrer pelo já mencionado “roubo de identidade”, como já exemplificado pelos casos citados por Mitnick (engenharia social). A terceira hipótese, fraude, poderia ser exemplificada pelo caso dos cartões de crédito citado por Garfinkel, todavia, o que o autor almeja com essa hipótese é a situação em que a pessoa responsável por parte do processo de verificação altera informações para fraudá-lo e não um estelionato. O caso do cartão de crédito aproxima-se mais da falha humana ou de sistema, como um erro ou insuficiência no processo de identificação do que a presença de dolo na identificação equivocada. Exemplo mais adequado e recente é o caso das duas brasileiras que acabaram presas ao viajar para a Alemanha após funcionários do setor de carga do aeroporto de Guarulhos trocarem a identificação de suas malas com malas que carregavam drogas. O crime foi cometido para que, caso as drogas fossem identificadas, as duas fossem presas no lugar dos criminosos e, caso não fossem percebidas, elas pegariam suas malas por identificá-las pela aparência e não pela etiqueta, enquanto os criminosos procederiam com o tráfico ao buscar as malas com as drogas. Ocorre que a polícia alemã identificou o conteúdo das malas, verificou as etiquetas e deteve as duas até que a situação fosse esclarecida (CNN, 2023). Apesar

do caso não versar sobre identificação virtual, é muito útil para exemplificar como a troca de uma etiqueta pode afetar todo o processo de identificação. Nesse sentido, o mesmo poderia ser feito quanto à identificação de uma amostra de sangue ou de impressões digitais em uma cena de crime ou quanto à alteração de IP de um computador usado para cometer algum ilícito nas redes.

Último tipo de perigo dos citados é o relativo ao uso de dados pessoais pelo governo. No Brasil e na América do Sul o exemplo mais notório é o da Operação Condor, durante a qual as ditaduras militares do Cone Sul criaram um banco de dados comum com o propósito de realizar a perseguição a opositores políticos e contando, inclusive, com a contribuição de empresas privadas (QUADRAT, 2002; CHAVES; MIRANDA, 2015). Outro exemplo é o ocorrido nos EUA, em 1941, quando, dois dias após o ataque japonês a Pearl Harbor, o *Census Bureau* (instituto de estatística oficial encarregado de realizar os censos) disponibiliza às autoridades militares dos EUA mesodados do censo de 1940 referentes à população registrada com ascendência nipônica, isto é, informações a nível de bairro ou quarteirão da quantidade de moradores japoneses. O propósito dessas informações era a remoção e internação forçada dessa população em campos de encarceramento. Da mesma forma, o nazismo na Europa também fez uso de dados censitários para a prática de genocídio e de crimes contra a humanidade, sendo o caso mais emblemático de uso instrumental desses dados para a violação de direitos humanos (SELTZER; ANDERSON, 2001).

DIMENSÃO NORMATIVA

Caso Telekall Infoservice (1ª multa aplicada pela ANPD)

Em 6 de julho de 2023 a ANPD aplica sua primeira multa, que recai sobre a empresa Telekall Infoservice, tendo sido lavrado auto de infração em 10 de março do mesmo ano, que foi recebido pela pessoa designada como responsável legal que, *in casu*, é o próprio proprietário da Microempresa Individual. O processo administrativo tem como origem documentos enviados pela Promotoria de Ubatuba, do MPSP. O auto de infração nº 3 de 2022 do Conselho Geral de Fiscalização da ANPD é o principal documento que culmina no despacho decisório que aplica a multa. Nesse primeiro momento, são suscitadas possíveis infrações a quatro artigos da LGPD: os arts. 7º e 11, 37 e 38 (respectivamente, as bases de tratamento; ausência de registro das operações de tratamento de dados pessoais e; ausência de envio de relatório de impacto à ANPD). O caso versa sobre empresa que oferecia serviço de marketing eleitoral direto, no qual ocorreu denúncia ao Ministério Público de que a empresa ofertava pacotes, de até cem mil contatos telefônicos, em conjunto com outros dados pessoais, como nome, endereço completo e código de ocupação. O MP, por sua vez, noticia o fato à ANPD que inicia procedimento administrativo. Descrevendo a investigação de forma muito suscinta, a empresa não responde às comunicações da ANPD, mesmo por carta, até que recebe notificação de lavratura de auto de infração, quando passa a indicar o encarregado, na figura do próprio proprietário da empresa, declarando, por própria iniciativa, a suspensão preventiva de seus serviços para fins de readequação à LGPD (o que foi apurado como verdadeiro) e justifica que realizava o tratamento de dados pessoais até então conforme o entendimento de que os dados usados eram dados públicos, por terem sido coletados da internet.

Após o relatório, procede-se à fundamentação da competência da ANPD, em sede de preliminar. Quanto à caracterização da atividade de tratamento de dados por parte da empresa, compreende-se que a atividade de coleta e organização de contatos telefônicos para envio de mensagens consubstancia-se em tratamento de dados nos termos do art. 5º, X da LGPD. A

competência de atuação, fiscalização e aplicação de sanções por parte da ANPD, por sua vez, é fundamentada no art. 55-J, I e XX da LGPD. Por fim, é destacada a Resolução CD/ANPD nº 1, de 28/10/2021 que, em seu art. 5º especifica os deveres dos agentes de tratamento perante a ANPD que podem ser resumidos aos deveres de entregar documentos e informações quando requisitados, permitir o acesso às suas instalações e de terceiros para apuração de fato relativo ao tratamento de dados, submeter-se a auditoria da ANPD e a armazenar os documentos legalmente exigíveis pelo prazo legal. Considerando-se todos os fatores apresentados a nível de preliminares, a ANPD declara-se competente para avaliar o caso.

Avançando à análise, esta parte é dividida em três subpartes: (1) circunstâncias de infração e autoria; (2) análise da defesa apresentada pelo autuado e; (3) subsunção do fato ao tipo infracional correspondente. A primeira subparte aprofunda os fatos apresentados a nível de relatório oficial, contudo, para maior celeridade, todas as informações já foram condensadas na síntese inicial do caso ora apresentado. Cabe ressaltar que é afirmado que, em sua resposta, a empresa não nega os fatos que lhe são imputados quanto à atividade que realizava e que muitas dessas informações constavam no próprio *website* dela. Quanto à análise da defesa, segunda subparte, é especialmente relevante a análise de que a defesa apresentada é marcada pela obscuridade, por não responder qual a base legal de tratamento empregada. Da mesma forma, enfatiza-se que eram coletados dados disponíveis na internet com intuito de obtenção de lucro, com a formação de um banco de dados. A existência do banco de dados, para a ANPD, é caracterizada pela presença de dados estruturados (o que atende à definição de banco de dados do art. 5º, IV da LGPD), que eram pré-requisito para o disparo de mensagens em massa pelo meio utilizado.

Progredindo à subsunção do fato ao tipo infracional, o primeiro silogismo é quanto à falta de base legal de tratamento (arts. 7º da LGPD). O entendimento adotado pela ANPD foi que, de fato, eram dados públicos, conforme o art. 7º, §4º da LGPD. Feita essa caracterização, concluiu-se pela violação do art. 7º, pois, por um lado, o tratamento de dados públicos não afasta os direitos dos titulares e, como estes não foram notificados, o exercício desses direitos

restou inviabilizado. Por outro lado, concluiu-se pela violação do princípio da finalidade (art. 6º, I da LGPD) uma vez que se enquadra na vedação expressa na segunda parte do inciso[2], já que o disparo de mensagens em massa para propaganda político-eleitoral não tinha relação com a razão pela qual os dados eram disponibilizados. Portanto, o desrespeito aos direitos dos titulares e aos princípios da LGPD configuram vício insanável do tratamento de dados pessoais como dados públicos. Por fim, também é afastada a hipótese de tratamento posterior de dados pessoais prevista no art. 7º, §7º da LGPD, sob a lógica de que a ausência de declaração quanto à base legal utilizada torna impraticável a análise quanto à existência de propósitos legítimos e específicos, assim como de garantia dos direitos dos titulares. Conclui-se pela violação ao art. 7º como a primeira violação confirmada à LGPD. É oportuno abordar em conjunto a avaliação quanto à possível violação dos arts. 37 e 38 da LGPD, pois, ainda que avaliados em separado, possuem a mesma fundamentação. Em suma, a hipótese de violação a ambos foi afastada, uma vez que tratam do dever do agente de apresentar documentos específicos à ANPD e estes não foram solicitados. Também foi suscitada e confirmada a hipótese de violação do art. 41, uma vez que apenas foi possível identificar o encarregado após a lavratura do auto de infração. A última violação suscitada é relativa à obstrução da atividade fiscalizatória da ANPD, nos termos do art. 6º c/c art. 5º, I do Regulamento de Fiscalização da ANPD em virtude do silencio da empresa ao longo de todo o procedimento. Logo, compreendeu-se que ocorreu a violação do dever de "fornecer (...) dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD" (art. 5º, I do Regulamento de Fiscalização da ANPD). Segundo a literalidade do art. 6º do mesmo regulamento essa conduta implica no ilícito de obstrução da fiscalização, o que foi corroborado pela ANPD (BRASIL, 2023a).

Prosseguindo à dosimetria, quanto à violação o dever de realizar tratamento de dados conforme uma das bases legais, a ANPD entendeu que fica caraterizada infração leve, por não impedir ou limitar o exercício de direitos ou a utilização de serviços, o que significaria na aplicação da sanção de advertência. Por outro lado, também foi considerado que:

> "o art. 7º da LGPD é a espinha dorsal da LGPD, sem o qual não existe fundamento legal para um tratamento legítimo de dados. Em outras palavras, o

[2] "Sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (LGPD, art. 6º, I)

> tratamento de dados sem amparo em pelo menos uma das bases legais do art. 7º da LGPD é uma infração que, isoladamente, possui contornos de maior gravidade uma vez que possui como objeto um dos fundamentos da própria existência da LGPD" (BRASIL, 2023a).

Com base nessa fundamentação, decide-se por aplicar o art. 10, inciso III do Regulamento de Dosimetria, como cláusula de abertura para incidência da pena de multa. Também é suscitada a alínea "b" do §3º (que trata de infrações graves) do art. 8º do Regulamento de Dosimetria para justificar que se trata de uma infração leve de maior gravidade, uma vez que existia o objetivo de auferir vantagem econômica, sendo cabível a pena de multa, definida pelo dobro da vantagem auferida ou pretendida (art. 15, inciso I do Regulamento de Dosimetria). Definida a aplicação da pena de multa, prossegue-se para a definição do faturamento da empresa, informação que havia sido requisitada durante o procedimento preparatório, mas não foi fornecida. Dessa forma, é aplicada a alínea "a" do inciso IV do parágrafo primeiro do Regulamento de Dosimetria para definir o faturamento conforme o limite máximo da LCP 123, isto é, trezentos e sessenta mil reais (art. 3º, I, LCP 123). Considerando-se o grau de dano dois em virtude do número de titulares possivelmente atingidos (banco de dados com dados pessoais de ao menos cem mil titulares), procede-se à aplicação da dosimetria e obtém-se um valor-base da multa de setecentos e noventa e dois reais que ainda são reduzidos pela metade uma vez que é aplicada a atenuante de cessação da infração até a instauração de processo administrativo sancionador, o que resulta em uma multa de trezentos e noventa e seis reais. Por fim, a adequação aos valores mínimos e máximos dá maior peso à punição, pois considera que a vantagem pretendida com o maior pacote de informações era de cinco mil duzentos e cinquenta reais, aplicando-se o art. 15, I do Regulamento para definir a multa como o dobro desse valor, fixada, portanto, em dez mil e quinhentos reais.

Posteriormente é definida sanção de advertência pela ausência de indicação do encarregado de dados (violação ao art. 41 da LGPD), considerando-se que não há qualquer tipo de reincidência. Por fim, calcula-se a multa pela obstrução à atividade de fiscalização (art.5º do Regulamento de Fiscalização), definida como grave pelo art. o, §3º, II do Regulamento de

Dosimetria. A definição da infração como grave também vincula a aplicação obrigatória de multa (BRASIL, 2023b). Também é arbitrado que o grau de dano em questão equivale ao nível um:

> "uma vez que consistiu em descumprimento de determinação ou envio ou disponibilização de informações fora dos prazos ou condições estabelecidos pela ANPD, sem prejuízo direto para o processo de fiscalização ou administrativo sancionador ou para terceiros e que não decorra de litigância de má-fé" (BRASIL, 2023a).

A multa-base para essa infração, portanto, é definida em dois mil oitocentos e oitenta reais. É considerado que não há incidência de atenuantes ou agravantes e, por fim, observa-se que a multa está abaixo do mínimo para o autuado (doze mil reais, conforme a tabela dois do apêndice I do Regulamento de Dosimetria). Contudo, também é considerado que a aplicação do valor nominal mínimo excederia o limite máximo de 2% do faturamento. Conclui a ANPD por fixar a multa por obstrução à fiscalização em sete mil e duzentos reais, valor equivalente a 2% do faturamento da empresa (sanção mais severa conforme a LGPD).

Por fim, é definida aplicação da multa global, reduzindo as multas aplicadas ao limite de 2% do faturamento anual (a multa de infração ao art. 7º é reduzida de dez mil e quinhentos reais para sete mil e duzentos reais e é mantida a multa de sete mil e duzentos reais para a obstrução à fiscalização, totalizando quatorze mil e quatrocentos reais), além da aplicação de advertência por ausência de indicação de encarregado de dados (BRASIL, 2023a).

ADI 6.387 (reconhecimento dos direitos fundamentais implícitos à autodeterminação informativa e à proteção de dados pessoais)

No Brasil, o reconhecimento da proteção de dados pessoais como direito constitucional tem como um de seus principais marcos a Medida Cautelar concedida pelo STF nos autos das ADIs n. 6.387, 6.388, 6.389, 6.390 e 6.393/2020, conforme decisão da Ministra Rosa Weber

que foi referendada por maioria de 10 votos e suspendeu a eficácia da Medida Provisória 954/2020 (BIONI *et al*, 2021). A referida Medida Provisória, editada durante a pandemia visava à realização do censo do IBGE por meio telemático, obrigando empresas de telecomunicação prestadoras dos serviços de telefonia fixa e móvel (STFC e SMP) a compartilhar com o IBGE "a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas" (MPV 954/2020, art. 2º). O IBGE, por sua vez, utilizaria os dados para realizar entrevistas não presenciais, com caráter de pesquisa domiciliar (MPV 954/2020, art. 2º §2º), sendo previsto que teriam caráter sigiloso e seriam usadas exclusivamente para a finalidade de pesquisa de censo, sendo intransmissíveis a outros órgãos, assim como seriam eliminadas das bases de dados do IBGE após o término da emergência sanitária de COVID-19 (MPV 954/2020, art. 3º, I e II, §1º e art. 4º, *caput*).

Resumidamente, as ADIs, em conjunto, alegavam inconstitucionalidade material da MP, pois "a Medida Provisória em análise viola o sigilo de dados dos brasileiros e invade a privacidade e a intimidade de todos" (BRASIL, 2020). As ADIs 6.387, 6.389 e 6.390 também alegaram a violação à dignidade humana e duas delas (ADIs 6.393 e 6.389) alegaram violação a um direito implícito à proteção de dados que decorre dos demais direitos fundamentais supracitados. A ADI proposta pelo Conselho Federal da OAB ainda postula a violação ao direito fundamental à autodeterminação informativa, também implícito na CRFB. Por fim, duas delas (ADIs 6.389 e 6.387) também postularam inconstitucionalidade formal em decorrência da falta dos requisitos de relevância e urgência, conforme o art. 62 da CRFB. Por economia, será observada apenas a ADI da OAB, uma vez que, conforme o próprio voto da Ministra Relatora, das cinco ADI's, ela "é a mais ampla, abarcando o objeto das demais" (BRASIL, 2020).

Em seu relatório, a Ministra Relatora Rosa Weber resgata os principais argumentos suscitados ao conceder medida cautelar antecedente. Destaca que as disposições do art. 5º, XII da CRFB (corriqueiramente referidas como "sigilo de correspondência", mas que a Ministra também destaca abranger, explicitamente, a inviolabilidade de dados) são uma instrumentalização do direito à privacidade (que entende como cristalizado no art. 5º, X da

CRFB, por meio da inviolabilidade de direitos da personalidade), relativizada apenas perante autorização judicial em âmbito criminal. Afirma que os dados pessoais, nos termos da LGPD, são efetivamente protegidos pela liberdade individual geral (art. 5º, *caput*), pela privacidade (art. 5º, X) e pela autodeterminação informativa (que identifica como o art. 5º, XII, isto é, o sigilo de correspondência). Avança à análise das disposições acerca do tratamento previsto pela Medida Provisória, entende que elas são escassas, sem que delimitem objeto, finalidade e amplitude específicos das pesquisas estatísticas e que apenas a previsão de duração até o término da pandemia de Covid-19 permite alguma inferência quanto à finalidade ser a contenção da crise sanitária (BRASIL, 2020).

Em razão dessas considerações, entende que não há demonstração de legítimo interesse público que fundamente o compartilhamento dos dados e que a indefinição quanto à finalidade e à forma de uso acarretam em impossibilidade de avaliação da adequação (conforme a finalidade) e a necessidade (conforme o mínimo necessário), o que, por sua vez, implica violação do devido processo legal. Também entende que a MPv falha em garantir a proteção dos dados pessoais, pois apenas delega ao Presidente do IBGE o ato de delimitar a forma como se dará o procedimento, sem prever mecanismos de proteção. Afirma que, por um lado, em apenas cinco dias foram enviados ofícios às empresas de telefonia requisitando os dados com urgência, com base em Instrução Normativa publicada no mesmo dia da MPv, quando o prazo definido nela era de cinco dias e, por outro lado, o projeto de lei de conversão da MPv conta com mais de trezentas propostas de emenda, muitas das quais visando restringir o âmbito do tratamento de dados e incluir maiores garantias aos titulares, o que expressa certa discordância do parlamento e que a eventual lei de conversão não será aprovada de forma célere. Dessa forma, ainda destaca que "não se subestima a gravidade do cenário de urgência decorrente da crise sanitária, (...). O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição" e que, por outro lado,

> "a adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade. Vale dizer, uma vez afrontada a norma de proteção de tais direitos, o ressarcimento se apresenta como tutela insuficiente aos deveres de proteção" (BRASIL, 2020).

Em complementação, ao submeter o deferimento da tutela cautelar ao plenário para referendo, a Ministra Rosa Weber destaca que, mesmo com a concessão da medida cautelar, o IBGE obteve êxito em realizar pesquisa demográfica[3], cumprida com o uso de números telefônicos já cadastrados na consulta PNAD Contínua de 2019. Segundo a Ministra Rosa Weber, isso já denota "a desnecessidade e o excesso do compartilhamento de dados tal como disciplinado na MP nº 954/220" (BRASIL, 2020). Além disso, destaca que a pesquisa foi realizada por meio de amostragem, metodologia consolidado pelo IBGE e que fez uso de uma base de dados correspondente a cerca de 0,1% daquela que seria utilizada conforme a MPv (211 mil telefones da PNAD Contínua 2019 comparados com mais de 200 milhões de linhas telefônicas cadastradas no Brasil). Também resgata o Decreto nº 10.212 de 2020, que internaliza o Regulamento Sanitário Internacional (RSI 2005) da OMS, para enfatizar que o tratamento de dados para avaliação e manejo de um risco para a saúde pública deve ter como requisitos a limitação do tratamento ao essencial e que os dados, assim como o tempo de armazenamento não sejam excessivos. Dessa forma, além da excessividade de dados já abordada, também ocorre excesso quanto ao tempo de armazenamento, uma vez que os dados poderiam ser armazenados e tratados a até trinta dias após o término da emergência de saúde. Esse período posterior, por si só, contradiz a finalidade de enfrentamento à crise sanitária de Covid-19. Ademais, agrava-se a situação pela ausência da vinculação do tratamento a requisitos mínimos de segurança, em especial a anonimização e a pseudoanonimização. Da mesma forma, a Ministra destaca que não há previsão de auditoria externa ou de responsabilização por tratamento irregular. Concluindo seu voto, a eminente Ministra afirma que reconhece a relevância da realização de pesquisas estatísticas para o planejamento de políticas públicas, porém, que este interesse não se sobrepõe aos direitos fundamentais e da personalidade. Ademais, apresenta citação à qual merece transcrição integral, ao afirmar quanto aos riscos da flexibilização de direitos fundamentais em momentos de grave crise, como a pandemia de Covid-19:

> "uma oportunidade sem precedentes para os governos justificarem a expansão pós-pandêmica de políticas de vigilância e de coleta de dados tanto de cidadãos quanto de não cidadãos" (BRASIL, 2020).
>
> "a história nos ensina que uma vez estabelecidos, é improvável que poderes governamentais de vigilância e coleta de dados de seus cidadãos e residentes

[3] PNAD Covid, sobre os impactos da pandemia no mercado de trabalho

> retrocedam voluntariamente. E a história também tem nos ensinado que uma vez que dados são coletados para um propósito, é muito difícil evitar que sejam usados para fins outros não relacionados.
>
> (...)
>
> Sempre haverá a próxima pandemia em algum momento no futuro, se não de COVID-19, de algum outro agente infeccioso. Os desafios que as pandemias apresentam para a privacidade da informação não irão embora nem se atenuarão com brevidade" (LONG, 2020 *In*: BRASIL, 2020).

Em sequência, o eminente Ministro Edson Fachin apresenta seu voto e divide sua argumentação em duas partes principais, cada qual relativa aos bens jurídicos em conflito: produção de pesquisas estatísticas para fundamentar políticas públicas e direitos individuais afetados. Quanto ao primeiro aspecto, afirma que as pesquisas estatísticas têm relevante papel:

> "garantem não somente a efetiva realização das funções do Estado, ou o apuro técnico dos serviços públicos, mas também o justo controle político dos Poderes republicanos. Porque as políticas públicas podem ser analisadas racionalmente, elas também podem ser objeto do escrutínio dos cidadãos nos 'fluxos de formação discursiva da opinião e da vontade' (HABERMAS, Jürgen. Fakzität und Geltung: Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtstaats. Frankfurt am Main: Suhrkamp, 1992). Em outras palavras, Demografia e Estatística contribuem de forma decisiva para a racionalização do debate público e, neste sentido, são essenciais para o pleno exercício da cidadania" (BRASIL, 2020).

Por outro lado, entende que a MPv prevê severa intervenção na vida privada, a qual só seria possível com garantias procedimentais específicas. Prosseguindo com fundamentação próxima das anteriores, acompanha o voto da eminente Ministra Relatora Rosa Weber.

O eminente Ministro Luiz Fux contextualiza a questão referente ao conflito entre "(i) a exigência de produção estatística para o desenho de políticas públicas de combate ao

coronavírus e (ii) os direitos fundamentais à proteção de dados, à autodeterminação informativa e à privacidade" (BRASIL, 2020). Resgata a máxima de que os dados são o novo "petróleo" e cita o caso *Cambridge Analytica* para destacar o valor dos dados e os riscos "à privacidade dos indivíduos e à própria democracia" (BRASIL, 2020), qualificando os dados como uma mercadoria sem uma tutela legal eficaz. Também cita a célebre decisão do Tribunal Constitucional alemão no caso Lei do Censo de 1983, destacando que "não existem mais dados insignificantes" (BRASIL, 2020), de forma que mesmo dados simples como nomes apresentam riscos se cruzados com outros dados, seja pelo controlador "primário" ou por aquele com quem eles foram compartilhados. Prosseguindo ao caso em tela, afirma que "a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos" (BRASIL, 2020). Dessa forma, o eminente Ministro Luiz Fux entende que tratam-se de direitos fundamentais implícitos na CRFB, que decorrem de "interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do *habeas data* (art. 5º, LXXII)" (BRASIL, 2020).

Ressalte-se que o voto foi proferido em 2020 e apenas em 2022 seria aprovada a EC 115, incluindo a proteção de dados no rol do artigo quinto. Essa postura (tanto do Ministro Fux, quanto dos demais que também se manifestam no mesmo sentido) indica raízes no constitucionalismo brasileiro desses direitos, descaracterizando-os como meros implantes do direito estrangeiro. Todavia, a influência do direito comparado não é ignorada, sendo citada a Carta de Direitos Fundamentais da União Europeia, que prevê a proteção de dados pessoais como direito fundamental em seu art. 8º. O mesmo status foi conferido a esse direito pelo Tribunal de Justiça da União Europeia, no caso *Digital Rights Ireland* (C-293/12), assim como na célebre decisão do Tribunal Constitucional Alemão no caso da Lei do Censo de 1983, a qual reconhece o direito fundamental à autodeterminação informativa. Desse último caso, o eminente Ministro Luiz Fux ainda destaca que a decisão culminou na declaração de inconstitucionalidade parcial da norma em razão de sua vagueza e amplitude, considerados os riscos do cruzamento dos dados coletados com outros já existentes (de forma similar ao caso em tela). Afirma que essa decisão reconhece a relevância fundamental da autodeterminação do indivíduo quanto aos seus dados como instrumento do livre desenvolvimento de sua personalidade e cita parte da fundamentação da Corte alemã:

> "(...) Esse poder [do uso de dados] necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (...) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas" (MARTINS, 2005; In BRASIL, 2020).

Prosseguindo, cita os princípios da LGPD referentes ao tratamento de dados (art. 6º da LGPD) para listar as previsões legais mínimas obrigatórias sobre o tratamento de dados pessoais. Realizando o silogismo desses princípios com o caso concreto, conclui pela plena desconformidade da MPv com a Lei: não tem finalidade legítima, específica, explícita e informada, pois "não delimita (i) o objeto da estatística a ser produzida, (ii) a finalidade específica, (iii) a amplitude da pesquisa, ou (iv) a necessidade da disponibilização dos dados" (BRASIL, 2020); não segue a minimização dos dados por almejar tratamento de dados referentes a milhões de titulares quando pode atingir o mesmo resultado com dados de menos de cem mil titulares (conforme prática reiterada do próprio IBGE); não atende aos requisitos de segurança, pois "falha em determinar os padrões de segurança e de anonimização, a supervisão da comunicação e a autoridade responsável por fiscalizar o processo de compartilhamento" (BRASIL, 2020) e; não previne riscos por determinar que o relatório de impacto seja realizado *a posteriori*, ao invés de *a priori*. Nas palavras do eminente Ministro Luiz Fux, esse conjunto de deficiências cria grande preocupação, pois

> "dados como nome, endereço e telefone de todos os usuários de telefonia móvel e fixa, somados às entrevistas pessoais, podem gerar um nível preocupante de precisão na identificação dos usuários. (...) Com efeito, a necessidade de suspensão da eficácia da MPv 954/2020 não deriva da determinação do compartilhamento de dados *per se*, mas da ausência de especificação dos objetivos, métodos e procedimentos que envolvem esse compartilhamento. Faltou ao texto normativo a

> transparência e informação necessários para uma adequada composição e conciliação entre a necessidade de produção estatística e os direitos fundamentais à proteção de dados e à autodeterminação informativa" (BRASIL, 2020).

Também ressalta que, a LGPD (à época ainda em *vacatio legis*) dispensa o consentimento para o tratamento de dados pessoais voltados à execução de políticas públicas (LGPD, art. 7º, III), mas não dispensa a observância dos princípios atribuídos ao tratamento de dados pelo art. 6º da LGPD (LGPD, art. 26, *caput*). Também alerta para o perigo da normalização da supressão de direitos em tempos de crise, citando o jurista estadunidense Daniel Solove:

> "Sacrifícios de direitos e liberdades civis devem ser feitos somente quando o governo justifica adequadamente por que esses sacrifícios são necessários. É preciso submeter tais restrições a um escrutínio meticuloso, especialmente porque, em tempos de crise, o medo distorce nosso julgamento. (...) devemos ser extremamente cautelosos ao fazer sacrifícios desnecessários" (SOLOVE, 2011 *In*: BRASIL, 2020).

Concluindo seu voto, o eminente Ministro Luiz Fux reconhece a existência de *fumus boni juris* e de *periculum in mora*, tendo em vista o dano à privacidade intrínseco pela transferência de dados ao IBGE e encerra seu voto nos seguintes termos:

> "*Ex positis*, referendo a decisão cautelar proferida pela Ministra relatora Rosa Weber, para suspender a eficácia da Medida Provisória 954/2020, cujo teor viola os direitos fundamentais à proteção de dados e à autodeterminação informativa, extraídos da garantia da inviolabilidade da intimidade e vida privada (art. 5º, X, CF/88), do princípio da dignidade da pessoa humana (art. 1º, III, CF/88) e da garantia processual do habeas data (art. 5º, LXXII, CF/88), bem como da proporcionalidade, notadamente nas vertentes adequação e necessidade" (BRASIL, 2020)

O eminente Ministro Ricardo Lewandowski, de princípio, apresenta interessante reflexão:

> "Penso que o maior perigo para a Democracia nos dias atuais não é mais representado por golpes de Estado tradicionais, perpetrados com fuzis, tanques ou

> canhões, mas pelo progressivo controle da vida privada dos cidadãos, levado a efeito por governos de distintos matizes ideológicos, mediante a coleta massiva e indiscriminada de informações pessoais, incluindo, de maneira crescente, o reconhecimento facial. E esses dados são submetidos ao novo instrumental da tecnologia de informações denominado *big data*, que consegue armazenar, interligar e manipular uma enorme quantidade de dados, para o bem ou para o mal" (BRASIL, 2020).

De forma clara, o Ministro demonstra a inequívoca a relação entre dados pessoais e democracia, isto é, como condição *sine qua non* ou fundamento do Estado democrático de Direito (o que pode ser entendido como direito fundamental intrínseco). Da mesma forma que nos votos anteriores, também aborda as previsões da LGPD quanto à minimização dos dados e finalidade, assim como a decisão do Tribunal Constitucional Alemão sobre a Lei do Censo de 1983. Acrescenta à lista de elementos do direito comparado a Convenção 108 do Conselho da Europa (sobre tratamento automatizado de dados, destacando a previsão de imprescindibilidade de sua proteção) e o *Freedom of Information Act*, dos EUA (de conteúdo similar ao do instituto brasileiro do *Habeas Data*). Concorda com os votos dos demais Ministros quanto ao atribuir à MPv "extrema vagueza e indeterminação quanto a seus limites" (BRASIL, 2020). Enfatiza que a relação entre indivíduo e Estado é vertical e desigual, sendo necessário impor limites aos poderes públicos, tal como no caso em tela. De forma ilustrativa, o eminente Ministro os temas 990 e 225 (RE 1.055.941/SP-RG; RE 601.314/SP-RG), que reconhecem a constitucionalidade do compartilhamento de dados bancários e fiscais para autoridade administrativa sem autorização judicial. Cabe ressaltar que as teses fixadas pelos dois temas citados pelo eminente Ministro preveem alguns requisitos e condições específicas:

> "O compartilhamento pela UIF e pela RFB (...) deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios" (STF, Tese 990).

> "O art. 6º da Lei Complementar 105/01 não ofende ao direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o translado do dever de sigilo da esfera bancária para a fiscal" (STF, tema 225).

Ricardo Lewandowski também destaca que o dado pessoal referente ao número da linha telefônica móvel usada pelo titular tem valor que transcende seu significado *de per se*. Esse número, corriqueiramente também é usado como "chave de identificação e de acesso a um universo de plataformas eletrônicas, como bancos, supermercados, (...), todas elas detentoras das mais variadas informações sobre o titular daquela linha telefônica" (BRASIL, 2020). Complementa que essa miríade de possibilidades é um risco concreto, especialmente devido ao *big data*. Em contraste, enfatiza a relevância da atuação do IBGE para identificar "os potenciais e as carências dos diversos setores da sociedade, coletando dados que servirão de base para a elaboração das políticas públicas voltadas ao desenvolvimento nacional e à melhoria da qualidade de vida dos brasileiros" (BRASIL, 2020). Por outro lado, assevera que a mesma lei que criou o IBGE (Lei 5.878/73) também elenca a preservação do sigilo estatístico como uma das diretrizes de atuação do Instituto. Outrossim, assim como os demais Ministros, também reconhece a desproporcionalidade no uso dos dados de mais de duzentas milhões de pessoas físicas para a realização de pesquisas que costumam ser feitas por amostragem (cerca de 200 mil entrevistados para a PNAD Contínua, segundo a eminente Ministra Relatora Rosa Weber). O eminente Ministro Ricardo Lewandowski também concorda que a realização de relatório de impacto *a posteriori* é prejudicial, pois exclui a possibilidade de prevenção ao dano. O eminente Ministro conclui seu voto afirmando que a MPv afronta os direitos à privacidade, à autodeterminação informativa, à inviolabilidade e da intimidade dos consumidores, da defesa do consumidor, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania. Por fim, referenda integralmente a medida cautelar proferida pela eminente Ministra Relatora Rosa Weber.

DISCUSSÃO

A falsa simplicidade dos direitos fundamentais

Alexy opera verdadeira dissecção de um direito fundamental em quinze possíveis subcategorias, o que, por si só, já expressa a complexidade dessas normas. Porém, antes de submeter o direito fundamental à proteção de dados a esse método, é interessante abordar a análise de Möllers sobre a dignidade humana para esclarecer um aspecto prévio: a falsa simplicidade dos direitos fundamentais e o consequente risco de achatamento de seus conteúdos.

Möllers adota uma concepção do conceito de dignidade humana conforme determinado contexto histórico e político da democracia que, no recorte do autor, é a constituinte alemã e significa o "reconhecimento recíproco como razoáveis e abertos a deliberação" (MÖLLERS, 2009, tradução nossa). Em sequência, resgata o pensamento kantiano para afirmar que, assim como o imperativo categórico, a dignidade humana é um conceito indeterminado que depende do consenso dos intérpretes. Dessa forma, entende que o parlamento, como coletivo, consagra o indivíduo como ponto de partida da Constituição. Também destaca que a dignidade humana é tanto um requisito apenas da democracia quanto um requisito dos direitos fundamentais. Partindo de uma interpretação negativa, o autor entende que o único ato que atenta exclusivamente contra a dignidade humana é a tortura. Por meio dessa observação, entende que a dignidade humana pode ser entendida como o direito do indivíduo (1) a não ser reduzido a um corpo, (2) a não ser "mero objeto da causalidade", ou, de forma positiva (3) a usufruir da "habilidade de tomar decisões racionais e de ser livre" (MÖLLERS, 2009, tradução nossa). O autor também conceitua que a dignidade humana pode ser compreendida como o "direito a ter direitos", mas que também deve ser entendida como o "direito a receber justificativas", de forma a fortalecer a autodeterminação do indivíduo, por garantir maior grau de racionalidade às suas decisões. De forma a exemplificar a aplicação desse entendimento, critica o Tribunal Constitucional Alemão por que declarar que a exclusão da obrigatoriedade de supervisão

judicial sobre escutas telefônicas não incide sobre aa dignidade humana (MÖLLERS, 2009). Consequentemente, percebe-se que o indivíduo tem a sua autodeterminação protegida pela dignidade humana. Por outro lado, entende que, uma vez que o indivíduo é o ponto de partida da Constituição, um atentado contra a dignidade humana também é uma ameaça à "integridade democrática da comunidade política" (MÖLLERS, 2009, tradução nossa), isto é, uma ameaça contra a coletividade e contra o Estado. Assim, afastamos interpretações levianas de que a dignidade humana faz referencia a determinado grau de qualidade de vida (o que não está errado, mas é impreciso) e delimitamos esse tão controverso direito como o direito a tomar decisões por si mesmo.

Conceitos elementares e construções jurídicas

R. Alexy divide os tipos de direitos fundamentais conforme o seu objeto, categorizando-os como direito a algo, liberdades e competências. Apesar dessa divisão, os direitos a algo tem especial relevância dentro da teoria de Alexy, uma vez que apresentarem unidades básicas conforme as quais são definidas a liberdade e a competência. O direito a algo é dividido em dois grandes grupos: direitos a ações negativas (direitos de defesa) e direitos a ações positivas (direitos a prestações). Aprofundando o direito de defesa, inicialmente se destaca que o titular do direito é indeterminado (pessoa física ou jurídica) e o destinatário desse direito sempre é o Estado. O autor subdivide o direito a algo em três grupos, sendo o primeiro deles o "direito ao não-embaraço". O "embaraço" ao qual se refere é a criação de obstáculos à efetivação do direito, que podem variar quanto à sua natureza (fáticos ou institucionais/ jurídicos) e quanto à sua intensidade (transponíveis ou intransponíveis). Ressalta-se que o objeto desse direito é a condição de liberdade de uma ação do indivíduo, como por exemplo, a liberdade de ir e vir, que pode ser limitada conforme as hipóteses suscitadas. Essa categoria de direito de defesa não foi observada nos casos em análise e inexiste no âmbito da proteção de dados pessoais, mas cabe ressaltar por sua existência no âmbito do direito digital dentro do MCI. Como suscitado por Bodin e Teffé, a neutralidade da rede e a liberdade de expressão são parte do tripé axiológico do MCI e sua violação se manifesta pela censura na internet. A título de exemplo, pode ser

citado o "*Golden Shield Project*", que existe na China desde 1998 e é uma política pública de controle do conteúdo da internet acessível a seus cidadãos (CHAN *et al*, 2011).

O segundo deles, "o direito à não-afetação de características e situações do indivíduo" é a proteção a características do indivíduo e a estados ou situações dele. Alexy exemplifica-os pelo direito a viver e a ser saudável (característica) e pela inviolabilidade do domicílio (situação). Destaca-se, por outro lado, que a ausência de um direito à não-afetação enseja um dever de tolerância do titular para com a intervenção ou limitação do direito específico em questão. Este é encontrado na ADI 6.387, que, por meio dos votos abordados, apresenta como a moldura jurídica posta pela LGPD é imprescindível para garantir que o tratamento de dados pessoais seja realizado de forma a respeitar a privacidade do titular de dados (situação protegida).

Por fim, o terceiro deles é o "direito à não-eliminação de posições jurídicas". Esse direito tem em sua essência três esferas de normas que são protegidas como um sistema uno: normas sobre a constituição da posição, normas sobre sua desconstituição e normas sobre as consequências da situação jurídica. O autor exemplifica pelo direito à propriedade, que tem sua constituição pela aquisição, sua desconstituição pela alienação e suas consequências pelos poderes de domínio (uso, fruição e disposição). Alexy também afirma que de forma geral, todo direito positivado também tem um direito implícito à não-afetação, pois constitui uma posição jurídica válida (ALEXY, 2015). Portanto, este direito de defesa também é um aspecto do direito à proteção de dados pessoais, uma vez que o art. 5º, X da CRFB positiva a necessidade da existência de normas sobre a proteção de dados pessoais, de forma a garantir maior estabilidade às normas de constituição, desconstituição e consequências jurídicas dos dados pessoais que constam na LGPD.

Concluída a análise do direito de defesa, cabe observar o direito a prestações. Este é dividido por Alexy em dois grupos: direito a uma prestação fática e direito a uma prestação normativa. O primeiro deles é caracterizado pela irrelevância da forma jurídica pela qual a pretensão subjetiva é satisfeita, tendo como objetivo uma ação material do Estado. Já o segundo é o direito à produção legislativa voltada a assegurar, proteger ou trazer condições de efetivação de um direito. Alexy também destaca que dentre os direitos a prestações fáticas existem os direitos à proteção, que define como "direitos constitucionais a que o Estado configure e aplique a ordem jurídica de uma determinada maneira no que diz respeito à relação dos sujeitos de direito de mesma hierarquia entre si" (ALEXY, 2015). Essa diferenciação tem especial relevância ao tema, por pormenorizar e proteger diferentes direitos uma vez que passam a ser ter uma existência isolada. Inicialmente, os direitos a prestações fáticas em sentido estrito compõem o rol de aspectos do direito fundamental à proteção de dados pessoais pela necessidade de que os titulares de dados sejam conscientizados de seus direitos por meio de políticas públicas. Caso contrário, o desconhecimento desses direitos implica em situação análoga à do casoo Telekall: impossibilidade de seu exercício pela ausência de pressupostos básicos. Da mesma forma que o titular não consegue exercer seus direitos se não tem ciência da realização de tratamento de seus dados pessoais, também é incapaz desse exercício se sequer conhecer seus direitos. Assim, para que esse âmbito funcione de forma privada e com reduzida intervenção pública, é necessário garantir que os titulares tenham condições mínimas de se autodeterminar. Caso contrário, a tendência da ocorrência de lesões aos particulares e de judicialização e submissão à competência regulatória da ANPD tende a ser desnecessariamente maior.

O autor também destaca que o direito de proteção não deve ser confundido como um dever geral do Estado. Inserido no rol dos direitos fundamentais de 1ª Geração, frutos da teoria constitucional do contratualismo, o direito de proteção é um direito individual. Dessa forma, é exigível pelo indivíduo isolado, sem que seja necessária demonstração de ofensa à coletividade (ALEXY, 2015). Podemos observar o direito à proteção no caso Telekall, no qual, apesar do impulso inicial ser de uma instituição pública (Ministério Público), há uma intervenção do Estado na esfera privada em razão de uma violação da ordem jurídica. Sendo a atuação a ANPD ainda muito recente no Brasil, não foram observados casos de exercício do direito de proteção propriamente dito (como direito subjetivo). Ainda assim, é possível analisar como funciona esse

microssistema de proteção, do qual destacam-se, dentro de suas características, a relevância conferida à infração de obstrução da atividade fiscalizatória da ANPD e a regra de definição da multa conforme o dobro da vantagem auferida ou pretendida.

Prosseguindo para o direito a organização e procedimento, incialmente, o autor aborda a existência dos dois elementos que formam o grupo. O primeiro deles é a organização, ou seja, o direito a normas procedimentais que estruturam organizações e que vincula o legislador. Já o direito a procedimentos, é aquele direcionado ao judiciário, que tem como papel instrumental na efetivação de um direito fundamental (ALEXY, 2015). Subdivide o direito a organização e procedimento em quatro aspectos: "(1) competências de direito privado; (2) procedimentos judiciais e administrativos (procedimento em sentido estrito); (3) organização em sentido estrito; e (4) formação da vontade estatal" (ALEXY, 2015).

O primeiro subgrupo, "competências de direito privado", trata dos clássicos institutos jurídicos (matrimônio, propriedade privada e outros), tendo sua relevância como direito subjetivo fundamental justificada pelo fato de que, apenas com base na existência desses institutos é que os direitos fundamentais correspondentes se tornam possíveis (ALEXY, 2015). Em síntese, não há como se falar em direito à propriedade privada se as modificações de seus status (aquisição e alienação, em especial) não forem permitidas. Mais do que isso, se existe um dever do Estado de preservação da propriedade privada, também há um dever de preservação das normas (de competência) que garantem a existência jurídica da propriedade privada em si. Esse âmbito é possivelmente um dos mais ricos no âmbito do direito À proteção de dados pessoais, pois, na esteira da discussão suscitada por Schreiber ao abordar o *notice and take down*, no âmbito do MCI, a LGPD tem um claro intuito de desjudicializar (ou extrajudicializar) conflitos atuais e que tendem a multiplicar-se. Isso ocorre pois, ao serem definidas competências de direito privado, é estipulada uma moldura jurídica para as relações privadas, de forma que essa segurança jurídica torne mais interessante que conflitos sejam resolvidos *inter partes* do que em onerosos e demorados processos judiciais.

Quanto ao segundo subgrupo, o autor ressalta que o "direito a procedimento em sentido estrito" tem relevância primordialmente procedimental, uma vez que a observância do procedimento não é o bastante para garantir a plena satisfação de determinado direito fundamental, devendo prevalecer sempre sua análise material (ALEXY, 2015). Este direito possuí uma natureza bivalente no âmbito da proteção de dados pessoais, pois, ainda que a LGPD disponha de regras gerais acerca do procedimento para que os titulares exerçam e assegurem seus direitos, são as normas infralegais da ANPD que vem a pormenorizar esse exercício. Dessa forma, configura-se a referida natureza bivalente: legal e infralegal, de forma que o art. 5º, X da CRFB é capaz de ensejar remédios constitucionais no âmbito da produção normativa da ANPD.

Já a organização em sentido estrito, terceiro subgrupo, é definida por Alexy como "direitos dos indivíduos a que o legislador crie normas de organização que sejam conformes aos direitos fundamentais" (ALEXY, 2015), diferenciando-se do direito negativo à não eliminação de posições jurídicas por também abranger deveres e proibições objetivos. Assim, enquanto ao se abordar a não-afetação foi restringida sua incidência sobre as normas de constituição, desconstituição e consequências jurídicas dos dados pessoais, no atual âmbito, há ampla proteção a todas as disposições da LGPD.

Quarto e último subgrupo trata do "direito à formação da vontade estatal" e versa sobre normas que garantam impacto da opinião individual sobre as decisões do Estado, incluindo desde o conjunto de regras que determina a legitimidade para o exercício do direito ao voto (sem confundir-se com o direito do voto em si) à própria liberdade de expressão (ALEXY, 2015). Observa-se que o que importa é a existência de alguma finalidade política da ação e cujo objetivo seja um impacto sobre o Estado (e não sobre a sociedade civil). Este pode ser observado no âmbito da proteção de dados pessoais por meio da obrigação de realização de consultas públicas por parte da ANPD antes de editar normas e regulamentos (LGPD, arts. 53 e 58), conforme já vem ocorrendo (por exemplo, quanto ao regulamento de dosimetria). Observa-se,

portanto, que os quatro aspectos do direito a procedimentos estão presentes no direito à proteção de dados pessoais, sem que sejam limitados aos exemplos empregados.

Estrutura do sistema jurídico e fundamentação no âmbito dos direitos fundamentais

Com relação à estrutura do sistema jurídico, Alexy inicialmente aborda o papel das normas de direitos fundamentais dentro do sistema jurídico. Considera que elas são formadas por dois fatores: fundamentalidade formal e fundamentalidade substancial. Explica que a fundamentalidade formal é a posição da norma na hierarquia jurídica, ocupando o ápice desta e vinculando os três poderes; por outro lado, a fundamentalidade substancial é definida pela caracterização dessas normas como "decisões sobre a estrutura normativa básica do Estado e da sociedade" (ALEXY, 2015). Assim, a fundamentalidade formal tem efeito sobre as outras normas e sobre o Estado ao determinar quais normas são válidas e quais são inválidas; já o aspecto substancial define o que é necessário e o que é vedado. Observa-se que, em certa medida, os dois elementos representam diferentes aspectos de um mesmo fenômeno (por exemplo, proibição substancial e invalidade formal significam o mesmo).

Com relação à fundamentalidade formal do direito à proteção de dados pessoais, tem destaque a discussão aventada no âmbito da EC 115. Nesse contexto, foi expressamente declarado que um dos objetivos da constitucionalização desse direito foi a garantia de maior segurança jurídica ao conferir uma posição privilegiada a esse direito dentro da hierarquia normativa. Para tanto, a fixação de competência legislativa federal exclusiva em âmbito constitucional tem destaque. Já no que tange à fundamentalidade substancial, é a inclusão desse direito no rol do art. 5º da CRFB que tem relevância central. Nessa seara, a Ministra Rosa Weber e o Ministro Luis Roberto Barroso abordaram diretamente esse tema, apontando que a coleta

de dados pessoais sem limitações legais pode levar a um nível de vigilantismo tão intenso que afete outros direitos fundamentais e, em última instância, seja a derrocada da democracia.

Em sequência, o autor passa a dissertar sobre um dos temas pelo qual mais é reconhecido, o efeito horizontal dos direitos fundamentais. Inicialmente, afirma que o sistema jurídico pode ser observado tanto como um sistema de normas quanto como um sistema de posições e relações jurídicas. Afirma que a primeira caracterização enfatiza a aplicação universal da norma e que a segunda destaca a diferenciação, pois, além de definirem direitos subjetivos em face do Estado, os direitos fundamentais também abrangem "direitos a proteção contra outros cidadãos e a determinados conteúdos da ordem jurídico-civil" (ALEXY, 2015). Também destaca que, por essas razões, os direitos fundamentais também influenciam o direito civil, uma vez que vinculam o poder judiciário e, portanto, impõem limites às sentenças proferidas. Dessa forma, demonstra como, além de influenciarem as relações entre o cidadão e o Estado, também influenciam as relações entre cidadãos. Alexy destaca que além de consubstanciarem-se em direitos subjetivos, os direitos fundamentais também firmam uma "ordem objetiva de valores" (ALEXY, 2015). Explica que os "valores" são os princípios; que a "ordem" significa que os princípios devem "produzir efeitos substanciais abrangentes em todas as posições do sistema jurídico" (ALEXY, 2015); e que o caráter objetivo se dá pela síntese de cada princípio em um "simples dever-ser" (ALEXY, 2015), abstraído de especificidades, isto é, uma ordem de "princípios de nível máximo de abstração" (ALEXY, 2015). O autor também ressalta que essa forma resulta em um alto grau de indeterminação e que, por essa razão, os princípios não devem ser usados como ponto de partida da fundamentação jurídica, mas apenas como meio para a escolha e justificação de premissas mais precisas. Dessa forma, os princípios passam a fomentar a racionalidade da fundamentação jurídica, ao invés de incentivar "uma das formas mais obscuras de fundamentação jurídica, a "dedução" ou "derivação" de conteúdos concretos a partir de princípios abstratos" (ALEXY, 2015).

Aprofundando a discussão do efeito horizontal, Alexy aponta diferenças entre a relação cidadão/Estado e cidadão/cidadão. Enquanto na primeira, apenas um dos polos é titular de

direitos fundamentais, na segunda, ambos os polos o são. Considerando isto, o autor afirma que, no segundo caso, existem dois paradigmas quanto aos direitos fundamentais: a construção (como produz efeitos) e a colisão (extensão dos efeitos). Para trazer mais densidade à concepção de "efeito irradiador", Alexy, inicialmente, apresenta sua teoria de três níveis sobre o problema da construção. Os níveis são "o do dever estatal, o dos direitos em face do Estado e o das relações jurídicas entre os sujeitos privados" (ALEXY, 2015). Em síntese, o primeiro nível trata dos efeitos dos direitos fundamentais perante a legislação infraconstitucional; o segundo nível, da prestação jurisdicional respeitar seus direitos fundamentais; e o terceiro nível, do respeito de terceiros pelos direitos fundamentais do indivíduo (ALEXY, 2015). Alexy ainda indica três consequências dessa teoria: (1) que o conteúdo substancial dos direitos fundamentais limita os "possíveis conteúdos do direito ordinário" (ALEXY, 2015); (2) que levam a um sistema jurídico aberto, uma vez que a aplicação dos direitos fundamentais depende de um sopesamento; e (3) que é "um sistema aberto em face da Moral" (ALEXY, 2015), uma vez que conceitos básicos como dignidade, liberdade e igualdade são conceitos filosóficos (ALEXY, 2015). Dessa forma, no âmbito do direito fundamental à proteção de dados pessoais, podemos observar como o STF, em controle de constitucionalidade concentrado, não só declara a inconstitucionalidade de norma infraconstitucional com base em direito fundamental implícito (positivado pela EC 115), mas também indica que os parâmetros para o sopesamento são as previsões da LGPD. Assim, observam-se tanto o primeiro nível, com a limitação do direito ordinário, quanto o segundo nível, pela prestação jurisdicional conforme aos direitos fundamentais. Já o terceiro nível, é observado pela prévia discussão sobre o dever geral do Estado de proteção dos direitos individuais e como o caso Telekall exemplifica esse aspecto.

Quanto ao problema da colisão, isto é, a extensão dos efeitos dos direitos fundamentais, é interessante abordar a teoria de Alexy acerca das restrições. Alexy aborda duas teorias a respeito do tema: a externa e a interna. A teoria externa supõe que os direitos fundamentais são plenos em sua essência e que, a partir de uma exigência (elemento externo) passam a ser forçadamente limitados. A teoria interna, por vez, traz uma visão de unicidade, segundo a qual, ao invés de restrições, os direitos fundamentais têm um conteúdo próprio que determina limites. A questão, portanto, deixa de ser a amplitude das restrições e passa a ser o alcance do próprio conteúdo dos direitos, isto é, suas "restrições imanentes". Contrapondo as duas teorias, o autor aponta que elas podem ser relacionadas à conceituação dos direitos fundamentais, de forma que

regras possuem limites predeterminados e princípios possuem uma abertura hermenêutica intrínseca. Enfatiza, de toda forma, que o direito fundamental não é restringido por outro, ao invés disso, é restringido pelas normas oriundas da lei de colisão (ALEXY, 2015). Nessa esteira é interessante observar que vêm se desenvolvendo um microssistema de proteção de dados pessoais na legislação, de forma que o direito fundamental existe principalmente em prol da constitucionalidade formal e, substancialmente, como mero direito cujo objeto é a própria legislação (direito à não-eliminação de posições jurídicas, direito a competências de direito privado, direito a procedimentos e direito à organização em sentido estrito). Por outro lado, é a legislação infraconstitucional (LGPD, futuras normas sobre dados pessoais e regulamentos da ANPD) que vêm a determinar os limites materiais do direito fundamental.

Oportuna reflexão feita por Alexy é aquela sobre a colisão de direitos amplos, como a liberdade geral. Ao abordar esse tema, o autor conceitua a dignidade humana de forma a estabelecer uma relação íntima entre esta e a privacidade, o que faz com que o tema ganhe especial relevância no contexto da proteção de dados pessoais. Entende que a dignidade humana é um feixe de condições, de forma que:

> "A dignidade humana está 'baseada na compreensão do ser humano como um ser intelectual e moral, capaz de se determinar e de se desenvolver em liberdade'. A Constituição alemã não concebe essa liberdade como a liberdade de um indivíduo isolado e autocrático, mas como um indivíduo relacionado a uma comunidade e a ela vinculado" (ALEXY, 2015).

> "trata-se de uma liberdade exterior, que consiste na inexistência de coerção exterior sobre o indivíduo na sua escolha entre determinadas alternativas de decisão, pois, em um contexto jurídico, não seria possível falar em 'independência da pessoa' e em 'personalidade auto-responsável' em qualquer outro sentido. Mas uma tal liberdade sempre inclui a liberdade jurídica negativa. É possível, então, afirmar que sem a liberdade jurídica negativa não há dignidade humana em um sentido juridicamente relevante" (ALEXY, 2015).

Em sequência, o autor discute a teoria das esferas e a teoria dos direitos de liberdade implícitos para traçar um conceito material de liberdade. Afirma que o desenvolvimento da

teoria pelo Tribunal Constitucional Alemão considera três níveis: em seu núcleo está a esfera privada, referente ao "último e inviolável âmbito de liberdade humana"; em um nível intermediário, a "esfera privada ampliada"; e, em uma esfera mais externa, a "esfera social" (ALEXY, 2015). O autor explica que a esfera privada é marcada pela impossibilidade da aplicação da regra do sopesamento quando do conflito com outro direito fundamental, por serem direitos absolutos, como a vida ou a vedação à tortura. Em uma segunda escala, a esfera privada ampliada é marcada pela estrita proporcionalidade: a necessidade de "razões especialmente relevantes" (ALEXY, 2015). Por fim, sem que comente a esfera social, apresenta crítica à Teoria das Esferas, com base em dois argumentos. O primeiro deles é que, a intensidade da afetação também é relevante, de forma que uma afetação intensa da esfera social pode ser mais prejudicial do que uma afetação mínima da esfera privada ampliada. O segundo argumento versa sobre a dificuldade em delimitar cada uma das esferas, em especial a esfera privada ampliada e a social, uma vez que "entre o mais privado e aquilo que não tem nada de privado existe uma transição gradual" (ALEXY, 2015). Por outro lado, também ressalta um aspecto positivo da teoria:

> "o que a diferenciação entre esferas privada e social corretamente põe em destaque é o fato de que a proteção a direitos fundamentais deve ser tão maior quanto maior for o peso dos princípios protetores da privacidade que estejam aliados ao princípio da liberdade geral de ação" (ALEXY, 2015).

A discussão acerca da aplicação da teoria das esferas no âmbito da dignidade humana traça uma clara relação com as categorias de dados pessoais. Tal qual nessa teoria, existem três tipos básicos de dados considerados pela LGPD: dados comuns, dados pessoais e dados pessoais sensíveis. São possíveis outros arranjos, mas o interessante é observar que as fronteiras entre a caracterização dos dados como de um tipo ou de outro também tem grande fluidez. Afinal, como já foi abordado, dados comuns (por exemplo, dados anonimizados) podem ser processados junto a outros dados comuns de forma a que o resultado do tratamento seja um dado pessoal. Por sua vez, dados pessoais podem ser tratados junto com outros dados e ter como resultado dados pessoais sensíveis. Portanto, dados comuns e dados pessoais devem ser tratados com cautela, uma vez que, como ensina Alexy ao abordar a teoria das esferas, o mais relevante é o grau de afetação do direito do titular e a proporcionalidade entre direito e o tratamento. Tal

ocorre pois, como prescrito pela LGPD, até dados pessoais sensíveis podem ser tratados sem consentimento a depender da finalidade do tratamento.

Nesse ponto também é interessante realizar digressão para destacar que Alexy, em uma teoria geral dos direitos fundamentais reconhece relevância primordial da privacidade para uma adequada compreensão da dignidade humana. Se Möllers, por um lado fala em tortura para justificar que a dignidade humana é o direito "de tomar decisões racionais e ser livre" (MÖLLERS, 2009, tradução nossa) e de não ser reduzido a um corpo; Alexy, por outro lado, trabalha com o conceito de liberdade negativa como direito a alternativas de ações para atingir uma finalidade. Em ambos os casos, o conceito de privacidade existe como a determinação do "eu", ou seja, como a separação das vontades e pensamentos individuais daqueles do coletivo ou de terceiros (o que ocorre com a tortura). Da mesma forma, quando Möllers entende que a dignidade humana também significa um "direito a receber justificativas" (MÖLLERS, 2009, tradução nossa), Alexy afirma que o sopesamento de direitos fundamentais que compõem alguma das esferas da dignidade humana requer uma estrita proporcionalidade. Dessa forma, há uma remissão à privacidade como pressuposto da racionalidade, pois, não há objetivo em uma fundamentação proporcional da dignidade humana se o indivíduo sequer pode se autodeterminar. Por outro lado, a afetação infundada da dignidade humana também debilita a autodeterminação por meio da intimidação.

Por fim, quanto à fundamentação no âmbito dos direitos fundamentais, enfim cabe abordar os conceitos de liberdade e de competências conforme Alexy. Primeiramente, o conceito de liberdade, para o autor, é formado por três elementos: (1) a pessoa que não é livre; (2) o obstáculo à sua liberdade e (3) o embaraço ou impedimento posto pelo obstáculo. Dessa forma, o conceito abrange todos os fatores colaterais que podem privar alguém de uma faculdade, isto é o direito de agir ou de não agir (ALEXY, 2015). Com base nos três elementos que compõem a liberdade, Alexy afirma que a liberdade geral do indivíduo é o conjunto de suas liberdades específicas e que a liberdade de uma sociedade é a soma da liberdade de seus membros. O autor vai além e afirma que a verdadeira liberdade jurídica é a liberdade negativa, por ser a única que garante alternativas de ação (ALEXY, 2015). Assim, destaca a disponibilidade de alternativas para uma ação como elemento essencial ao invés da simples permissão de agir. Nesse sentido, a concepção do direito à proteção de dados pessoais como um

direito fundamental complexo ganha maior relevância para destacar que não trata-se de um mero "não-embaraço", mas de uma efetiva liberdade específica que compõem a liberdade geral de cada indivíduo e a liberdade de uma sociedade. Dessa forma, está exposto, de forma resumida a concepção do direito à proteção de dados pessoais como um dos fundamentos do Estado Democrático de Direito. O conjunto de deveres de abstenção e de agir (fático e legislativo) do Estado transcende a existência de meros direitos subjetivos, determinando uma ordem objetiva de valores com base no direcionamento do agir estatal pelos três poderes. No âmbito executivo, por deveres gerais do Estado; no âmbito legislativo, pelo direito à organização em sentido estrito e, no âmbito judiciário, pelo efeito horizontal dos direitos fundamentais.

Prosseguindo à competência, inicialmente, o autor apresenta dois conceitos de "competência", que podem ser aglutinados em um único: a faculdade de, validamente, criar normas individuais e gerais, assim como de alterar posições jurídicas de sujeitos submetidos a essas normas (ALEXY, 2015). Em suma, a competência é composta de um procedimento e de uma moldura legal para que o particular crie normas ou altere situações jurídicas conforme sua vontade. Alexy afirma que, conforme apresentado no caso das outras relações, também é possível chegar à relação conversa (complementar) da competência: a sujeição (ALEXY, 2015). Se "a" tem competência para alterar a situação jurídica de "b", então "b" tem uma relação de sujeição com "a". Dessas duas relações também podem ser deduzidas duas mais, suas negações: a não-competência e a não-sujeição ("a" não tem competência para alterar a situação de "b"; "b" não tem relação de sujeição com "a"). Em sentido material, o autor resgata Jellinek para afirmar que a competência jurídica aumenta a capacidade de ação do indivíduo a um nível superior que o que lhe é natural. Mais do que mero acréscimo, a competência também é um pressuposto conceitual para a liberdade de realizar um ato jurídico, pois sua redução ou não reconhecimento implica na obstacularização do fim (ALEXY, 2015). Destaca, por fim, que a competência é a forma mais ampla de liberdade jurídica, por ser a única que garante alternativas de ação ao indivíduo em acréscimo às ações diretamente protegidas. Conclui ressaltando a relevância do correto reconhecimento de direitos constitucionais, pois, sempre que se declara uma competência, também são declaradas obrigações, não-direitos e não-competências (ALEXY, 2015). Portanto, a relação entre liberdade e competência, para Alexy, é de expansão. Conforme o contratualismo kantiano, o indivíduo renuncia à sua liberdade do estado natural

para assumir o estado civil pois, se passam a existir normas que lhe impõem limites, estas são o reflexo de sua própria autonomia. Por outro lado, apesar de abandonar totalmente sua liberdade natural, o indivíduo adquire um novo tipo de liberdade, que não apenas é fruto de sua autonomia, mas que também é mais ampla por contar com a segurança jurídica, que inexiste no estado de natureza (QUINTANA, 2014). O aspecto de competência do direito à proteção de dados pessoais decerto não é o primeiro que se pensa ao abordar o tema, todavia, foi suscitado por diversas vezes ao longo da pesquisa: nas discussões da EC 115 e na ADI 6.387, em especial, é enfatizado que a conectividade das redes criou um vibrante paradigma socioeconômico cuja fruição segura e pacífica é o objetivo último do direito à proteção de dados pessoais.

CONCLUSÕES

A presente pesquisa teve como propósito expor de que forma o direito à proteção de dados pessoais, mais do que mero direito subjetivo e do que um direito fundamental, também é verdadeiro fundamento do Estado Democrático de Direito contemporâneo. Para esse propósito, foi definido como objetivo específico a aplicação da teoria geral dos direitos fundamentais de Robert Alexy a esse direito fundamental, levando à sua dissecção em dimensão empírica, normativa e analítica.

Ao longo da dimensão empírica, em um primeiro momento, foram observadas normas relacionadas à proteção de dados pessoais, com destaque para a própria Lei Geral de Proteção de Dados Pessoais, analisada de forma mais minuciosa. Também foi analisado o trâmite da EC 115, de forma a expor a vontade do legislador ao discutir o Projeto de Emenda Constitucional ao longo das duas Casas do Congresso Nacional. Nesse âmbito, ressaltou-se, principalmente a preocupação em garantir maior segurança jurídica a esse fenômeno, tanto no âmbito formal, pela competência legislativa exclusiva da União, quanto no âmbito material, por garantir status constitucional a esse direito. Por fim, nessa dimensão também foram abordadas considerações materiais da proteção de dados pessoais, contextualizando problemas contemporâneos, como o uso da inteligência artificial na segurança pública e a falibilidade da tecnologia e dos métodos de identificação.

Adentrando a dimensão normativa, foram observados os juízos de valores de dois núcleos decisórios centrais à proteção de dados pessoais: a ANPD, como agência reguladora da área, e o STF, como corte constitucional. No âmbito da ANPD, foram estudados os contornos infralegais (regulamentares) da tutela de dados pessoais, por meio da análise do primeiro processo sancionador da agência, com destaque para duas ferramentas de dissuasão dela: a configuração da obstrução à sua atividade fiscalizatória como infração grave e a definição do *quantum* da multa como o dobro da vantagem pretendida ou auferida. Já a ADI 6.387, ilustra

como a Corte Constitucional pondera um conflito envolvendo a proteção de dados pessoais, que *in casu*, colide com o direito à eficiência e racionalidade da prestação estatal (finalidade das pesquisas censitárias).

Progredindo à dimensão analítica, enfim são aplicadas categorias de Alexy ao direito fundamental à proteção de dados pessoais. Inicialmente, pela perspectiva dos conceitos elementares e construções jurídicas, foi possível verificar que trata-se de um direito fundamental complexo, composto, parcialmente, pelos direitos de defesa (não-afetação e não-eliminação) e pelos direitos a prestações fáticas e normativas *in totum.* Progredindo à estrutura do sistema jurídico e à fundamentação no âmbito dos direitos fundamentais, é apresentada a teoria de Alexy acerca do efeito irradiador, assim como suas concepções de liberdade e de competência. Quanto à primeira, é resumida a uma ordem objetiva de valores, que vincula direitos subjetivos a deveres objetivos do Estado, materializados pelos supracitados aspectos do direito fundamental à proteção de dados pessoais. Por fim, ao aplicar o conceito de competência de Alexy, é ressaltado o papel da segurança jurídica como aporte para a liberdade e para a autodeterminação dos indivíduos que compõem a sociedade.

Dessa forma, resta claro que o acentuado peso valorativo do direito à proteção de dados pessoais deve ser considerado ao ser submetido ao método do sopesamento quando em conflito com outros direitos fundamentais, sob risco de afetar a liberdade e a autodeterminação dos indivíduos e, inclusive, atentar contra o próprio Estado Democrático de Direito. Para esse objetivo, é importante ter clareza quanto aos diversos aspectos desse direito fundamental, compreendendo, em especial, seu enquadramento e consequências jurídicas. De toda forma, a proporcionalidade e a racionalidade, de forma geral, sempre terão papel central sempre que este ou qualquer outro direito fundamental encontrar-se em conflito com outra norma.

REFERENCIAS BIBLIOGRÁFICAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. 2. ed. São Paulo: Malheiros, 2015.

BAHIA, Andreia. Brasileiras que estavam presas na Alemanha após troca de malas voltam ao Brasil. **CNN Brasil**, São Paulo, 14 de abril de 2023. Disponível em: <https://www.cnnbrasil.com.br/nacional/brasileiras-que-estavam-presas-na-alemanha-apos-troca-de-malas-voltam-ao-brasil/>. Acesso em: 23/06/2023.

BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. São Paulo: RT, 1998. *In*: DONEDA, Danilo Cesar Maganhoto **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BARROSO, Luis Roberto. **Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010.

BERGHEL, Hal. Malice Domestic: **The Cambridge Analytica Dystopia. Computer**, EUA, 51, p. 84-89, maio, 2018.

BIONI, Bruno *et al* (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

BRASIL, Agência Nacional de Proteção de Dados (Coordenação Geral de Fiscalização), **Relatório de instrução Nº 1/2023/CGF/ANPD**. Brasília: ANPD, 2023a. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf>. Acesso em 04/08/2023.

BRASIL, Agência Nacional de Proteção de Dados, **Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023**. Brasília: ANPD, 2023b. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077>. Acesso em 04/08/2023.

BRASIL, Câmara dos Deputados Federais. **Parecer do Relator, PRL 1 PEC01719**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Câmara dos Deputados Federais, 2019d.

Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1841176&filename=Tramitacao-PEC%2017/2019>. Acesso em 04/08/2023.

BRASIL, Senado Federal. **Parecer s/n, de 2019**. Parecer da Comissão de Constituição, Justiça e Cidadania, sobre a Proposta de Emenda à Constituição nº 17, de 2019, do Senador Eduardo Gomes e outros, que acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal, 2019b. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7954439&ts=1647518557730&disposition=inline&_gl=1*16jniv3*_ga*NTA4MjI1MDg3LjE2NTI2NjE0Njc.*_ga_CW3ZH25XMK*MTY5Njk1ODkzMS4yLjEuMTY5Njk1OTQxOC4wLjAuMA..>. Acesso em: 04/08/2023.

BRASIL, Senado Federal. **Parecer s/n, de 2019**. Parecer da Comissão de Constituição, Justiça e Cidadania, sobre a Proposta de Emenda à Constituição nº 17, de 2019, do Senador Eduardo Gomes e outros, que acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal, 2019c. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7956536&ts=1647518557553&disposition=inline&_gl=1*7eztlu*_ga*NTA4MjI1MDg3LjE2NTI2NjE0Njc.*_ga_CW3ZH25XMK*MTY5Njk1ODkzMS4yLjEuMTY5Njk1OTQxOC4wLjAuMA..>. Acesso em: 04/08/2023.

BRASIL, Superior Tribunal de Justiça (6. Turma). ***Habeas Corpus* 639.792/RS**. Habeas Corpus. Homicídio qualificado. Reconhecimento fotográfico de pessoa realizado na fase do inquérito policial. Inobservância do procedimento previsto no art. 226 do CPP. Reconhecimento presencial. Acusado sozinho na cela. Provas inválidas como fundamento para a pronúncia. Rigor probatório. Necessidade para evitar erros judiciários. Ordem concedida. Impetrante: Matheus Gonçalves dos Santos Trindade. Impetrado: Tribunal de Justiça do Estado do Rio Grande do Sul. Relator: Min. Rogerio Chietti Cruz, 23 de março de 2021. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100106699&dt_publicacao=23/03/2021>. Acesso em 23/08/2023.

BRASIL, Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade 6.387/DF**. Medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida

provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. *Fumus boni juris*. *Periculum in mora*. Deferimento. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relatora: Min. Rosa Weber, 07 de maio de 2020. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em 23/08/2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD**. Brasília: Congresso Nacional, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em 04/08/2023.

BRASIL. Senado Federal. **Projeto de Emenda à Constituição nº 17, de 12 de março de 2019**. Acrescenta o inciso X/1-A, ao art. 5o e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal, 2019a. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1647518557279&disposition=inline&_gl=1*14tkw9a*_ga*NTA4MjI1MDg3LjE2NTI2NjE0Njc.*_ga_CW3ZH25XMK*MTY5Njk1ODkzMS4yLjAuMTY5Njk1ODkzMS4wLjAuMA..>. Acesso em: 04/08/2023.

Campanha Tire Meu Rosto da Sua Mira. Mini guia para juristas sobre o uso de tecnologias de reconhecimento facial na segurança pública. **Coalizão Direitos na Rede**: 2022.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. Fundamentos da constituição. Coimbra: Coimbra Editora, 1991. *In*: MORAES, Alexandre de. **Direito constitucional**. 34. ed. São Paulo: Atlas, 2018.

CHAN, Conrad *et al*. **Free speech vs Maintaining Social Cohesion**. Stanford CS181: Computers, Ethics and Public Policy Final Project. Stanford: 2011. Disponível em: <https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html>. Acesso em 04/08/2023.

CHAVES, João Guilherme Pereira; MIRANDA, João Irineu de Resende. Terror de Estado e Soberania: Um Relato sobre a Operação Condor. **Revista Internacional de História Política e Cultura Jurídica**, Rio de Janeiro, vol. 7, no. 3, p. 516-532, setembro-dezembro 2015.

CORRÊA, Alessandra. **ONU aprova resolução contra espionagem apresentada por Brasil e Alemanha. BBC**, Nova Iorque, 18 de dezembro de 2012. Disponível em: <https://www.bbc.com/portuguese/noticias/2013/12/131218_onu_espionagem_ac>. Acesso em: 24/06/2023.

DONEDA, Danilo Cesar Maganhoto **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

GARFINKEL, Simson. **Database Nation**: The Death of Privacy in the 21st Century. 1. ed. Sebastopol: O'Reilly, 2000.

LIMA, João Ademar de Andrade. **A base de dados como objeto de proteção de direito autoral**. Curitiba: Spei, 2004.

LONG, Clarissa; Privacy and Pandemics, 2020 *In*: BRASIL, Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade 6.387/DF**, *op cit*.

LUHN, Alec; HARDING, Luke; LEWIS, Travis. Edward Snowden asylum: US 'disappointed' by Russian decision. **The Guardian**. Londres, 1o de agosto de 2023. Disponível em: <https://www.theguardian.com/world/2013/aug/01/edward-snowden-asylum-us-disappointed>. Acesso em: 23/06/2023.

MALDONADO, Vivane Nóbrega; BLUM, Renato Ópice (coord.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão, 2005 *In*: BRASIL, Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade 6.387/DF**, *op cit*..

Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally. **Amnesty International**. Londres, 19 de julho de 2021. Disponível em: <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/>. Acesso em: 24/06/2023.

MITNICK, Kevin D.; SIMON, William L. **The art of Deception**: Controlling the Human Element of Security. 1. ed. Indianapolis: Wiley, 2002.

MÖLLERS, Cristoph. Democracy and Human Dignity: Limits of a Moralized Conception of Rights in German Constitutional Law. **Israel Law Review**, Cambridge, vol. 42, Issue 02, p. 416-439, January 2009.

MORAES, Alexandre de. **Direito constitucional**. 34. ed. São Paulo: Atlas, 2018.

QUADRAT, Samantha Viz. Operação Condor: o "Mercosul" do terror. **Estudos Ibero-Americanos**, Rio Grande do Sul, v. XXVIII, n. 1, p. 167-182, junho 2002.

QUINTANA, Fernando. **Ética e política**: da antiguidade clássica à contemporaneidade. São Paulo: Atlas, 2014.

Reino Unido. Information Comissioner's Office. **Penalty Notice** COM0804337. 30 de outubro de 2020. Disponível em: <https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf>.

Russia gives citizenship to ex-NSA contractor Edward Snowden. **AP News**. Nova Iorque, 26 de setembro de 2022. Disponível em: <https://apnews.com/article/edward-snowden-russian-citizenship-441ab3c037b91145d17f2de2237f834d>. Acesso em 23/06/2023.

SCHREIBER, Anderson. Marco Civil da Internet: Avanço ou Retrocesso? A responsabilidade civil por danos derivado do conteúdo gerado por terceiro. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. **Direito e Internet III**: Marco Civil da Internet, Lei nº 12.965/2014, Tomo II. São Paulo: Quartier Latin, 2015, p. 277-305.

SELTZER, William. ANDERSON, Margo. The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses. **Social Research**, Nova Iorque, vol. 68, no. 2, p. 481-513, Summer 2001.

SILVEIRA, Sergio Amadeu. Dados, algoritmos, desinformação e os riscos para a democracia. *In*: VIANNA, Manoela (org.). **A democracia aceita os termos e condições? Eleições 2022 e a política com os algoritmos**. Rio de Janeiro: Fundação Heinrich Böll, 2022.

SIMANOWITZ, Stefan. How the US pursuit of Julian Assange is a distractionfrom impunity for war crimes. **Amnesty International**. Londres, 26 de outubro de 2021. Disponível

em: <https://www.amnesty.org/en/latest/news/2021/10/how-the-us-pursuit-of-julian-assange-is-a-distraction-from-impunity-for-war-crimes/>. Acesso em: 23/06/2023.

SOLOVE, Daniel J. Nothing to hide: The false tradeoff between privacy and security. Yale University Press, 2011 *In*: BRASIL, Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade 6.387/DF**, *op cit*..

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

TEMER, Michel. Elementos de direito constitucional. 11. ed. São Paulo: Malheiros, 1995. *In*: MORAES, Alexandre de. **Direito constitucional**. 34. ed. São Paulo: Atlas, 2018.

Transcript of MarkZuckerberg's Senate hearing. **Washington Post**. Washington, 10 de abril de 2018. Disponível em:<https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/>. Acesso em: 24/06/2023.