REVISTA JURÍDICA DO BANCO DO NORDESTE

EDIÇÃO ESPECIAL

ISSN: 2236-8086
ISSN online: 2525-5312

Banco do Nordeste

REVISTA JURÍDICA
DO BANCO DO NORDESTE

Endereço para correspondência:
Superintendência Jurídica do Banco do Nordeste, Av. Dr. Silas Munguba, 5.700, bloco D1 superior, Passaré,
CEP: 60.743-902, Fortaleza, Ceará, Brasil.
Fone: (85) 3299.3085.
revistajuridica@bnb.gov.br

Revista Jurídica do Banco do Nordeste
V. 1, Ano 11, N. 6. Banco do Nordeste do Brasil S.A, Fortaleza – Ceará. Semestral
ISSN: 2236-8086
ISSN online: 2525-5312
N. de páginas: 358
1. Direito – Periódico 2. Doutrina 3. Jurisprudência 4. Atualização Legislativa
CDU – 34 (D05)

Depósito Legal junto a Biblioteca Nacional conforme a
Lei nº 10.994 de 14/12/2004

Sumário

EDITORIAL

Há 11 anos um grupo de advogados, apaixonados pelo estudo da ciência jurídica, resolveu materializar o sonho de criação da Revista Jurídica do Banco do Nordeste.

Compreendíamos, à época, que a iniciativa representaria um veículo qualificado para compartilhamento de conhecimento e espaço para debates de temas relevantes para a sociedade. Tal compreensão se consolidou ao longo dos anos, posicionando a Revista Jurídica do Banco do Nordeste como um periódico de referência para aqueles que amam a ciência e o livre circular de ideias e ideais.

Honrado pelo convite para escrever o presente Editorial, cuja ideia proposta foi de pronto aceita, não pelo fato de ter idealizado esta Edição Especial, mas, antes, pela oportunidade singular de abrandar a distância com a Superintendência Jurídica, imposta pelos afazeres cotidianos. Tamanha honra exigiu esforço e dedicação e, para tanto, busquei nos clássicos minha inspiração. Encontrei em Rui Barbosa fonte para iniciar este texto. Em sua indelével Oração aos Moços, há um século o jurista alertava os jovens bacharéis, recém-formados no Largo do São Francisco, que *ninguém que empreenda uma jornada extraordinária, primeiro que meta o pé na estrada se esquecerá de entrar em conta com suas forças, para saber se a levarão ao cabo.*

De fato, colocar em prática uma ideia, quanto mais se esta for extraordinária, exige do idealizador consultar se possui as forças necessárias para concretizar o projeto. Antecipo aos leitores que não foi possível reunir em uma única pessoa as forças exigidas para o presente intento. A publicação desta Edição Especial da Revista Jurídica do Banco do Nordeste, dedicada ao tema privacidade e proteção de dados pessoais, é fruto do esforço conjunto de inúmeras pessoas, que acreditaram que o propósito é relevante e gera valor para a sociedade. A essas pessoas meu reconhe-

cimento e profunda gratidão.

Vivemos na era da informação, na qual o uso dos dados pessoais desempenha protagonismo econômico. Mas, não podemos olvidar a necessidade da proteção destes dados pessoais como fundamento para a preservação dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Estarem adequadas à legislação de proteção de dados pessoais aumenta a relação de confiança com os seus clientes, gera valor aos seus produtos e serviços e, consequentemente, promove a competividade das empresas.

Neste particular, a relevância e o valor desta Edição Especial estão alinhados com a Visão do Banco do Nordeste de ser reconhecido pela sua capacidade de promover o bem-estar das famílias e a competitividade das empresas da região.

Na presente Edição os artigos apresentados demonstram a transversalidade da temática de proteção de dados pessoais, com abordagens que evidenciam sua abrangência e interação com diversos ramos do conhecimento.

Analisando a utilização de algoritmos para tomada de decisões automatizadas, para definição de risco de crédito com metodologia de *scoring,* o artigo *Risco de crédito e o direito a revisão de decisões automatizadas: uma sistematização de elementos mínimos a serem observados em tratamentos de scoring de crédito,* traz uma reflexão sobre a necessidade de utilização de critérios mínimos a serem observados no atendimento ao direito de revisão de decisões automatizadas, em razão da ausência de definições concretas no art. 20 da LGPD, acreditando que isto pode orientar os agentes de tratamento do setor financeiro na busca da conformidade à citada legislação.

Certamente um dos temas mais sensíveis previstos na LGPD, a natureza jurídica da responsabilidade civil dos agentes de tratamento de dados pessoais, em razão de danos causados aos titulares de dados pes-

soais, está muito bem explorada no artigo *A responsabilidade civil no enfoque da lei nº 13.709/2018: sua natureza jurídica no particular dos agentes de tratamento de dados pessoais.* A partir da constatação da omissão legislativa, os autores exploram as diversas correntes doutrinárias sobre o tema, para concluírem que a melhor opção seria considerar a Corrente Dualista, na medida em que a análise deve ser realizada de acordo com o caso concreto, podendo a responsabilidade civil dos agentes de tratamento de dados pessoais ora ter natureza subjetiva, ora natureza objetiva, de acordo com o risco da especificidade da atividade de tratamento desempenhada.

A partir do cotejamento entre a LGPD e os princípios da livre iniciativa e da livre concorrência, consagrados constitucionalmente, o artigo *Dados pessoais como ativo na sociedade da informação: a LGPD como instituição e suas interações nas livres iniciativa e concorrência,* evidencia que os dados pessoais se tornaram ativos econômicos capazes de gerar grandes fortunas, aumentando a esfera de influência das organizações e seu poderio econômico, proporcionando uma crescente ameaça à ordem econômica e financeira, bem como aos direitos dos titulares de dados pessoais. Analisa, ainda, os impactos da LGPD no fundamento da ordem econômica e nos princípios constitucionais da livre iniciativa e da livre concorrência, em especial no que respeita aos impactos econômicos que a adequação à nova legislação pode causar às microempresas e empresas de pequeno porte, em razão dos custos de conformidade.

O artigo *Open banking, sigilo bancário e LGPD: como resolver essa equação?,* analisa as implicações do recém criado Sistema Financeiro Aberto, com a LGPD e a Lei do Sigilo Bancário, para concluir que o *Open Banking* demonstrará para o consumidor o quanto seus dados pessoais são valiosos e devem ser usados em seu benefício, sob pena de aplicação das salvaguardas legais previstas na LGPD e na Lei do Sigilo Bancário, para que sejam combatidos desvios e excessos.

No artigo *Proteção de dados pessoais, privacidade e ética na sociedade da informação: as lições da superinteligência artificial,* o leitor é convocado a pensar, em especial à luz da LGPD, sobre algumas aplicações da inteligência artificial, sob a perspectiva dos impactos dessa nova tecnologia na privacidade e proteção de dados pessoais, sugerindo que a concepção da IA requer a adoção de técnicas mínimas e razoáveis de conformidade, com o estabelecimento de padrões éticos, para composição de uma *amálgama de justiça e de razoabilidade.*

Por fim, mas não menos importante, o artigo *Responsabilização civil na LGPD: novos dilemas ou desafios preexistentes na dogmática jurídica?*, busca refletir, a partir da omissão da nova legislação e de decisões judiciais atuais, se os debates em torno da temática exigem novas abordagens ou se situam no campo de interpretação dos elementos nucleares das teorias da responsabilização consagrados na doutrina e jurisprudência pátrias.

Na Seção Jurisprudência, esta edição oferece ao leitor a oportunidade de conhecer dois julgamentos paradigmáticos do Supremo Tribunal Federal, que reconhecem a existência de um direito fundamental autônomo à proteção de dados pessoais na ordem jurídico-constitucional brasileira. Na Ação Direta de Inconstitucionalidade nº 6.388 o STF analisa a inconstitucionalidade da Medida Provisória nº 954 que previa *o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19)*. Por sua vez, na Ação Direta de Inconstitucionalidade nº 6.649 o STF avalia *se é legítimo o compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, examinando a compatibilidade do Decreto 10.046/2019 com o regime de proteção de dados estabelecido pela ordem constitucional brasileira*.

Encerrando esta edição, a Seção Legislativa compartilha a Emenda Constitucional nº 115/2022, que incluiu na Constituição Federal a proteção de dados pessoais no rol de direitos fundamentais, a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014), por compreender ser o mínimo necessário para aqueles dispostos a iniciar o estudo da temática.

Tenho certeza de que esta Edição Especial da Revista Jurídica do Banco do Nordeste, construída com muito esmero por diversas pessoas, não se limitará a transferir conhecimento, mas servirá de instrumento de criação das possibilidades para própria produção ou construção deste conhecimento, pois, como afirmado por Paulo Freire, este é o verdadeiro significado da palavra 'ensinar'.

Boa leitura.

Marcel Alvarenga
DPO do Banco do Nordeste

DOUTRINA

REVISTA
JURÍDICA
DO BANCO DO NORDESTE

Risco de crédito e o direito a revisão de decisões automatizadas: uma sistematização de elementos mínimos a serem observados em tratamentos de scoring de crédito

Credit risk and the right to review automated decisions: a systematization of minimum elements to be observed in credit scoring treatments

Alisson Possa

» Advogado, mestrando em Direito Constitucional pelo Instituto Brasiliense de Direito Público (IDP), coordenador do Subcomitê de Acompanhamento Legislativo e Regulatório do GT de Proteção de Dados e Tecnologia da Frente Parlamentar do Setor de Serviços. É Certified Information Privacy Professional/Europe (CIPP/E) pela International Association of Privacy Professionals (IAPP) e Data Protection Professional pela Academy of European Law (ERA).

» E-mail: *alisson.possa@possaconsultoria.com.br*

Julia Lonardoni Ramos

» A Advogada, cursando LL.M. em Privacy, Cybersecurity and Data Management na Universidade de Maastricht, Holanda. LL.M. em Direito Digital na Universidade Presbiteriana Mackenzie. Formada em Direito pela Pontifí-

REVISTA JURÍDICA DO BANCO DO NORDESTE

cia Universidade Católica do Paraná. É Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Manager (CIPM) e Certified Data Protection Officer/Brazil (CDPO/BR) pela International Association of Privacy Professionals (IAPP) e Data Protection Officer (DPO) pela EXIN.

» E-mail: julial.ramos@outlook.com

Recebimento: 31/08/2022
Aprovação: 27/10/2022

RESUMO

A utilização de decisões automatizadas por algoritmos para definir risco de créditos com metodologias de *scoring* podem trazer danos aos titulares, gerando a necessidade de critérios mínimos para a observância de requerimentos referentes a revisão de decisões automatizadas, um direito previsto no art. 20 da LGPD e que ainda não possui definições concretas. O presente artigo busca identificar esses critérios mínimos no contexto dessas decisões para a atribuição de risco de crédito através de uma análise hipotético-dedutiva das definições internacionais e nacionais sobre esse direito, sob a ótica das regulações setoriais específicas do setor financeiro e as interpretações jurisprudenciais já existentes.

PALAVRAS-CHAVE

Risco de Crédito; *Scoring;* Direito à Revisão de Decisões Automatizadas; Regulações Setor Financeiro; Jurisprudência Brasileira.

ABSTRACT

The use of automated decisions by algorithms to define credit risk with scoring methodologies can harm holders, generating the need for minimum criteria for compliance with requirements referring to the review of automated decisions, a right provided for in art. 20 of the LGPD and which still does not have concrete definitions. This article seeks to identify these minimum criteria in the context of these decisions for the assignment of credit risk through a hypothetical-deductive analysis of international and national definitions of this right from the perspective of specific sectoral regulations of the financial sector and existing judicial decisions.

KEYWORDS

Credit risk; Scoring; Right to Review Automated Decisions; Financial Sector Regulation; Brazilian jurisprudence.

SUMÁRIO

INTRODUÇÃO

Uma das grandes dificuldades da sociedade atual está sendo a criação de mecanismos para a proteção de direitos perante a crescente evolução de algoritmos e usos de dados. Segundo a UNCTAD (*United Nations Conferente of Trade and Development*), 137 de 194 países já possuem legislações voltadas para a proteção de dados e privacidade[1].

O Brasil faz parte desses países, com sua Lei n° 13.709/18 – Lei Geral de Proteção de Dados Pessoais, que contém previsões de várias naturezas, desde regras para tratamentos de dados por empresas privadas que buscam proveitos econômicos até regras para tratamentos de dados por órgãos públicos a fim de atingir as finalidades da administração pública.

Dentre as disposições da legislação, ela inova ao trazer direitos aos titulares de dados pessoais, alguns previstos expressamente no art. 18 e outros dispersos como limitações a usos de determinadas bases legais. Um dos direitos que ela insere no ordenamento jurídico e que foi de grande polêmica na etapa legislativa foi o art. 20, que trata sobre o direito à revisão de decisões automatizadas.

O artigo 20, que contava com redação que previa expressamente que a revisão de decisões automatizadas deveria ser realizada por ser humano, um paralelo com a previsão do mesmo direito na Regulação Geral de Proteção de Dados da União Europeia[2], sofreu veto e modificações em sua redação na formulação da Lei nº 13.853/2019, que converteu a Medida Provisória n° 869/18.

Ocorre que atualmente inúmeros segmentos econômicos contam

1 Números divulgados na plataforma interativa oficial do órgão. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 28 jul. 2022.

2 PALHARES, Felipe. *Revisão de decisões automatizadas*. Portal JOTA, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/revisao-de-decisoes-automatizadas-29092019. Acesso em: 28 jul. 2022.

com sistemas automatizados para a análise de grandes bases de dados pessoais e tomadas de decisões. Cotidianamente estamos sujeitos a decisões automatizadas em todos os momentos da vida social, principalmente em uma sociedade informacional[3] que os dados relativos a indivíduos são fonte primária da economia. Nesse contexto, o direito à revisão de decisões automatizadas é um importante instrumento contra danos a direitos e liberdades fundamentais causados por algoritmos.

É nesse contexto de embate entre direitos com atores econômicos que o presente artigo se insere, uma vez que o tema a ser abordado é relativo ao direito de revisão de decisões automatizadas no contexto bancário.

Instituições financeiras possuem um papel importante no desenvolvimento econômico e social dos Estados modernos, principalmente em períodos de crises. Considerando o seu papel, o setor financeiro é um dos setores da economia mundial que mais busca modernizar suas operações, estando na vanguarda na adoção de inovações tecnológicas. Podemos citar, por exemplo, o desenvolvimento de ferramentas para análise de risco crédito com base em cálculos matemáticos por Henry Wells, funcionário da Spiegel Inc, na década de 1940[4].

É justamente com o avanço de algoritmos e da tecnologia da informação dos mecanismos para análise de risco de crédito, através de métodos de cálculos de *scoring* de indivíduos, com base em grandes bases de dados, que o direito à revisão de decisões automatizadas inaugura uma nova realidade como um modulador de práticas já estabelecidas no setor.

Conforme já citado, essa nova previsão legal ainda é eivada de incertezas e falta de critérios objetivos para a determinação de seu cumpri-

3 CASTELLS, Manuel. *A era da informação*: economia, sociedade e cultura. *In*: A Sociedade em rede. V. 1. São Paulo: Paz e Terra, 2000.

4 SILVERIO, Murilo. *Aplicação de Algoritmos de Aprendizado de Máquina no Desenvolvimento de modelos de Escore de Crédito*. Dissertação (Mestrado). INSPER, 2015.

mento. Quando analisada dentro do contexto de um setor que, além de estar na vanguarda de inovações tecnológicas, também é altamente regulado, muitos questionamentos sobre os limites para o exercício dele acabam surgindo. Especificamente, os tratamentos de dados pessoais para análise de risco de crédito, muitos deles com base em métodos de *scoring*, são uma das principais atividades que suscitam problemas, considerando os danos individuais que as decisões automatizadas podem gerar.

O presente artigo, portanto, busca responder a seguinte pergunta: através da análise de regulações e práticas do setor financeiro, podem ser identificados critérios mínimos para a observância do direito à revisão de decisões automatizadas tomadas para a determinação de risco para concessão de crédito?

O objetivo geral é identificar, valendo-se de uma metodologia hipotético-dedutiva com revisão legal, jurisprudencial e bibliográfica, critérios mínimos para a garantia da observância do direito à revisão de decisões automatizadas nos tratamentos de dados pessoais que instituições financeiras realizam para a determinação de risco de crédito, principalmente aquelas decisões que causam impactos negativos nos titulares de dados pessoais.

Os objetivos específicos que deverão ser alcançados para responder à pergunta serão buscados na seguinte ordem: o primeiro capítulo destacará o entendimento atual, brasileiro e internacional, acerca do direito à revisão de decisões automatizadas, principalmente elementos gerais que são necessários para sua observância. O segundo capítulo buscará as determinações legais, regulatórias e jurisprudenciais acerca das atividades para análise de risco de crédito de pessoas naturais. O terceiro capítulo analisará os padrões comuns entre as determinações levantadas no primeiro capítulo com aquelas gerais identificadas no segundo capítulo, identificando as que podem ser concretizadas em procedimentos internos de instituições financeiras.

1. DIREITO A REVISÃO DE DECISÕES TOMADAS COM BASE NO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

A utilização de algoritmos na tomada de decisão é extremamente relevante na economia da informação e um grande diferencial competitivo de mercado, vez que, com seu uso, as organizações tomam melhores decisões, com risco reduzido e em um curto espaço de tempo.

Em tempos de *Big Data*, inúmeros segmentos econômicos contam com sistemas automatizados para a análise de grandes bases de dados pessoais e tomadas de decisões. Um grande exemplo disso é a utilização de inteligência artificial por instituições financeiras para análise de risco de crédito, sendo muitas delas baseadas em métodos de *scoring*.

Segundo Mendes e Mattiuzzo, o desenvolvimento tecnológico trouxe importantes contribuições para o crescimento do uso de algoritmos nas tomadas de decisões, pois hoje, além de ser possível coletar e processar um elevado número de informações para avaliação de risco, essa avaliação pode ser quantificada por uma pontuação ou um prognóstico de comportamento futuro de um indivíduo, permitindo assim a classificação de um indivíduo em uma categoria de risco específica.[5]

Dessa forma, os riscos de lesão aos direitos e garantias fundamentais dos titulares são evidentes e, no intuito de conceder uma proteção às partes vulneráveis nesses processos de decisões automatizadas, que influenciam diretamente nos interesses e direitos dos indivíduos, é que a Lei Geral de Proteção de Dados (LGPD) se apresenta.

5 MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithms and Discrimination: The Case of Credit Scoring in Brazil. *In*: ALBERS, Mario; SARLET, Ingo Wolfgang (Eds.). *Personality And Data Protection Rights on The Internet*: Brazilian and German Approaches. Springer, 2022. P. 407-443.

A Lei nº 13.709/2018, conhecida como LGPD, foi promulgada em 14 de agosto de 2018 com o objetivo de regulamentar o tratamento de dados pessoais realizados por pessoas físicas ou jurídicas de direito público ou privado e proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, ou seja, dos indivíduos.

Nesse contexto, as atividades de *scoring* realizadas por instituições financeiras devem observar os dispostos trazidos na LGPD, especialmente as disposições referentes ao direito de revisão de decisão automatizada previsto no art. 20 da Lei:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
>
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
>
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

A Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011) também dispõe sobre o direito a revisão realizada exclusivamente por meios automatizados em seu art. 5º, inciso VI.

A partir disso, surge a discussão a respeito de quais seriam os critérios e informações mínimas a serem fornecidos ao titular de dados em observância ao direito à revisão de decisões automatizadas tomadas para a determinação de risco para concessão de crédito, que será objeto de análise no presente capítulo.

A LGPD não inovou ao dispor sobre o direito a revisão de decisões tomadas unicamente com base em tratamento automatizado. O regulamento europeu de proteção de dados *General Data Protection Regulation - GDPR* trata desse direito em seu art. 22, onde estabelece que o titular possui o direito de não se sujeitar a uma decisão baseada exclusivamente no tratamento automatizado - incluindo a definição de perfis, que produza efeitos jurídicos sobre ele ou o afete significativamente de forma semelhante. Ainda, nos termos do artigo 22(3), o titular possui o direito de revisão dessas decisões por intervenção humana.

Muito se foi discutido no âmbito europeu – e ainda é – o que se caracterizaria esse direito a revisão, ou seja, quais informações deveriam ser concedidas ao titular e de que forma. No intuito de sanar as inconsistências o Grupo de Trabalho do Artigo 29 (*Article 29 Working Party*) – atual *European Data Protection Board (EDPB)* – publicou uma orientação sobre o tratamento de dados pessoais por decisões automatizadas e a definição de perfis para efeitos do GDPR.

Conforme a orientação, as instituições devem identificar uma forma simples de comunicar ao titular dos dados a lógica ou os critérios utilizados na tomada a decisão. Assim, caso uma instituição financeira, que se utiliza de algoritmos para *scoring* de crédito, apresentar uma decisão negativa ao titular, como a rejeição de um pedido de empréstimo, e o titular exercer seu direito de revisão em face da decisão tomada, a instituição deve apresentar os dados referentes às principais características consideradas na tomada da decisão, a fonte dessas informações e a sua relevância, como os dados pessoais utilizados para a avaliação e os métodos de pontuação de crédito utilizados.[6]

No mesmo sentido, a autoridade de proteção de dados do Reino Unido (*Information Commissioner's Office - ICO*) publicou um guia com a

6 EUROPA. *European Comission*. 2022. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 18 ago. 2022.

finalidade de auxiliar as instituições que realizam o tratamento automatizado de dados pessoais a atenderem os direitos previstos no GDPR.

De acordo com a Autoridade, as informações que devem ser concedidas aos titulares quando do pedido de revisão da decisão automatizada referem-se inicialmente à transparência pela instituição no uso de processos de tomada de decisão automatizadas, a lógica envolvida nas tomadas de decisões, o motivo pelo qual a instituição utiliza esses métodos e os resultados prováveis, ou seja, quais são as possíveis consequências aos indivíduos.[7]

Ressalta-se que, ao dispor sobre a lógica envolvida na tomada de decisões, a Autoridade esclarece que as informações devem descrever, de forma compreensível ao titular, o tipo de informação (dados pessoais) coletado ou utilizado na criação do perfil ou na tomada de decisão automatizada e a relevância dessas informações na decisão tomada. O importante é que fique claro ao titular como a instituição chegou à decisão.[8]

No contexto brasileiro, alguns pontos devem ser destacados quanto às informações a serem apresentadas ao titular, quando da solicitação de revisão da decisão tomada exclusivamente com base em tratamento automatizado. Isso porque a LGPD determina que o controlador deverá fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão.

Contudo, o simples fornecimento dos critérios e procedimentos utilizados, ou seja, a explicação da lógica por trás da decisão, é insuficiente para que o titular realmente consiga compreender a decisão tomada. É muito difícil compreender o *output*, isto é, o resultado da decisão, sem saber qual foi o *input* das informações.

---

7 REINO UNIDO. *Information Commissioner's Office*. 2022. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/. Acesso em: 18 ago. 2022.

8 Idem.

Em termos práticos, o titular não tem como entender claramente uma tomada decisão de rejeição de empréstimo em uma instituição financeira, apenas com informações dos critérios e/ou procedimentos utilizados (como a análise de comprometimento da renda e históricos de pagamentos realizados), pois não tem a compreensão de quais dados foram utilizados sob avaliação desses critérios, bem como sua origem. Dados incorretos, inexatos ou desatualizados podem significativamente alterar o resultado de uma avaliação realizada com base nos mesmos critérios apontados.

Nesse ponto, cabe destacar a importância da compreensão do titular em relação ao tratamento de seus dados pessoais, pois, para que possa se autodeterminar em relação aos seus dados, ou seja, para que possa exercer seu poder de decisão a respeito do tratamento ou não e, consequentemente, exercer seus direitos previstos na LGPD, uma série de informações devem ser concedidas.

Como mecanismo de efetivação do princípio da transparência, a LGPD dispõe, em seu art. 9º, que o titular possui direito ao acesso facilitado às informações referentes ao tratamento de seus dados, que devem ser disponibilizadas de forma clara, adequada e ostensiva acerca da: (i) finalidade específica, forma e duração do tratamento; (ii) identificação e informações de contato do controlador; (iii) informações acerca do uso compartilhado de dados pelo controlador, bem como a finalidade; (iv) a responsabilidades dos agentes que realizarão o tratamento; e (v) quais são os seus direitos previstos no art. 18 da legislação.

Nesse sentido, tem-se que o titular possui duas classificações de direitos quando do tratamento automatizado de seus dados pessoais: direitos referentes à formação da decisão e direitos referentes ao resultado da decisão automatizada[9], sendo os primeiros pressupostos dos segundos.

9 REIS, Nazareno César Moreira. *Decisões automatizadas, revisão humana e direito à proteção de dados*: uma análise à luz da Lei Geral de Proteção de Dados Pessoais. Dissertação (Mestrado). IDP/iCEV, 2021.

Os direitos referentes à formação da decisão dizem respeito à confirmação da existência do tratamento de dados pessoais (art. 18, inciso I e art.19 da LGPD), ao acesso às informações utilizadas pelo controlador para a tomada de decisão (art. 6º, inciso IV, art. 9º e art. 18, inciso II da LGPD) e à correção de dados incompletos, inexatos ou desatualizados (art. 18, inciso III da LGPD).

A partir da ciência e entendimento de quais são os dados pessoais tratados, bem como sua origem, há a possibilidade de o titular avaliar a veracidade das informações e corrigi-las, caso necessário.

Esse direito à informação, também entendido por doutrinadores como direito à explicação, é apresentado por Souza, Perrone e Magrani[10] que sustentam que na LGPD pode-se fundar "um direito à explicação a partir de três pontos principais: o princípio da transparência, o direito de acesso à informação e como um pressuposto para o exercício dos outros direitos e, particularmente, do direito a requerer revisão de decisões automatizadas.".

Por sua vez, os direitos relativos ao resultado da decisão automatizada referem-se ao direito de revisão da decisão propriamente dita (art. 20 caput e §1º da LGPD). Aqui os critérios e procedimentos utilizados para a decisão automatizada devem ser apresentados ao titular, para que possa compreender o motivo da tomada de decisão.

A avaliação dos critérios utilizados é um ponto fundamental acerca da avaliação da decisão tomada, vez que existe a possibilidade de os critérios utilizados não serem legais e muitas vezes enviesados, o que pode acarretar uma tomada de decisão discriminatória ao titular, decisão esta que é vedada pela LGPD.

---

10 SOUZA, Carlos Afonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e sua positivação na LGPD. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. Edição do Kindle.

Presente no inciso IX, do art. 6º da LGPD, o princípio da não discriminação consiste na impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. A discriminação algorítmica pode ocorrer por diversos motivos, cite-se a discriminação por generalização e por erro estatístico.

Conforme Mendes e Mattiuzzo, a discriminação por generalização ocorre nos casos em que, "embora o modelo funcione bem e seja estatisticamente correto, leva a uma situação na qual algumas pessoas são equivocadamente classificadas em certos grupos"[11]. Um exemplo apresenta-se quando o modelo considera que determinado bairro é de baixa renda e nega pedidos de créditos de quem a ele pertença.

Já, a discriminação por erro estatístico trata-se de algum erro "genuinamente estatístico, abrangendo desde dados incorretamente coletados, até problemas no código do algoritmo, de modo que ele falhe em contabilizar parte dos dados disponíveis, contabilize-os de forma incorreta etc."[12].

Dessa forma, conhecer os critérios e procedimentos utilizados na tomada de decisão auxilia na compreensão, pelo titular, das razões motivadoras do resultado apresentado e lhe permite questionar acerca de sua legalidade ou não.

Portanto, conclui-se que o direito à revisão das decisões tomadas com base em tratamento automatizado de dados pessoais abrange tanto o direito de informação quanto os dados pessoais tratados e sua origem, assim como os critérios e procedimentos utilizados na tomada de decisão.

Cumpre esclarecer que a Autoridade Nacional de Proteção de Dados (ANPD) possui um papel importante no atendimento ao pedido de revisão

11 MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithms and Discrimination: The Case of Credit Scoring in Brazil. *In*: ALBERS, Mario; SARLET, Ingo Wolfgang (Eds.). *Personality And Data Protection Rights on The Internet*: Brazilian and German Approaches. Springer, 2022. P. 407-443.

12 Idem.

da decisão automatizada pelo titular, nas situações em que o Controlador alegar que o atendimento ao pedido fere o segredo comercial e industrial. Nesses casos, nos termos do parágrafo segundo da LGPD, a ANPD poderá realizar uma auditoria para verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais.

Para melhor compreensão do direito a revisão de decisões automatizadas de dados pessoais no contexto da análise de riscos de crédito por instituições financeiras, faz-se necessária a compreensão das normas e entendimentos acerca do uso de métodos de *scoring* de crédito, que serão apresentadas no capítulo a seguir.

2. RISCOS DE CRÉDITO COM BASE EM METODOLOGIAS DE SCORING NO BRASIL

O presente capítulo irá abordar as legislações, regulações e entendimentos jurisprudenciais acerca das metodologias de *scoring* de crédito utilizadas por instituições financeiras para análise de riscos de crédito, que, atualmente, são realizadas através de algoritmos automatizados e cada vez mais avançados.

Destarte, é necessário esclarecer a relação entre riscos de crédito e metodologias de *scoring* de crédito.

A análise de riscos de crédito por instituições financeiras obteve grande importância no cenário das regulações de instituições financeiras com o Acordo de Basileia I em 1988, que estabeleceu recomendações fins de mitigação de riscos de créditos. Esse Acordo foi elaborado pelo Comitê de Basileia para Supervisão Bancária, um fórum internacional para discussões e sugestões de regulações voltadas para o cenário financeiro internacional[13].

13 A definição está no site oficial do Banco Central do Brasil. Disponível em https://www.bcb.gov.br/estabilidadefinanceira/recomendacoesbasileia. Acesso em 29 jul. 2022.

Enquanto o Acordo de Basileia I tratava ativos de riscos de forma uniforme com o mesmo peso no cálculo na alocação de capital, o Acordo de Basileia II, em 2004, determinou a diferenciação de ativos no cálculo da ponderação do capital alocado conforme o risco associado a cada ativo[14].

É com essa mudança, em 2004, que modelos internos para mensuração de risco de cada ativo passaram a ter importância essencial para a gestão de risco do crédito.

Os modelos de *scoring* de crédito, portanto, são modelos matemáticos que permitem a tomada de decisões para uma gestão de risco de crédito.

A definição de *scoring* de crédito por Araújo e Carmona é que "são sistemas que atribuem pontuações às variáveis de decisão de crédito de um proponente, mediante a aplicação de técnicas estatísticas. Esses modelos visam a segregação de características que permitam distinguir os bons dos maus créditos"[15].

O *scoring* é uma pontuação que representa a probabilidade de perda de um crédito gerada através de uma equação com variáveis referentes ao proponente ou à operação[16] e que pode ser utilizada para classificação de crédito em diferentes categorias, como adimplementos ou inadimplentes, bons ou maus, tudo a depender da pontuação[17].

Atualmente, com a velocidade de processamento de grandes bases de dados disponível às instituições financeiras e as grandes bases de dados, o cálculo do *scoring* de crédito e a classificação é comumente reali-

14 SILVERIO, Murilo. *Aplicação de Algoritmos de Aprendizado de Máquina no Desenvolvimento de modelos de Escore de Crédito*. Dissertação (Mestrado). INSPER, 2015, p. 16.

15 ARAÚJO, Elaine Aparecida; CARMONA, Charles Ulises de Montreuil. Desenvolvimento de modelos Credit Scoring com abordagem de regressão logística para a gestão da inadimplência de uma instituição de microcrédito. *Contabilidade Vista & Revista*, v. 18, n. 3, 2007. p. 109.

16 Idem. P. 110.

17 Idem. P. 110.

zada por algoritmos automatizados. Segundo Mendes e Mattiuzzi, "essa pontuação é criada por meio de um procedimento automatizado, no qual os dados existentes são incorporados a um algoritmo e os indivíduos são atribuídos a uma categoria de risco específica"[18] (tradução nossa).

Sobre o funcionamento desse modelo, Araújo e Carmona[19] explicam que os modelos de *scoring* de crédito são pontuações que representam o risco da perda do valor para a instituição, sendo uma probabilidade de inadimplência quando comparado com uma pontuação mínima aceitável, podendo, ainda, classificar bons ou maus pagadores. Ainda, segundo eles, quando esses modelos são aplicados a pessoas físicas, são utilizados dados cadastrais e de comportamento dos indivíduos, identificando fatores para a probabilidade de inadimplência.

Considerando a importância da análise de risco para as instituições financeiras, principalmente com os Acordos de Basileia e a necessidade de grandes quantidades de dados sobre indivíduos e empresas para a melhor tomada de decisões, o Brasil aprovou, em 2011, Lei n° 12.414, que trata sobre "a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.".

A legislação foi atualizada em 2019 através da Lei Complementar n° 166 a fim de facilitar e automatizar o compartilhamento dos dados pelos gestores e fontes, sem a necessidade de anuência e consentimento dos titulares.

Ela disciplina a criação de bancos de dados que devem ser instituí-

18 No original: "This score is created through an automated procedure, in which the existing data is incorporated into an algorithm and the individuals are assigned to a specific risk category". MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithms and Discrimination: The Case of Credit Scoring in Brazil. *In:* ALBERS, Mario; SARLET, Ingo Wolfgang (Eds.). *Personality And Data Protection Rights on The Internet*: Brazilian and German Approaches. Springer, 2022. P. 408.

19 ARAÚJO, Elaine Aparecida; CARMONA, Charles Ulises de Montreuil. *Opt. Cit.* P. 107.

dos ou geridos por pessoas jurídicas de direito público interno (art. 1°, parágrafo único), que devem ser alimentados pelos gestores com dados originários de fontes, definidas no art. 2º, inciso IV, como

> [...] pessoa natural ou jurídica que conceda crédito, administre operações de autofinanciamento ou realize venda a prazo ou outras transações comerciais e empresariais que lhe impliquem risco financeiro, inclusive as instituições autorizadas a funcionar pelo Banco Central do Brasil e os prestadores de serviços continuados de água, esgoto, eletricidade, gás, telecomunicações e assemelhados[20].

Os dados a serem compartilhados devem ser relativos ao adimplemento de operações de crédito (art. 3°), com informações claras, verdadeiras e de fácil compreensão, e que sejam necessárias para avaliação da situação econômica do cadastrado (art. 3°, §1º), sendo definido como objetivas (art. 3°, §2º, inciso I) "aquelas descritivas dos fatos e que não envolvam juízo de valor;", como claras (art. 3°, §2º, inciso II) " aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica", como verdadeiras (art; 3º, §2°, inciso III) "aquelas exatas, completas e sujeitas à comprovação" e como de fácil compreensão (art.3°, §2°, inciso IV) "aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados".

São vedadas expressamente informações excessivas (art. 3°, §3°, inciso I) "assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor" e informações sensíveis (art. 3°, §3°, inciso II) "assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

---

20 BRASIL. *Lei Complementar nº 166*, de 8 de abril de 2019. Disponível em: nhttp://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm Acesso em: 28 jul. 2022.

O art. 17 do Decreto 9.936/19, que regulamenta a referida legislação, discrimina exatamente os dados que devem ser compartilhados: dados da fonte (nome e CPF/CNPJ), dados do cadastrado (nome, CPF/CNPJ, endereço residencial, endereço eletrônico e telefone), informações de adimplemento (todos os dados relativos à natureza do crédito, condições, valores, datas de pagamentos, valores devidos etc.).

A utilização desses dados é limitada a finalidades específicas de "realização de análise de risco de crédito do cadastrado" (art. 7º, inciso I) ou "subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente" (art. 7°, inciso II)[21].

Ocorre que, conforme descrito anteriormente, são alcançadas através de utilização de sistemas automatizados, que nem sempre são claros sobre os critérios efetivamente utilizados. A legislação, para limitar os efeitos das decisões automatizadas, estabelece como direito do cadastrado a solicitação de revisão de decisões realizada exclusivamente por meios automatizados (art. 5º, inciso VI), o direito ao conhecimento de elementos e critérios considerados para análise de risco (art. 5º, IV) e a obrigação dos gestores de bancos de dados em fornecer "política de coleta e utilização de dados pessoais para fins de elaboração de análise de risco de crédito[22]" (art. 7º-A, §1º).

Disposições de grande importância para auxiliar a responder à pergunta problema do presente artigo são as constantes dos incisos do art. 7º-A, que veda elementos e critérios a serem utilizados na composição da nota ou pontuação de crédito, sendo aquelas ligadas a dados pessoais sensíveis ou não vinculadas à análise do risco de crédito (inciso I), de pessoas que não possuam com o cadastrado relação de dependência ou

21 BRASIL. *Decreto nº 9936, de 24 de julho de 2019*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9936.htm Acesso em: 28 jul. 2022.

22 Idem.

parentesco de primeiro grau (inciso II) e relacionadas ao exercício de direitos pelo cadastrado (inciso III).

No próximo capítulo explorar-se-á como essas vedações, ligadas às previsões dos tipos de dados que devem ser utilizados no contexto da finalidade de concessão de crédito, indicam pontos que devem ser obrigatoriamente explicitados e explorados em um pedido de revisão de decisão automatizada.

A referida legislação também já foi objeto de análise pelo Superior Tribunal de Justiça em sede de Repercussão Geral em duas oportunidades, que geraram os Temas Repetitivos 710 e 915. Importante destacar que os julgamentos foram realizados antes da alteração pela Lei Complementar n° 166/2019, em que mudanças significativas ocorreram ao criar a possibilidade de compartilhamento automatizado pelos gestores e fontes.

O Tema Repetitivo 710/STJ[23] gerou a seguinte tese:

> I - O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). II - Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). III - Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. IV - Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. V - O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e

23 BRASIL. Superior Tribunal de Justiça. *Acórdão no Resp1419697/RS*. Relator: Paulo de Tarso Sanseverino. Distrito Federal, Brasília, DF, 12 de novembro de 2014). Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=39037908&num_registro=201303862850&data=20141117&tipo=51&formato=PDF Acesso em: 01 ago. 2022.

> solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

Na decisão do Resp. 1419697/RS, o Relator, antes mesmo da Lei Geral de Proteção de Dados, em seu voto, efetuou uma análise da licitude do método de *scoring* com limites no direito à privacidade e na transparência e boa-fé na prestação de informações, sendo reservado o segredo da atividade empresarial da metodologia em si do cálculo, sem necessidade de divulgação das fórmulas matemáticas[24].

Com base no julgamento acima, outras ações foram ajuizadas sobre a questão, gerando a fixação do Tema Repetitivo 915/STJ[25]:

> Em relação ao sistema "credit scoring", o interesse de agir para a propositura da ação cautelar de exibição de documentos exige, no mínimo, a prova de: i) requerimento para obtenção dos dados ou, ao menos, a tentativa de fazê-lo à instituição responsável pelo sistema de pontuação, com a fixação de prazo razoável para atendimento; e ii) que a recusa do crédito almejado ocorreu em razão da pontuação que lhe foi atribuída pelo sistema "scoring".

Em seu voto, o Relator assevera que, para o preenchimento do segundo requisito acima apontado, o consumidor necessita conhecer os dados utilizados e as respectivas fontes, fazendo, inclusive, referente ao instrumento constitucional do *habeas data* como um fundamento da transparência de informações no Brasil[26].

---

24 STJ. Ibidem Págs. 34-35.

25 BRASIL. Superior Tribunal de Justiça. *Acórdão REsp n. 1.304.736/RS*, Relator Ministro Luis Felipe Salomão. Distrito Federal, Brasília, DF, 24 de fevereiro de 2016. Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=57414028&num_registro=201200318393&data=20160330&tipo=91&formato=PDF Acesso em: 01 ago. 2022.

26 STJ. Ibidem, Pág. 19.

Essas definições do Poder Judiciário também ajudam na identificação dos requisitos mínimos para o direito à revisão de decisões automatizadas baseadas em metodologias de *scoring* para determinação de risco de crédito.

Ante o exposto, faz-se necessário avaliar quais medidas devem ser adotadas pelas instituições financeiras no sentido de garantir ao titular de dados pessoais o devido acesso a suas informações, a transparência no tratamento, assim como o direito à explicação e revisão das decisões tomadas exclusivamente com base em decisões automatizadas, considerando as determinações legais, regulatórias e jurisprudenciais acerca das atividades para análise de risco de crédito apresentadas.

3. REVISÃO DE DECISÕES AUTOMATIZADAS NO CONTEXTO DAS INSTITUIÇÕES FINANCEIRAS

No primeiro capítulo tratamos sobre o direito à revisão de decisões automatizadas presente em legislações que tratam sobre o uso de dados pessoais. O consenso, tanto por parte da doutrina quanto por parte de órgãos de fiscalização e regulação na questão é que esse direito passa, necessariamente, pela obrigação de informar os titulares sobre os dados pessoais que foram efetivamente utilizados pelo Controlador.

A conclusão estabelecida sob o prisma de um direito geral à revisão é que não estamos falando de informações que somente abordam categorias gerais e amplas como “dados de identificação” ou “dados de consumo”, mas sim de especificação objetiva dos dados que foram utilizados no caso concreto do titular. Assim, exemplificativamente, não estaríamos falando de “dados de identificação”, mas sim de “nome completo e CPF n° X”, assim como “dados de consumo” deveriam ser “medicamento A, B e C”.

Cabe ressaltar que os agentes de tratamento já possuem a obrigação de manter registros de tratamentos de dados pessoais (art. 37 da LGPD)

com os fluxos que identificam os tipos de dados utilizados no tratamento específico, entre outras informações. Esses fluxos auxiliam o Controlador a buscar os dados pessoais específicos relativos ao titular, permitindo a correta informação que permite um direito à revisão.

No segundo capítulo, examinamos disposições legais específicas a tratamentos de dados pessoais para determinação de risco de crédito e duas grandes decisões judiciais que estabeleceram interpretações sobre essas disposições, especificamente em relação a obrigações de transparência como mecanismos de controle na conformidade desses tratamentos perante a legislação de crédito.

Também é importante destacar que esse cenário é pré-LGPD e constitucionalização da proteção de dados no país. Isso importa pois, se perante a lógica do direito do consumidor e outros sistemas normativos já se encontrava a tônica da transparência efetiva, com a nova ordem protetiva essas disposições e interpretações são reforçadas e ganham novos contornos.

A importância de uma transparência efetiva pode evitar erros como, por exemplo, a recente análise da *Federal Trade Comission* dos Estados Unidos, que identificou margem de erros para determinação de risco de crédito entre 10% e 21% no país.[27]

De acordo com Mattiuzo e Mendes, esses problemas são potencializados nas análises de risco de crédito por conta da predominante utilização de ferramentas automatizadas:

27 Texto original: "Credit reports are commonly described as black boxes, as their results are difficult to understand. The scoring procedure is criticized for being incomprehensible to the individual, since she normally receives no information about the internal structure of the algorithm. She also does not know what precisely influences her score. It is obvious that the lack of transparency has an influence on the error rate of the loan information since the procedure cannot be controlled either by the person concerned or by the supervisory authority". MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithms and Discrimination: The Case of Credit Scoring in Brazil. *In*: ALBERS, Mario; SARLET, Ingo Wolfgang (Eds.). *Personality And Data Protection Rights on The Internet*: Brazilian and German Approaches. Springer, 2022. P. 421.

> Os relatórios de crédito são comumente descritos como caixas pretas, pois seus resultados são difíceis para entender. O procedimento de pontuação é criticado por ser incompreensível para o indivíduo, pois normalmente ele não recebe informações sobre a estrutura interna do algoritmo. Ela também não sabe exatamente o que influencia sua pontuação. É óbvio que a falta de transparência tem influência na taxa de erro das informações sobre o empréstimo, uma vez que o procedimento não pode ser controlado nem pelo interessado nem pela autoridade supervisora[28] (tradução nossa).

Assim, aplicando os entendimentos descritos no primeiro capítulo às disposições legais e interpretações do Superior Tribunal de Justiça, podemos afirmar que o direito à revisão de decisões automatizadas no contexto de determinação de risco de crédito utilizando métodos de *scoring* necessita observar os seguintes elementos:

a) A legalidade dos tratamentos de dados para determinação de risco de crédito passa, necessariamente, por essa transparência efetiva e, principalmente, sob a ótica do Tema 710/STJ, itens "iv" e "v".

b) Ainda que se tratando do sistema Cadastro Positivo, as limitações de finalidade, necessidade e transparência (art. 3° e 6º da Lei n° 12.414/2011) devem ser observadas nas análises de risco de crédito pelas instituições (e não somente nos cadastros de bases de dados previstos nessa legislação).

c) O direito à revisão de determinação de risco de crédito passa pela informação de dados efetivamente utilizados (e não somente indicação de categorias) no método de *scoring*.

d) A informação dos dados efetivamente utilizados, garantindo a legalidade da operação, deve, também, permitir a efetiva correção desses dados pessoais na hipótese de falta de acurácia.

28 Idem, p. 423.

e) Descrições genéricas sobre o procedimento adotado não caracterizam transparência objetiva, clara e de fácil compreensão (art. 3°, §2º da Lei nº 12.414) e, portanto, não garantem o direito à revisão.

f) Como direito do titular de dados pessoais, as determinações de risco de crédito por tratamentos utilizando o método de *scoring* e a observância dos requisitos de canais de comunicação dos agentes de tratamento estão sujeitas à fiscalização da Autoridade Nacional de Proteção de Dados e não somente do Banco Central do Brasil.

CONSIDERAÇÕES FINAIS

O presente artigo se propôs a identificar requisitos mínimos e concretos para a observância do direito à revisão de decisões automatizadas nos tratamentos de dados pessoais que ocorrem em métodos de *scoring* de crédito para determinação de risco de crédito por instituições financeiras.

Através de um raciocínio dedutivo que utilizou premissas gerais do direito em questão e premissas específicas relativas ao setor financeiro, foi possível identificar pontos em comum que foram condensados na lista do capítulo 3, a fim de garantir segurança jurídica para as instituições financeiras e melhor controle para os titulares. Após a constitucionalização da proteção de dados como um direito fundamental na Constituição do Brasil, existe um reforço para a interpretação de procedimentos de análise de risco de crédito perante a autodeterminação informacional dos titulares.

Acreditamos que essa interpretação e a fixação dos elementos mínimos podem orientar os agentes de tratamento do setor financeiro ao buscarem a conformidade à legislação de proteção de dados nesses processos de tratamentos de dados específicos.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Elaine Aparecida; DE MONTREUIL CARMONA, Charles Ulises. Desenvolvimento de modelos Credit Scoring com abordagem de regressão logística para a gestão da inadimplência de uma instituição de microcrédito. *Contabilidade Vista & Revista*, v. 18, n. 3, p. 107-131, 2007.

BANCO CENTRAL DO BRASIL. *Recomendações de Basileia*. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/recomendacoesbasileia Acesso em: 29 jul. 2022.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. *In: A Sociedade em rede*. V. 1. São Paulo: Paz e Terra, 2000.

EUROPA. *European Comission*. 2022. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 18 ago. 2022.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Algorithms and Discrimination: The Case of Credit Scoring in Brazil. *In*: ALBERS, Mario; SARLET, Ingo Wolfgang (Eds.). *Personality And Data Protection Rights on The Internet*: Brazilian and German Approaches. Springer, 2022. P. 407-443.

PALHARES, Felipe. *Revisão de decisões automatizadas*. Portal JOTA, 2019. Disponível em https://www.jota.info/opiniao-e-analise/artigos/revisao-de-decisoes-automatizadas-29092019. Acesso em 28 jul. 2022.

REINO UNIDO. Information Commissioner's Office. 2022. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/. Acesso em: 18 ago. 2022.

REIS, Nazareno César Moreira. *Decisões automatizadas, revisão humana e direito à proteção de dados:* uma análise à luz da Lei Geral de Proteção de Dados Pessoais. Dissertação (Mestrado). IDP/iCEV, 2021.

SILVERIO, Murilo. *Aplicação de Algoritmos de Aprendizado de Máquina no Desenvolvimento de modelos de Escore de Crédito*. Dissertação (Mestrado). INSPER, 2015.

SOUZA, Carlos Afonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e sua positivação na LGPD. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. Edição do Kindle.

BRASIL. *Lei nº 12414, de 9 de junho de 2011*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm Acesso em: 29 jul. 2022.

BRASIL. *Lei Complementar nº 166*, de 8 de abril de 2019. Disponível em: nhttp://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm Acesso em: 28 jul. 2022.

BRASIL. *Decreto nº 9936, de 24 de julho de 2019*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9936.htm Acesso em: 28 jul. 2022.

BRASIL. Superior Tribunal de Justiça. *Acórdão no Resp1419697/RS*. Relator: Paulo de Tarso Sanseverino. Distrito Federal, Brasília, DF, 12 de novembro de 2014). Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=39037908&num_registro=201303862850&data=20141117&tipo=51&formato=PDF Acesso em: 01 ago. 2022.

BRASIL. Superior Tribunal de Justiça. *Acórdão REsp n. 1.304.736/RS*, Relator Ministro Luis Felipe Salomão. Distrito Federal, Brasília, DF, 24 de fevereiro de 2016. Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=57414028&num_registro=201200318393&data=20160330&tipo=91&formato=PDF Acesso em: 01 ago. 2022.

A responsabilidade civil no enfoque da lei nº 13.709/2018: sua natureza jurídica no particular dos agentes de tratamento de dados pessoais

Civil responsability in the focus of Law nº 13.709/2018: its legal nature in particular of personal data processing agents

Cláudio Germando Sampaio Machado

» Graduado em Direito pela Universidade de Fortaleza (UNIFOR); graduação (em trancamento) em Comunicação Social – Jornalismo pela Universidade Federal do Ceará (UFC); e pós-graduação em Direito Processual pela Universidade da Amazônia (UNAMA). Atualmente é Mestrando em Direito Empresarial pelo Centro Universitário 7 de Setembro (UNI7); professor da Universidade Corporativa Banco do Nordeste do Brasil (BNB) e advogado dessa mesma Instituição.

» E-mail: gdomdo@gmail.com.

Bruno Leonardo Câmara Carrá

» Graduado em Direito pela Universidade Federal do Ceará (UFC); Mestre em Direito (Direito e Desenvolvimento) pela Universidade Federal do Ceará (UFC); Doutor pela Universidade de São Paulo (USP). Pós-Doutor pela

REVISTA JURÍDICA DO BANCO DO NORDESTE

"Scuola di Giurisprudenza", da Universidade de Bolonha (Itália). Docente da graduação e da pós-graduação *stricto sensu* do curso de Direito do Centro Universitário 7 de Setembro (UNI7). É Juiz Federal no Tribunal Regional Federal da 5ª Região.

» E-mail: brunolccarra@gmail.com

Recebimento: 29/09/2022
Aprovação: 27/10/2022

RESUMO

Com a expansão da realidade no mundo digital, tornou-se necessária a regulamentação sobre o tratamento dos dados pessoais, de modo a proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural. Nesse ínterim, surge a Lei nº 13.709/2018, que será abordada na particularidade da responsabilidade civil dos agentes de tratamento de dados, uma vez que o legislador não especificou tal problemática de forma assertiva. Através de técnica de pesquisa doutrinária e legislativa, além da existência de fatores sociopolíticos, inclusive oriundos de ordenamentos jurídicos estrangeiros, conclui-se que a ideia dominante se posiciona pela natureza subjetiva quanto à responsabilidade civil em estudo, não obstante os vieses objetivos e dualistas estejam alicerçados em argumentos jurídicos bem fundamentados.

PALAVRAS-CHAVE

Responsabilidade civil; agentes de tratamento de dados pessoais; proteção de dados; Lei nº 13.709/2018; LGPD.

ABSTRACT

With the expansion of reality in the digital world, it became necessary to regulate the processing of personal data, in order to protect the fundamental rights of freedom and privacy, in addition to the free development of the personality of the natural person. In the meantime, Law No. 13,709/2018 appears, which will be addressed in the particularity of the civil liability of data processing agents, since the legislator did not specify such problem assertively. Through a doctrinal and legislative research technique, in addition to the existence of sociopolitical factors, including

those from foreign legal systems, it is concluded that the dominant idea is positioned by the subjective nature regarding the civil liability under study, despite the objective and dualist biases being based on well-founded legal arguments.

KEYWORDS

Civil responsability; personal data processing agents; data protection; Law nº 13,709/2018; LGPD.

SUMÁRIO

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) foi concebida com o intuito de ser uma resposta legislativa às ações de tratamento de dados pessoais, em especial nos tempos pós-modernos, em que a inteligência artificial, através de algoritmos pujantes, se tornou capaz de processar o tratamento dessas informações em uma velocidade em crescimento exponencial, gerando muitas susceptibilidades à sociedade em geral.

Com efeito, os dados pessoais são amplamente reconhecidos como um dos insumos mais superlativos da atualidade, quiçá o maior. Dessa forma, buscou-se assegurar direitos e garantias constitucionalmente estabelecidos aos titulares, em detrimento da crescente do capitalismo de vigilância e correspondente busca pelo superávit comportamental.

Nesse ínterim, estaríamos diante de uma ordem econômica ávida por aspectos das pessoas, extraídos, tratados e comercializados de modo a garantir a máxima eficiência produtiva do mecanismo tecnológico concebido pela disruptiva Revolução Industrial 4.0, vulnerando vários aspectos da segurança e da intimidade humanas.

Como se percebe, a presente atividade, já amplamente realizada no cotidiano atual, com perceptíveis impactos nos âmbitos sociais e econômicos, necessitava de uma regulamentação legal.

Nesse sentido, o tópico inaugural dissertará sobre a LGPD, suas acepções referentes aos fundamentos, conceitos terminológicos e principiológicos, promovendo uma apresentação panorâmica do dispositivo legal em estudo.

O segundo capítulo versará sobre a definição de responsabilidade civil, genericamente considerada, seus pressupostos, suas espécies, diferenciações e aplicabilidades, para, em seguida, aprofundar suas vertentes associadas à lei em análise.

O terceiro item fará um cotejamento da evolução legislativa do Diploma de Proteção, desde seus projetos de lei iniciais (Câmara dos Deputados e Senado Federal) e suas principais influências estrangeiras, momento em que se adentrará à parte derradeira do estudo, com abordagem das correntes doutrinárias e seus principais argumentos quanto à problemática principal do presente estudo, a saber, a natureza jurídica da responsabilidade civil dos agentes de tratamento de dados pessoais.

Pelo evidenciado acima, a presente exposição tem como objetivos específicos: a) apresentar os expedientes legislativos – nacional e estrangeiro – e socioeconômicos que influenciaram a edição da LGPD; b) expor a evolução da mentalidade doutrinária acerca da responsabilização civil no âmbito da LGPD; e c) expressar possíveis soluções em caráter de definitividade à omissão legislativa.

O método de abordagem a ser utilizado nessa pesquisa é o dedutivo, em que se pretende avançar no entendimento quanto à natureza jurídica da responsabilização que será imposta ao agente de tratamento em caso de descumprimento aos ditames expostos na lei de proteção.

Para tanto, se utilizará da técnica de pesquisa por meio da análise bibliográfica de textos nacionais e estrangeiros no campo do Direito sobre os temas "responsabilidade civil", "agentes de tratamento de dados pessoais", "proteção de dados"; "Lei nº 13.709/2018" e "LGPD".

2. A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS NUANCES SEMÂNTICAS E TERMINOLÓGICAS

Inicialmente, abordaremos aspectos importantes à compreensão da LGPD. Para tanto, seguiremos a ordem crescente de seus artigos, a co-

meçar por seus fundamentos, previstos em seu artigo 2º[29], momento em que, para fins pedagógicos, os dividiremos em blocos.

Os incisos I e IV são decorrentes da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, direitos e garantias assegurados pela Constituição Federal de 1988 (CF), em seu artigo 5º, inciso X, bem como pelo novel inciso LXXIX, recentemente acrescido pela Emenda Constitucional (EC) nº 115/2022, que giza: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

O disposto nos incisos III e VII encontra-se no mesmo diapasão magno, porém sem o predicado de fundamental, nos devidos termos do artigo 5º, IX, X e XII, da CF.

Em seguida, os incisos restantes – II, V e VI – representam a conciliação entre a viabilidade do progresso tecnológico, potencializado pela Quarta Revolução Industrial – marcada pelo advento de tecnologias que alteraram, em grande escala, as fases de produção e os modelos de negócio – e a conservação dos direitos dos titulares, consumidores em essência, de modo a conter o capitalismo de vigilância e sua busca pelo superávit comportamental, ofensivos à intimidade privada.

Outrossim, a autora Shoshana Zuboff[30] pontua que:

---

29 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

30 ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância.** A luta por um futuro humano na nova fronteira do poder. 1ª. Ed. Rio de Janeiro, RJ. Editora Intrínseca, 2021.

Nessa nova lógica, a experiência humana é subjugada aos mecanismos de mercado do capitalismo de vigilância e renasce como "comportamento". Este é transformado em dado, pronto para se juntar a uma fila infindável que alimenta as máquinas para fabricação de predições e eventual transação nos novos mercados futuros comportamentais.

A partir de então, passaremos a analisar alguns institutos jurídicos importantes à contextualização do objeto do presente estudo, previstos principalmente no artigo 5º da Lei de Proteção, a saber: dado pessoal, dado pessoal sensível, titular, agentes de tratamento, tratamento e autoridade nacional.

Conforme será explicado mais adiante, a LGPD possuiu substancial influência do Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD), em especial quanto à amplitude conferida ao dado pessoal, através de sua adjetivação "identificável", que, para além das informações que efetivamente identifiquem uma pessoa natural, também admite a compreensão de informações a ela relacionadas.

Já o subtipo dado pessoal sensível é aquele que se refere a aspectos existenciais e sociais, capazes de representar vultosa vulnerabilidade ou discriminação ao titular, pessoa natural proprietária dos dados pessoais objetos do tratamento.

Por sua vez, o gênero agente de tratamento de dados tem como espécies o operador, o controlador e o encarregado. O operador é o executor das deliberações referentes ao tratamento de dados pessoais tomadas pelo controlador, o mandante; logo, sobre este recaem as principais responsabilidades, inclusive referente ao ônus da prova sobre o consentimento do titular. Ao operador, restará a responsabilização solidária apenas quando o tratamento de dados afronte a LGPD, adiante (grifos adicionados):

> Art. 42. **O controlador ou o operador** que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patri-

monial, moral, individual ou coletivo, **em violação à legislação de proteção de dados pessoais**, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I – **o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador**, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II – **os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente**, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Ainda nessa senda, tem-se o encarregado, responsável pelos procedimentos de recebimento de comunicação oriunda dos titulares dos dados tratados, bem como pelo funcionamento como elo entre as espécies acima, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853/2019, órgão superior na seara da governança dos dados pessoais, com atribuição de zelar, implementar e fiscalizar o cumprimento da LGPD.

Por sua vez, o significado de tratamento é bastante vasto, tendo início desde a coleta do dado que será tratado, passando pelas possibilidades de seus manejos até, finalmente, sua eliminação.

Superada a etapa conceitual, passemos a seus princípios orientadores, previstos no artigo 6º, em suma: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, cuja inobservância pode gerar a imputação de penalidades, em caso de danos provocados em seus titulares.

Registre-se, por oportuno, que esse rol é meramente exemplificativo, conforme prescreve o artigo 64: “Os direitos e princípios expressos nesta

Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte".

A finalidade denota que o tratamento de dados deve se ater aos limites do informado ao titular, isto é, ao seu fim legítimo, garantindo-se, pois, o cumprimento da boa-fé da relação jurídica ora celebrada junto ao agente de tratamento.

A adequação é entendida como a pertinência entre a finalidade informada ao titular e o tratamento efetivamente realizado. Já a necessidade se revela como o limite imposto ao tratamento de dados, restrito ao mínimo necessário ao atingimento do objetivo previamente informado.

O livre acesso consubstancia-se na garantia de facilitação à consulta junto ao banco de dados onde se localizam os dados de cada titular. A qualidade dos dados evidencia a precisão, a clareza, a relevância e a atualização dos dados assegurados aos seus proprietários.

A transparência remete à clareza dos dados que estão sendo tratados e do agente responsável por tal atividade, excetuando-se os segredos comercial e industrial. A segurança e a prevenção designam a adoção de cautelas de ordem técnica e administrativa durante o tratamento de dados, sob pena de responsabilização dos agentes.

Por seu turno, a não discriminação significa a não admissão de práticas ilícitas e abusivas, alheias à ordem jurídica vigente. Por derradeiro, a responsabilização e prestação de contas expressam a necessidade de o agente obedecer a todas as exigências legalmente estabelecidas.

Superada essa etapa conceitual, passemos ao aspecto fulcral do presente estudo, o tema da responsabilidade civil, suas nuances doutrinárias, evolução legislativa e influência estrangeira.

3. RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

O instituto jurídico da responsabilidade civil pertence ao ramo do Direito Obrigacional, cuja função primordial é o restabelecimento do equilíbrio econômico e jurídico prejudicado pela ocorrência de algum evento danoso, posicionando a vítima em situação anterior à lesão, conforme apregoa o princípio da reparação integral, previsto na CF, em seu artigo 1º, III.

Nesse particular, importante a distinção semântica dos vocábulos obrigação, que traz consigo um dever jurídico originário, e responsabilidade, em que há um encargo jurídico sucessivo, isto é, sua existência está condicionada à violação prévia de uma obrigação já firmada.

Bruno Carrá[31] contribui com o tema, ao afirmar que (grifos adicionados):

> Eis a diferença entre obrigação e **responsabilidade civil, na medida em que esta é revelada através do descumprimento de uma regra obrigacional prévia**, porquanto repousa ou em disposição contratual anterior ou na cláusula geral de não prejudicar terceiros ("neminen laedere").

Em seus primórdios, nos idos do Código Civil (CC) de 1916, esse instituto se resumia ao artigo 159, com previsão expressa de a responsabilidade ocorrer mediante a comprovação de culpa (jaez subjetivo).

A evolução das complexidades referentes às relações humanas impeliu o legislador pátrio a conferir maior envergadura a tal instituto, a ponto de, com a adoção do CC de 2022, a esse instituto foi conferido um título (Da Responsabilidade Civil), dois capítulos (Da Obrigação de

31 CARRÁ, Bruno Leonardo Câmara. Aspectos das modalidades subjetiva e objetiva no sistema atual de responsabilidade civil brasileiro. **Revista Esmafe: Escola de Magistratura Federal da 5ª Região**, Recife, n. 11, p. 187-209, dez. 2006.

Indenizar e Da Indenização) e vinte e oito artigos (do 927 ao 954), com registro acerca das estirpes subjetiva e objetiva.

Como se percebe pelo exposto acima, para além da já existente classificação da responsabilidade civil em contratual e extracontratual – a depender da fonte do direito violado, se prevista em negócio jurídico preteritamente avençado ou se não estabelecido por vínculo formal, respectivamente – o CC vigente inovou ao assinalar as cepas subjetiva e objetiva, de acordo com a demonstração de culpa – *lato sensu*: ação ou omissão voluntária; ou *stricto sensu*: negligência, imperícia ou imprudência – ou não, tema que será objeto de análise do presente estudo e passaremos, então, a expor.

Iniciemos pela responsabilidade subjetiva, doutrinariamente denominada de Teoria da Culpa, considerada a regra geral no ordenamento jurídico pátrio, com fulcro no artigo 927 caput do CC de 2022, que pressupõe a comprovação de dolo ou culpa do infrator, sob pena de a indenização não ser juridicamente aceitável. Ademais, ainda se torna necessária a caracterização de pressupostos como ato ilícito, mediante conduta culposa, dano e nexo causal.

A primeira das premissas equivale ao procedimento humano e voluntário, podendo ser comissivo ou omissivo, de natureza antijurídica e suficiente a provocar o já mencionado desequilíbrio econômico e jurídico, ocasionando o dano (segundo pressuposto), conforme previsão do artigo 186 do CC, respectivamente nos trechos "Aquele que, por ação ou omissão voluntária, negligência ou imprudência" e "violar direito e causar dano a outrem".

Enfim, tem-se o nexo de causalidade, o elo referencial entre os elementos recém-mencionados, representado pela passagem "violar direito e causar dano a outrem" e que denota a individualização de materialidade do autor do dano, como também o alcance da responsabilidade a ser imputada.

Passemos à responsabilidade objetiva, também designada de Teoria do Risco, que tem como pressuposto-mestre o disposto no artigo 927, parágrafo único do CC de 2022. Apesar de prescindir do reconhecimento de culpa por parte do agente, possui as mesmas exigências quanto às premissas acima expostas, conforme aduz Sérgio Cavalieri Filho[32] (destaques inovados):

> [...] **também na responsabilidade objetiva teremos uma atividade ilícita, o dano e o nexo causal. Só não será necessário o elemento culpa**, razão pela qual fala-se em responsabilidade independentemente de culpa. Esta pode ou não existir, mas será sempre irrelevante para a configuração do dever de indenizar.

A doutrina de Flávio Tartuce[33] complementa esse raciocínio, na medida em que afirma ser a Revolução Industrial de 1850 e, em seguida, a expansão da globalização mundial responsáveis pela necessária reestruturação da responsabilidade civil (destacou-se):

> De acordo com a aclamada **teoria do risco** iniciaram-se os debates para a responsabilização daqueles que realizam determinadas atividades em relação à coletividade. Verificou-se, **a par dessa industrialização**, uma maior atuação estatal, bem como a exploração em massa da atividade econômica, o que **justificou a aplicação da nova tese de responsabilidade sem culpa.** Mesmo com resistências na própria França, a teoria da responsabilidade sem culpa prevaleceu no direito alienígena, atingindo também a legislação do nosso país.

Passo adiante, entre os diversos diplomas legislativos que versam sobre responsabilidade civil, daremos ênfase ao Código de Defesa do Consumidor (CDC), que adotou a Teoria do Risco como regra geral para fins da indenização dos fornecedores de produtos e serviços, sob o argumen-

32 CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil.** 15ª Ed. São Paulo: Grupo GEN, 2022.

33 TARTUCE, Flavio. Direito Civil - **Direito das Obrigações e Responsabilidade Civil**. 17ª Ed. Vol. 2. Rio de Janeiro: Grupo GEN, 2022.

to de que o consumidor ocupa posição de hipossuficiência. A fundamentação para tanto reside no disposto em seus artigos 12 (responsabilidade pelo fato do produto), 14 (responsabilidade pelo fato do serviço), 18, 19 e 20 (responsabilidade pelo vício do produto e do serviço).

No entanto, tal Códex também prevê, em caráter excepcional, a categoria subjetiva quanto ao fato do serviço realizado pelos profissionais liberais, conforme destacado adiante: "Art. 14. § 4° A responsabilidade pessoal dos profissionais liberais será apurada **mediante a verificação de culpa**".

4. ASPECTOS LEGISLATIVOS E DOUTRINÁRIOS À APLICAÇÃO DA RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

A partir de então, abordaremos aspectos referentes à evolução legislativa da LGPD, primeiro dispositivo legal brasileiro destinado exclusivamente ao regramento do tratamento de dados pessoais, desde a discussão na Câmara dos Deputados e no Senado Federal, inclusive com a participação da sociedade civil e influências internacionais, até o momento pós-vigência da lei e consequentes discussões jurídicas, em especial quanto à ausência de previsão expressa quanto à natureza da responsabilização dos agentes de tratamento de dados.

Conforme a doutrina de Danilo Doneda[34], o impulso para início da disposição legislativa nacional acerca do tema proteção de dados ocorreu em decorrência do I Seminário Internacional sobre Proteção de Dados Pessoais, realizado em 2005, com elaboração de documento formal rati-

34 DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. *In*: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021.

ficado pelos países-membros do Mercado Comum do Sul (MERCOSUL) cinco anos após, denominado "Medidas para a Proteção de Dados Pessoais e sua Livre Circulação".

Em novembro de 2010, o Ministério da Justiça brasileiro oportunizou a participação da sociedade civil, para fins de obter plúrimas colaborações ao desenvolvimento de projeto de lei hábil a versar sobre tratamento de dados pessoais em território nacional.

Na seara da Câmara dos Deputados, em 13/06/2012, propôs-se o Projeto de Lei (PL) nº 4.060/2012[35], com registro de tratamento de dados pessoais e outras providências. Anos após, em 13/05/2016, o Poder Executivo, através da Casa Civil, protocolou o PL nº 5.276/2016[36], com ementa sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, que, posteriormente, veio a ser apensado ao Projeto inaugural.

Daí em diante, a matéria ganhou ainda mais envergadura e passou a ser conduzida pela Comissão Especial de Tratamento e Proteção de Dados Pessoais da Câmara dos Deputados, que organizou nova série de audiências públicas, com ampla participação popular.

A título de exemplo, citamos o Manifesto sobre a Futura Lei de Proteção de Dados[37], datado de setembro de 2016, subscrito pela Associação Brasileira de Internet (ABRANET), pela Associação Brasileira de Emissoras de Rádio e Televisão (ABERT), pela Federação das Associações das Empresas Brasileiras de Tecnologia da Informação e Comunicação (ASSESPRO), pela Câmara Brasileira de Comércio Eletrônico (CAMARA-E.NET) e por mais de uma dezena de outras entidades representativas de classe.

35 https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066

36 https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378

37 https://www.abranet.org.br/Noticias/Em-manifesto,-Abranet-e-outras-entidades-pedem-criacao-de-autoridade-para-fiscalizar-lei-de-protecao-de-dados-1246.html?UserActiveTemplate=site

O mencionado texto apresentou algumas irresignações e sugestões, tais como: a criação de uma autoridade federal com autonomia e capacidade de interpretação, fiscalização quanto ao cumprimento das pertinentes normas legais; e averiguação e responsabilização individualizadas da atuação do agente de tratamento de dados, de modo que cada um responda dentro do seu limite de atribuição, sem a imposição de reprimenda objetiva e solidária.

Ainda nesse diapasão colaborativo, o Instituto Brasileiro de Defesa do Consumidor (IDEC) confeccionou documento[38] em dezembro de 2016, se posicionando contra o Manifesto acima aludido, em especial quanto à necessidade de responsabilização solidária dos agentes de tratamento de dados pessoais, quando inseridos em uma mesma cadeia de fornecedores de serviços, nos mesmos moldes do microssistema jurídico criado pelo CDC e já amplamente consagrado pelo Superior Tribunal de Justiça (STJ), nos termos da paradigmática decisão abaixo (grifos adicionados):

> O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), **pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis** (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

(Recurso Especial 1419697/RS, Segunda Seção, Relator Ministro Paulo de Tarso Sanseverino)

Após intensa participação da sociedade, o PL nº 4.060/2012 foi aprovado em 29/05/2018 e encaminhado ao Senado Federal, sob a referência de Projeto de Lei da Câmara (PLC) nº 53/2018[39].

38 https://idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf

39 https://www25.senado.leg.br/web/atividade/materias/-/materia/133486

Sob alçada da Câmara Alta do Congresso Nacional já tramitavam três Projetos de Lei do Senado (PLS), sob os números 330/2013[40], 131/2014[41] e 181/2014[42], que, inicialmente, passaram a tramitar de forma conjunta. Com o recebimento do PLC nº 53/2018, todos os projetos foram enviados à Comissão de Assuntos Econômicos, que decidiu pela aprovação deste e pela prejudicialidade dos três PLSs.

Em meio a todas essas discussões parlamentares brasileiras, em 23/05/2018, foi aprovado na europa o Regulamento Geral da Proteção Geral de Dados (RGPD), que, em seus artigos 1º e 2º, respectivamente, "estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (...) e defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais" com pertinência "ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União" [43].

Afora o aspecto diplomático, o Regulamento Europeu também buscou impactar a comunidade internacional no âmbito econômico, na medida em que passou a exigir que a transferência de dados de países da União Europeia a outros não pertencentes ao Eixo estaria vinculada à comprovação de um nível de proteção adequado (grifos adicionados):

> Art. 45. **Pode ser realizada uma transferência de dados pessoais para um país terceiro** ou uma organização internacional **se a Comissão tiver decidido que o país terceiro**, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, **assegura um nível de proteção adequado.** Esta transferência não exige autorização específica.

40 https://www25.senado.leg.br/web/atividade/materias/-/materia/113947

41 https://www25.senado.leg.br/web/atividade/materias/-/materia/116969

42 https://www25.senado.leg.br/web/atividade/materias/-/materia/117736

43 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

Em vista disso, o RGPD é considerado o estímulo decisivo aos legisladores brasileiros, tanto que, já em 05/07/2018, o PLC nº 53/2018 foi aprovado pelo plenário do Senado Federal e, posterior à sanção presidencial, em 14/08/2018, convertido na Lei nº 13.709/2018, inclusive reproduzindo idêntica concepção do Velho Mundo, como a ausência de previsão expressa da natureza jurídica da responsabilidade civil em análise.

Adentrando à realidade nacional, adstrita à LGPD, a responsabilidade civil está expressa na Seção III (Da Responsabilidade e do Ressarcimento de Danos), nos artigos 42 a 45, em que que, já no caput do artigo inaugural, tem-se a norma geral do instituto em análise.

Mais adiante, o legislador estabeleceu hipóteses de responsabilidade solidária entre controlador e operador (artigo 42, § 1º, I e II), as respectivas excludentes (artigo 43) e a possibilidade de inversão do ônus da prova em benefício ao titular dos dados pessoais em tratamento (artigo 42, § 2º).

Considerando a omissão do legislador em relação à natureza jurídica da responsabilidade civil dos agentes de tratamento de dados pessoais na LGPD, importante abordar as várias correntes tipificações acerca do tema.

A Corrente Subjetivista apregoa a necessidade da demonstração de culpa, além dos pressupostos elementares: conduta ilícita violadora do disciplinamento do tratamento de dados pessoais, dano patrimonial ou extrapatrimonial ao titular e nexo de causalidade entre ambos.

Os principais argumentos dos que defendem a Teoria da Culpa são os seguintes: a um, ausência de menção expressa sobre a responsabilidade objetiva, atraindo a regra geral prevista no artigo 927 caput do CC de 2002, que versa sobre a modalidade subjetiva, o que novamente revela a grande influência que o RGPD teve sobre a LGPD, na medida em que ambos os dispositivos foram omissos no tocante à natureza jurídica referente aos agentes de tratamento de dados, conforme se vê abaixo:

> RGPD. Art. 82, 1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.
>
> LGPD. Art. 42, caput. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A dois, registro quanto à subsunção ao CDC, de natureza excepcional, no artigo 45 da LGPD, quando pertinentes às relações consumeristas. A três, previsão de condutas hábeis a modular eventual responsabilização dos agentes de tratamento (*standard* comportamental), a exemplo da segurança, do sigilo, das boas práticas e da governança de dados (artigos 46 a 51 da LGPD).

A quatro, risco de desaceleração do progresso tecnológico em caso do reconhecimento do viés objetivo, caso contrário, haveria um temor generalizado quanto às indenizações cabíveis. Nesse diapasão, a observância da liturgia do princípio da culpa seria importante à condução de que os agentes seguissem os padrões legalmente estabelecidos.

A cinco, pertinente à proteção de dados não existe nenhuma norma legal no sentido da responsabilidade civil objetiva, de modo que "em todas as situações jurídicas que o legislador excepcionou a regra da responsabilidade subjetiva, o fez de modo expresso e inequívoco"[44].

A seis, pela leitura dos cinco projetos de lei mencionados no início do capítulo, percebe-se que, salvo no PL nº 4.060/2012 e no PLS nº 131/2014, o tema responsabilidade civil dos agentes de tratamento de dados pessoais possui previsão expressa, de modo que a retirada des-

44 TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 97-115, Janeiro-Março/2020.

sa patente indicação, em especial do PL nº 5.276/2016, que inspirou a versão final da LGPD, é entendida como uma clara menção do legislador pelo entendimento subjetivo da responsabilização, senão vejamos (grifos adicionados):

- **PLS nº 330/2013, Capítulo XI: Da Responsabilidade Civil**
  - Art. 14. Qualquer pessoa que sofra prejuízo decorrente do tratamento irregular ou ilícito de dados possui direito à reparação dos danos, materiais e morais.
  - § 1º A responsabilidade do proprietário, do usuário, do gestor e do gestor aparente de banco de dados, quando houver, independe da verificação de culpa.
  - § 2º O tratamento de dados realizado de forma associativa ou por qualquer outra forma, ainda que informal, acarreta a responsabilidade solidária e direta de todos os agentes envolvidos.
  - § 3º O disposto neste artigo não exclui outras hipóteses de responsabilidade previstas em lei.
- **PLS nº 181/2014, Capítulo I: Do Regime Jurídico do Tratamento de Dados Pessoais. Seção I: Das Regras para Tratamento de Dados Pessoais**
  - Art. 17. Aquele que, por tratamento inadequado de dados pessoais, causar dano material ou moral, individual ou coletivo, comete ato ilícito e obriga-se a ressarci-lo.
  - Parágrafo único. A atividade de tratamento de dados pessoais é de risco e os seus responsáveis respondem, independentemente da existência de culpa, pela reparação dos danos causados aos titulares ou a terceiros.
- **PL nº 5.276/2016, Seção II (Responsabilidade) e Seção III (Responsabilidade e Ressarcimento de Danos)**
  - Art. 35. O cedente e o cessionário respondem solidária e objetivamente pelo tratamento de dados, independentemente do local onde estes se localizem, em qualquer hipótese.

- Art. 42. Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo.

- Parágrafo Único. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados, quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

- Art. 43. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

- Art. 44. Nos casos que envolvam a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

- Parágrafo único. A responsabilidade solidária não se aplica aos casos de tratamento realizado no exercício dos deveres de que trata a Lei nº 12.527, de 2011, relativos à garantia do acesso a informações públicas.

Guinando à Corrente Objetivista, essa modalidade independe da configuração de culpa pelo agente causador do dano, bastando a presença dos pressupostos elementares: conduta ilícita, dano e nexo causal.

Os defensores da Teoria do Risco baseiam-se em: a) as excludentes de responsabilidade previstas no artigo 43 da LGPD não se referem à culpa, nem mesmo em sua acepção *lato*; b) a operação de tratamento de dados pessoais, por si só, já é dotada de risco intrínseco, por tutelar direito e garantia fundamental da proteção de dados pessoais, acrescido pela Emenda Constitucional (EC) nº 115/2022, hábil a atrair a aplicação do disposto no artigo 927, parágrafo único do CC de 2022; c) não existência de ameaça à alavancagem do desenvolvimento tecnológico, pois o mesmo expediente já fora reproduzido no CDC, sem qualquer registro de involução nesses trinta e dois anos seguintes; e d) entendimento do

Conselho da Justiça Federal, expresso no Enunciado nº 448 da V Jornada de Direito Civil[45].

Perpassando à Corrente Dualista, a exemplo da previsão do Código Consumerista, replicada no artigo 45 da LGPD, os doutrinadores militam no sentido de a análise precisar ser realizada de acordo com o caso concreto, podendo ora ter natureza subjetiva, ora tendo natureza objetiva, de acordo com o risco da especificidade da atividade de tratamento desempenhada.

Nesse ínterim, no particular da indenização, o CDC adota a regra geral de responsabilidade objetiva. No entanto, prevê a possibilidade da natureza subjetiva, quando o fato do serviço for prestado por profissionais liberais, nos devidos termos do artigo 14, § 4º.

Assim, os fundamentos se seus defensores são: a) diante da ausência de previsão expressa na LGPD sobre a natureza jurídica da responsabilização dos agentes de tratamento de dados pessoais, deve prevalecer a regra geral do viés subjetivo, porém, a análise há de ser realizada casuisticamente, sem exclusão da possibilidade de adoção da perspectiva objetiva, caso assim a particularidade analisada exigir; e b) nem toda atividade de tratamento traz consigo o caráter do risco, o que atrairia a imputação subjetiva, porém, quando o risco estivesse presente, o feitio objetivo haveria de preponderar.

45 A regra do art. 927, parágrafo único, segunda parte, do CC aplica-se sempre que a atividade normalmente desenvolvida, mesmo sem defeito e não essencialmente perigosa, induza, por sua natureza, risco especial e diferenciado aos direitos de outrem. São critérios de avaliação desse risco, entre outros, a estatística, a prova técnica e as máximas de experiência.

5. CONCLUSÃO

O presente trabalho abordou aspectos relevantes acerca natureza jurídica da responsabilidade civil no âmbito da LGPD. Para se chegar ao objeto da indagação principal, percorreu-se pela evolução parlamentar e pelos entendimentos doutrinários referentes ao tema, além da abordagem de seus pressupostos, definições, espécies e princípios.

Nesse movimento, abordou-se sobre o vultoso avanço evolutivo trazido pela Quarta Revolução Industrial, em especial no tocante às tecnologias de automação industrial, dotada de inteligência artificial, que, através da manufatura digital, se tornou capaz de promover a predição de comportamentos humanos e transformá-los em valiosos ativos, potencialmente lesivos aos interesses individuais de seus titulares.

Em seguida, avançou-se mais detidamente à cronologia dos projetos de lei e da versão definitiva da LGPD, fortemente influenciada pela doutrina europeia, que, pouco antes, havia concebido o RGPD, inclusive com a imposição de restrições a países não membros de sua Comunidade no tocante à transferência e o compartilhamento do tratamento de dados pessoais, caso não houvesse prévia comprovação de segurança quanto à adequação do nível de segurança desse mister.

Passo adiante, adentrou-se à responsabilização no âmbito específico da lei brasileira, inclusive com a apresentação de três teorias doutrinárias que se habilitaram a suprir a lacuna legislativa nesse particular, a saber: subjetiva ou da culpa, objetiva ou do risco e dualista, com ênfase no microssistema consumerista.

Realizado o cotejamento de todos os itens acima, enunciou-se que o ordenamento pátrio adota a modalidade subjetiva como regra, nos devidos termos do artigo 927, caput do CC de 2002, embora também possua aplicabilidade, quando dotado de previsão expressa e inequívoca, do jaez objetivo, com fulcro no artigo 927, § 1º do Códex Civil.

No entanto, a recente e veloz complexidade com que as relações humanas estão sendo travadas nos conduz ao entendimento de que a estirpe que melhor regule tal realidade seja a dualista, na medida em que a espécie subjetiva seria a regra geral, com modulação à objetiva, mediante necessária análise casuística, de modo que, caso a atividade desempenhada envolva risco intrínseco, a responsabilidade do agente de tratamento há de ser entendida pela vertente objetiva, independentemente da comprovação do elemento culpa.

Para solucionar esse vácuo legislativo e o impasse hermenêutico relativo à responsabilização estudada, e assim conferir segurança jurídica no que tange a resolução de contendas concretas, o recomendável seria haver uma complementação à LGPD, uniformizando a intenção do legislador à intenção da lei. Caso contrário, apenas o amadurecimento das decisões judiciais poderá resolver essa cizânia ainda existente no ordenamento jurídico brasileiro.

6. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE INTERNET. **Manifesto sobre a futura lei de proteção de dados pessoais.** Disponível em: https://www.abranet.org.br/Noticias/Em-manifesto,-Abranet-e-outras-entidades-pedem-criacao-de-autoridade-para-fiscalizar-lei-de-protecao-de-dados-1246.html?UserActiveTemplate=site. Acesso em 11 set. 2022.

BRASIL. **Projeto de Lei da Câmara n° 53,** 1º de junho de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em 11 set. 2022.

_____. **Projeto de Lei do Senado n° 181,** 20 de maio de 2014. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados

pessoais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/117736. Acesso em 11 set. 2022.

_____. **Projeto de Lei do Senado nº 131**, 16 de abril de 2014. Dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/116969. Acesso em 11 set. 2022.

_____. **Projeto de Lei do Senado nº 330,** de 13 de agosto de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em 11 set. 2022.

_____. **Projeto de Lei nº 4.060/2012,** de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em 11 set. 2022.

_____. **Projeto de Lei nº 5.276/2016,** de 13 de junho de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em 11 set. 2022.

CARRÁ, Bruno Leonardo Câmara. Aspectos das modalidades subjetiva e objetiva no sistema atual de responsabilidade civil brasileiro. **Revista Esmafe: Escola de Magistratura Federal da 5ª Região**, Recife, n. 11, p. 187-209, dez. 2006.

CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 15ª Ed. São Paulo: Grupo GEN, 2022.

COMISSÃO EUROPÉIA. **A proteção de dados na UE**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt. Acesso em 26 set. 2022.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais.** In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais.** 1. ed. Rio de Janeiro: Forense, 2021.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Audiência pública sobre Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, de 2012.** Disponível em: https://idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf. Acesso em 11 set. 2022.

TARTUCE, Flavio. Direito Civil - **Direito das Obrigações e Responsabilidade Civil**. 17ª Ed. Vol. 2. Rio de Janeiro: Grupo GEN, 2022.

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor.** Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 97-115, Janeiro-Março/2020.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância.** A luta por um futuro humano na nova fronteira do poder. 1ª. Ed. Rio de Janeiro, RJ. Editora Intrínseca, 2021.

Dados pessoais como ativo na sociedade da informação: a LGPD como instituição e suas interações nas livres iniciativa e concorrência

Personal data as an asset in the information society: the brazilian gdpr as an institution and its interactions in the free iniciative and competition

Carlos Eduardo Pinheiro da Silva

» Mestrando em Direito Constitucional pela Universidade Federal do Ceará (UFC). Pós-graduado em Direito Público pela Universidade Vale do Acaraú (UVA). Graduado em Direito pela Universidade de Fortaleza (UNIFOR). Advogado.

» E-mail: epinheiroadv@hotmail.com

Álisson José Maia Melo

» Professor Titular de Direito Empresarial e professor permanente do Programa de Pós-Graduação em Direito do Centro Universitário 7 de Setembro (UNI7). Doutor em Direito pela Universidade Federal do Ceará (UFC). Especialista em Direito Tributário pela UNI7. Analista da Agência Reguladora do Ceará (ARCE). Advogado.

» E-mail: alisson@uni7.edu.br

Recebimento: 01/09/2022
Aprovação: 27/10/2022

REVISTA JURÍDICA DO BANCO DO NORDESTE

RESUMO

O presente artigo contextualiza os dados pessoais como ativos da economia digital, para investigar os pontos de conexão da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) com o fundamento constitucional da livre iniciativa e com o princípio da livre concorrência, constantes no artigo 170 da Constituição Federal de 1988. Para tanto, expõe-se a evolução dos ativos econômicos, contextualizando o tratamento dos dados pessoais na obtenção de riquezas pelas organizações. Em seguida, efetua-se uma análise da política nacional de proteção dos dados pessoais, com a edição da LGPD e o reconhecimento do direito fundamental à proteção dos dados pessoais. Por fim, analisa-se como a LGPD influencia os princípios da livre iniciativa e concorrência. Conclui-se que a LGPD é um importante instituto de controle e garantia da ordem econômica.

PALAVRAS-CHAVE

Lei Geral de Proteção de Dados (LGPD). Dados Pessoais. Política de proteção. Atividade Econômica.

ABSTRACT

This paper contextualizes personal data as assets of the digital economy, in order to investigate the connection points of the Brazilian General Data Privacy Regulation (Law 13.709/2018) with the constitutional foundation of free enterprise and the principle of free competition, contained in the article 170 of the Federal Constitution of 1988. To this end, it exposes the evolution of economic assets, contextualizing the treatment of personal data in obtaining wealth by organizations. Then, it carries out an analysis of the Brazilian policy for the protection of personal data, with the edition of the Brazilian GDPR and the recognition of the

fundamental right to the protection of personal data. Finally, it analyzes how Brazilian GDPR influences the principles of free enterprise and competition. It concludes that this regulation is an important institute of control and guarantee of the economic order.

PALAVRAS-CHAVE

Brazilian General Data Privacy Regulation. Personal data. Protection policy. Economic activity.

SUMÁRIO

1. INTRODUÇÃO

Na sociedade contemporânea, a informação é um bem precioso, cuja manipulação é capaz de alterar situações e costumes existentes há séculos. A capacidade computacional de efetuar a análise de dados em larga escala – o que se convencionou chamar de *Big Data* – e extrair desses dados informações úteis para as mais diversas atividades, modificou significativamente a economia e a sociedade[46].

A noção clássica de mercado, no sentido de um espaço físico composto por um conjunto de compradores e vendedores que realizam trocas, vem sendo ultrapassada na era da globalização, pelo uso de ferramentas tecnológicas como a *internet* e pela economia digital. Sem prejuízo, prevalece a concepção de que o mercado contemporâneo se configura como um ambiente de realizações das atividades econômicas, moldado por opções políticas que formulam as regras do jogo[47].

Para a conceituação de mercado, acima destacada, utiliza-se a lição de Douglass C. North[48] sobre as instituições, assim entendidas "as restrições concebidas pelo homem que moldam a interação humana" formatadas em corpos de regras voltados para o cumprimento de determinados objetivos da unidade que se forma (instituição). As instituições conferem uma estrutura de regras previamente definidas e, por isso, reduzem as incertezas nos cenários sociais, entre os quais o econômico.

Dessa forma, nesse mercado com contornos modernos, os dados pes-

46 JIMÉNEZ SERRANÍA, Vanessa; ABRUSIO, Juliana. Big data: uma análise sob a óptica das práticas abusivas no acesso e uso de dados massificados na economia de plataforma. **Revista de Direito Brasileira**, Florianópolis, v. 28, n. 11, p. 387-404, jan./abr. 2021, p. 390).

47 MATIAS, João Luis Nogueira. **A função social da empresa e a composição de interesses na sociedade limitada**. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

48 NORTH, Douglas C. **Instituiçoes, mudança institucional e desempenho econômico**. Tradução de Alexandre Morales. São Paulo: Três Estrelas, 2018, p. 13.

soais tornam-se ativos econômicos capazes de gerar grandes fortunas a pessoas e organizações, que passam a os tratar com finalidade lucrativa. Entretanto, para além das riquezas que pode gerar, o tratamento de dados pessoais pode colocar em risco não apenas a privacidade dos seus titulares, mas vários outros direitos e garantias. Ademais, proporcionam, pelo aumento da esfera de influência das organizações e seu poderio econômico, uma crescente ameaça à ordem econômica e financeira.

O presente artigo investiga, portanto, a consideração dos dados pessoais como ativo econômico, bem como a preocupação do governo brasileiro na construção de uma política de proteção e regulamentação do tratamento desses dados.

O objetivo geral da pesquisa é trazer impactos da Lei Geral de Proteção de Dados (LGPD) no fundamento da ordem econômica e nos princípios constitucionais da livre iniciativa e da livre concorrência.

A pesquisa adota o método de abordagem dedutivo, valendo-se de modo auxiliar da análise bibliográfica e documental, buscando explorar obras especializadas e artigos científicos nacionais e estrangeiros, bem como a busca de dados secundários, para a apreciação da legislação constitucional e infraconstitucional nacional. Nesse sentido, o desenvolvimento está dividido em três seções, partindo-se inicialmente da análise mais ampla do contexto da sociedade da informação e como os dados pessoais passam a ser compreendidos como ativos econômicos. Em um segundo momento, põe-se sob exame a legislação brasileira para tratamento de dados pessoais e a emergência da identificação de um novo direito fundamental, como consequência disso. Ao final, avalia-se a LGPD como instrumento para estimular a livre iniciativa *vis a vis* garantir a livre concorrência.

2. A SOCIEDADE DA INFORMAÇÃO: DADOS PESSOAIS COMO ATIVO ECONÔMICO

Na Europa feudal, por volta do século X, a terra era a chave de toda a riqueza. A fortuna de um homem era determinada pela quantidade de terra que ele detinha, e, por ser a maior proprietária de terras, a Igreja era a instituição mais rica da época[49].

Embora a Idade Média seja um período vasto na História, com grandes variações geográficas e mudanças de contexto ao longo de dez séculos, pode-se afirmar que, especialmente na fase arcaica ou alta, a atividade comercial nesse período era bastante limitada, estando basicamente restrita aos feudos num contexto de economia de subsistência e funcionando por meio do escambo de mercadorias com vistas ao autoabastecimento das comunidades[50]. Várias eram as amarras que impediam o avanço do comércio. As moedas eram poucas e variavam de local para local, os pesos e as medidas também não tinham um padrão, e o transporte de pessoas e de mercadorias era perigoso, caro e penoso[51].

Entretanto, a considerável inexistência da atividade comercial fora modificada com as cruzadas, as quais criaram um enorme mercado consumidor para a época, pela necessidade de provisões, roupas, armamentos, cavalos, entre outros produtos. Surgiu, dessa forma, uma nova demanda, aumentando a quantidade de produtos disponíveis e o fluxo de troca de valores. Criou-se, por assim dizer, um mercado consumidor onde antes não existia, e surgiu também a necessidade e a importância do dinheiro, o qual era mais fácil de ser manuseado do que as mercadoriais anteriormente utilizadas para a troca. Com a expansão da prática

49 HUBERMAN, Leo. **História da Riqueza do homem**. 16. ed. Rio de Janeiro: Zahar, 1981, p. 19-22.

50 FREIRE, Ana Lucy Oliveira. O desenvolvimento do comércio e a produção do espaço urbano. **GeoTextos**, v. 6, n. 2, p. 11-32, dez. 2010, p. 18-19.

51 HUBERMAN, 1981, p. 27

mercante, a riqueza deixou de ser medida somente pela propriedade da terra, para ser medida também em dinheiro[52].

Dando um salto na história, do século X ao século XXI, com o avanço e a consolidação do sistema econômico capitalista, continuamos a presenciar o domínio e a força do dinheiro na economia, oriundo em grande parte da atividade comercial. O transporte de pessoas e bens tornou-se mais seguro e barato, mercados antes distantes e inacessíveis hoje são facilmente frequentados e disputados comercialmente. A globalização, enquanto processo antigo de integração internacional, avançou a passos largos com o desenvolvimento de novas tecnologias[53].

No mundo já globalizado, em 1969 surgiu a *internet*, a qual, aliada a já existente capacidade de processar dados em grandes escalas, modificou para sempre nosso modo de vida, e obviamente, a economia[54]. O uso das tecnologias, a possibilidade de análise da informação em grande escala, sua utilização para novos bens e serviços, e a globalização são as características do que Manuel Castells[55] chamou de economia informacional.

Em 2006, o matemático britânico Clive Humby cunhou a frase "dados são o novo petróleo"[56], no sentido comparativo do seu valor econômico no novo cenário mundial. Assim como o petróleo, os dados têm de ser coletados e processados para deles se extrair valor.

Na descomunal vastidão das informações coletadas e tratadas, en-

52 HUBERMAN, 1981, p. 36.

53 HARARI, Yuval Noah. **Sapiens:** uma breve história da humanidade. L&PM, 2015.

54 ARTESE, Gustavo. Compliance digital e privacidade. In: CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI, Rodrigo; VENTURINI, Otavio (Coord.). **Manual de Compliance**. 2. ed. Rio de Janeiro: Forense, 2020, p. 455-480.

55 CASTELLS, Manuel. **A Sociedade em Rede.** v. I. 6. ed. São Paulo: Paz e Terra, 1999.

56 ARTHUR, Charles. Tech giants may be huge, but nothing matches big data. **The Guardian**, International edition, Technology, 23 ago. 2013.

contram-se os dados pessoais, quais sejam, todos aqueles capazes de tornar uma pessoa natural identificada ou identificável, nos termos da definição trazida pelo artigo 5º, I, da Lei Geral de Proteção de Dados Pessoais (LGPD)[57].

Em qualquer aspecto da vida cotidiana, nossos dados pessoais são tratados. Nesse sentido, deve-se entender por tratamento, conforme o artigo 5º, X, da LGPD, todas as operações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Em resumo, tudo o que pode ser realizado com um dado pessoal pode ser caracterizado como tratamento.

Dados pessoais, portanto, passam a ser *commodities* no que se denomina de economia digital. Em pesquisa realizada no ano de 2021, as sete empresas mais valiosas ou são da área de tecnologia, ou realizam a sua atividade econômica com forte tratamento de dados pessoais[58]. Isso ocorre especialmente em relação aos dados voltados para a publicidade segmentada, modalidade pela qual as ofertas, de produtos e serviços, são dirigidas para um público previamente delimitado e que fora selecionado com base no tratamento dos seus dados pessoais, muitas vezes de forma desconhecida pelos próprios titulares dos dados.

Ainda segundo a pesquisa acima, as três primeiras empresas possuem, em conjunto, um valor de mercado avaliado em aproximadamente US$ 1,8 trilhão, o qual, apenas para efeitos comparativos, é maior do que o PIB brasileiro em dólar no ano de 2020[59].

---

57 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 15 de agosto de 2018.

58 KANTAR. **Kantar BrandZ:** 2021 most valuable global brands. London: Kantar Brandz, 2021.

59 ALVARENGA, Darlan; SILVEIRA, Daniel. PIB do Brasil despenca 4,1% em 2020. **G1**, Economia, 3 mar. 2021.

Importante destacar que, das dez mais valiosas empresas, duas delas, o *Google* e o *Facebook*, não cobram nada dos usuários pela sua utilização. Esse fato ilustra muito bem um jargão comum na área, segundo o qual "se você não paga pelo produto, o produto é você"[60], lição que reforça o valor dos dados pessoais tratados e negociados como ativo econômico por essas empresas. Dessa forma, além de dispor de uma excelente infraestrutura tecnológica, essas grandes corporações possuem uma enorme quantidade de agentes que lhes fornecem, de forma graciosa, voluntariosa e indiscriminada, dados pessoais e conteúdo, a saber, os próprios titulares dos dados, através de um novo mecanismo e lógica de extração do valor, chamado por Hamid Ekbia[61] de heteromação.

Perfis com dados pessoais de titulares são vendidos no mercado, como no caso ocorrido em 2020 envolvendo o Serasa S.A., quando a empresa fora proibida, por decisão liminar em processo no Tribunal de Justiça do Distrito Federal e Territórios[62], de vender dados pessoais diversos, tais como informações para contatos, sexo, idade e até endereços de seus titulares, ao custo de R$ 0,98 (noventa e oito centavos) por perfil, possuindo aquela empresa cerca de 150 (cento e cinquenta) milhões desses perfis.

Existe um novo mercado na economia mundial, o mercado de dados pessoais, o qual pode ser entendido como as "interações econômicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente"[63].

---

60 CARNEIRO, Felipe. O produto é você. **Veja,** Economia, 26 out. 2018.

61 EKBIA, Hamid R.; NARDI, Bonnie. **Heteromation, and other stories of computing and capitalism.** Cambridge: MIT Press, 2017.

62 DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios (2ª Turma Cível). **Agravo de Instrumento nº 0749765-29.2020.8.07.0000.** Agravante: Ministério Público do Distrito Federal e Territórios. Agravado: SERASA S.A. Relator: Desembargador Cesar Loyola. Acórdão nº 1341840, julgado em 26 maio 2021.

63 SILVEIRA, Sérgio A.; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc**, Rio de Janeiro, v. 12, n. 2, p. 217-230, nov. 2016.

Possuir grandes bancos de dados pessoais, e ter a capacidade de processá-los para deles extrair informações valiosas, significa um enorme e magnífico poder na sociedade contemporânea[64], representando essa capacidade, por sua enorme relevância social e econômica, um considerável risco às liberdades individuais dos cidadãos[65], bem como ao princípio da livre concorrência, constante no artigo 170, IV, da Constituição Federal[66].

Nesse diapasão, passa a ser uma missão estatal elaborar balizas para o adequado manejo dessas *commodities* tão sensíveis nos tempos digitais em que vivemos.

3. A EVOLUÇÃO LEGISLATIVA BRASILEIRA PARA A PROTEÇÃO DOS DADOS PESSOAIS: O RECONHECIMENTO DE UM NOVO DIREITO FUNDAMENTAL

A despeito de a proteção de dados pessoais ter se tornado mais visível a partir do ano de 2018, com a publicidade dada à LGPD, o Estado brasileiro já possui um histórico legislativo no sentido de preservação da privacidade das informações pessoais e do reconhecimento da proteção de dados pessoais como direito fundamental.

Tendo como ponto de partida o período posterior a promulgação da Carta Magna de 1988, encontramos no texto constitucional a dignidade da pessoa humana como fundamento da República (art. 1º, III, da CF/88). Para além disso, há também direitos constitucionais que se relacionam intimamente ao tema tratado nesse estudo, como:

64 ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.

65 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: RT, 2020.

66 BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República, 1988.

a) a garantia constitucional de inviolabilidade da intimidade;

b) a vida privada;

c) a imagem (art. 5º, X, da CF/88);

d) a garantia da inviolabilidade;

e) o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII, da CF/88);

f) a proteção da casa como asilo inviolável do indivíduo (art. 5º, XI, da CF/88); e

g) a possibilidade da concessão de *habeas data* para se garantir o acesso a informações relativas a pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, garantindo-se ainda a retificação dos dados (art. 5º, LXXII, a e b, da CF/88).

Todo o arcabouço constitucional acima delineado possui relação com a proteção de dados pessoais, ao resguardarem a privacidade, o sigilo de informações e seu respectivo acesso, inclusive com a possibilidade de corrigir dados que estejam sem qualidade.

A Lei nº 8.078, de 11 de setembro de 1990, mais conhecida como Código de Defesa do Consumidor (CDC), já demonstrava preocupação com a coleta e o uso de dados dos consumidores, incluindo seus dados pessoais. O CDC prevê, em seu artigo 43, várias regras para a criação e manutenção de bancos de dados e cadastros de consumidores. Posteriormente, entraram em vigência as Lei nº 12.414, de 9 de junho de 2011, a Lei do Cadastro Positivo, e a Lei nº 12.527, de 18 de novembro de 2011, mais conhecida como Lei de Acesso à Informação. Ambas tratavam da utilização de dados e privacidade, porém esta última foi a primeira lei brasileira que trouxe uma regulamentação quanto ao acesso à informa-

ção e à *internet*, sendo editada justamente para regular o inciso XXXIII, do art. 5º da CF.[67]

Em novembro de 2012 foi sancionada a Lei nº 12.737, a qual tipificou o crime de invasão a dispositivo informático, acrescentando os artigos 154-A e 154-B ao Codigo Penal. Em abril de 2014, ocorreu a maior e mais polêmica — até então — iniciativa do Estado brasileiro de regulação da internet. Através da Lei nº 12.373, o Marco Civil da Internet (MCI), estabeleceu as bases dos princípios, direitos e deveres para o uso da *internet* no Brasil, assim como diretrizes para o armazenamento de informações. Posteriormente foi editado o Decreto nº 8.771/2015, o qual regulamentava o MCI.

Em 14 de agosto de 2018, foi aprovada a Lei nº 13.709, a LGPD, a qual dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural. A aprovação dessa legislação nacional foi resultado de forte pressão por parte do mercado globalizado, haja vista a necessidade de uma legislação que estabelecesse um grau de proteção aos dados pessoais compatível com a normativa europeia, conhecida como *General Data Protection Regulation* (GDPR), como exigência para a contratação com empresas no ambiente da União Europeias[68].

Em decisão tomada nos dias 5 e 6 de maio de 2020, o Supremo Tribunal Federal, ao julgar a liminar deferida no julgamento das Ações Diretas de Inconstitucionalidades (ADIs) 6387, 6388, 6389, 6393, 6390, reconheceu a existência do direito fundamental à proteção de dados pessoais

67 RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de dados pessoais e seus reflexos nas ralações de trabalho. **Scientia Iuris,** Londrina, v. 23, n. 2, p. 127-146, jul. 2019.

68 MAGALHÃES, Rodrigo Almeida; OLIVEIRA, Erika Cristina Rodrigues Nardoni. O direito à privacidade na era digital. **Revista Jurídica da Fa7**, Fortaleza, v. 18, n. 1, jan./abr. 2021.

como uma garantia fundamental já existente na Constituição brasileira.[69] Por fim, em 2022 a Constituição recebe a sua 115ª Emenda ordinária, que incluiu o inciso LXXIX ao art. 5º para prescrever o direito fundamental à proteção dos dados pessoais em meio físico e digital.

Pela dinâmica acima estabelecida, é forçoso se concluir pela existência de uma política nacional de proteção de dados pessoais, o que reforça a importância dada à temática pelo Brasil. Considerando o exposto, indaga-se como a LGPD poderia produzir impactos econômicos e influenciar o princípio da livre concorrência e da livre iniciativa, próprios da ordem econômica brasileira.

4. A LGPD COMO INSTITUIÇÃO E FERRAMENTA DE ESTÍMULO À LIVRE INICIATIVA E A GARANTIA DA LIVRE CONCORRÊNCIA

Livre iniciativa é a liberdade que todos possuem para exercer uma atividade econômica, de produzir e tornar disponíveis a terceiros materiais e produtos necessários ao bem estar. Por sua vez, a livre concorrência é a garantia de que o Estado não irá, pelo menos em princípio, favorecer ou desfavorecer, por meios artificiais, agentes econômicos determinados, de forma que caberá a eles trilhar o seu próprio sucesso ou padecer no fracasso comercial, a depender das suas habilidades e das condições do mercado em que se inserem[70]. A livre concorrência é um dos princípios da ordem econômica, uma norma principiológica, pela qual o Estado deve propiciar a todos o livre exercício da atividade econô-

69 BRASIL. Supremo Tribunal Federal (Plenário). **ADI-MC 6.387/DF**. Relatora Min. Rosa Weber. Brasília, DF, 24 de abril de. 2020.

70 MACHADO SEGUNDO, Hugo de Brito. Algumas notas sobre a invocação do princípio da "livre concorrência" nas relações tributárias. **Nomos:** Revista do Programa de Pós-Graduação em Direito da UFC, Fortaleza, v. 28, n. 2, p. 61-81, jul./dez. 2008.

mica, de modo a permitir a disputa em paridade de armas no mercado, sem criar vantagens ou empecilhos indevidos que possam prejudicar a competição saudável dos agentes econômicos[71]. Como se percebe, livre iniciativa econômica e livre concorrência possuem uma forte conexão. O primeiro, por ser fundamento da ordem econômica, deve ser estimulado, porém de modo a não prejudicar o segundo.

A LGPD naturalmente promove impactos no ambiente de negócios, uma vez que a adequação às suas exigências implica um aumento dos custos de conformidade para que as empresas estejam permanentemente em cumprimento com a norma protetiva, o que exige a criação de instâncias internas, a capacitação de equipes, a contratação de consultorias, investimentos em infraestruturas de gestão da informação e permanente acompanhamento das ações internas.

Os ajustes necessários pelas empresas para se adequarem a LGPD poderiam resultar em perda de competitividade e barreiras de entrada para as micro e pequenas empresas, bem como para as *startups* e outras empresas de inovação, uma vez que as empresas de maior porte possuem, em virtude dos ganhos de escala, maiores e melhores condições para garantir a adequação, tais como maiores recursos financeiros e assessorias especializadas para esta finalidade.

Os custos de conformidade, para as grandes empresas, geram um pequeno impacto no faturamento, a despeito do possível aumento da quantidade de dados pessoais que essa empresa possa controlar. Exigir igual comportamento para micro e pequenas empresas pode acarretar custos proporcionalmente mais elevados, encarecendo sobremaneira seus produtos e serviços, caso o custo seja repassado para a composição dos preços. Tal situação, de exigência linear de adequação, poderia caracterizar uma situação de vulnerabilidade jurídica e negocial das mi-

71 MACHADO SEGUNDO, 2008.

cro e pequenas empresas. O ônus técnico e financeiro para as micros e pequenas empresas pode significar uma barreira na entrada de novos concorrentes no mercado, e consequentemente uma menor opção de produtos e serviços, e um aumento do preço por essa limitação ao mercado[72].

O uso dos dados pessoais na contemporaneidade é uma realidade irreversível que trouxe inúmeros benefícios à sociedade. A livre iniciativa não apenas permite, mas de certa forma estimula a utilização dos dados pessoais para fins econômicos, o que fora reafirmado pelo Estado brasileiro através da aprovação da Lei nº 13.874, de 20 de setembro de 2019, a chamada Lei da Liberdade Econômica. Em seu art. 4º, IV, dispõe ser vedado à administração pública abusar do poder regulatório para impedir ou retardar a inovação e a adoção de novas tecnologias, de processos ou modelos de negócios. As livres iniciativa e concorrência trazem em seu conteúdo a ideia de que tudo aquilo que for lícito poderá ser utilizado pelos agentes econômicos na criação e desenvolvimento das suas atividades. A concorrência estimula o mercado a melhorarem a qualidade, a quantidade, os preços e a inovarem em seus serviços e produtos.

Mas o uso dos dados pessoais pelas organizações não pode ser livre e desregulado ao ponto de permitir que se utilizem de meios não éticos — e até ilegais — no tratamento de dados pessoais e na extração de informações destes, os quais fazem parte dos direitos da personalidade do ser humano, e pertencem não as organizações que realizam os tratamentos, mas aos próprios titulares.

Os agentes econômicos que realizam tratamento de dados pessoais possuem uma vantagem concorrencial, sendo necessária a consideração da privacidade, da proteção de dados e da livre concorrência de forma conjunta, inclusive com revisitação as normas *antitruste*, para se garan-

72 ESTÊVES, Guilherme Mesquita. **Análise juseconômica da Lei Geral de Proteção de Dados Pessoais sob a ótica da eficiência na promoção de autodeterminação informativa**. Dissertação (Mestrado) – Universidade Federal de Ouro Preto, Ouro Preto, 2020.

tir a harmonização do sistema jurídico e econômico como um todo.[73]

Retornando a introdução deste estudo, quando utilizamos o conceito de mercado,[74] encontramos a LGPD como as "regras do jogo" no mercado de dados pessoais, como uma instituição formal que define e delimita o conjunto de escolhas dos indivíduos e das organizações.[75] A regulamentação do uso dos dados pessoais através da LGPD não veio mitigar a livre iniciativa, mas trouxe uma série de princípios, regras e obrigações a ser observada para que tais tratamentos sejam levados à efeito na forma constitucionalmente exigida, utilizando-se parâmetros internacionais de proteção.

Ademais, livre iniciativa e livre concorrência são fundamentos da LGPD, conforme destacado em seu art. 2º, VI, sendo descabido falar em violação desses institutos pela legislação protetora. A economia digital e seus agentes devem considerar a existência de outros fundamentos e princípios tão importantes quanto aqueles na sua atividade, tais como o respeito à privacidade, a autodeterminação informativa, à transparência, a segurança, os direitos humanos, entre outros, tanto destacados na Constituição Federal, quando na própria LGPD.

A proteção dos dados pessoais deve ser efetivada em um contexto de liberdade econômica; no entanto, com limitações impostas pelo próprio texto constitucional e reforçado pelas regras e princípios contidos na LGPD. Essa lei é uma ferramenta poderosa para a garantia da livre concorrência, mantendo o mercado digital equilibrado e aberto a novos participantes, impedindo o "vale tudo" no tratamento dos dados pessoais, o que poderia levar a uma postura de abuso do poder econômico advindo

73 FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas digitais e o negócio de dados: necessário diálogo entre o direito da concorrência e a regulação dos dados. **Direito Público**, v. 17, n. 93, o. 58-81, maio/jun. 2020.

74 MATIAS, 2009.

75 NORTH, op. cit., p. 14.

dos dados pessoais, e a movimentação das *big techs* para a prática de monopólio e de extinção da concorrência, além de várias outras violações a direitos fundamentais.

Tal impacto da LGPD na livre concorrência e na livre iniciativa em relação às micro e pequenas empresas, bem como as *startups*, não poderia ser exigido imediatamente mas sim ser resolvido posteriormente, através de normas regulamentares, orientações e procedimentos diferenciados, compatíveis com o grau de complexidade e capacidade de tratamento dessas empresas, a serem editadas pela Agência Nacional de Proteção de Dados (ANPD), conforme art. 55- J, XVIII, da norma[76].

Nesse sentido, em janeiro de 2022, a ANPD editou a Resolução CD/ANPD nº 2, aprovando o regulamento da LGPD para agentes de tratamento caracterizados como de pequeno porte, assim compreendidos como as microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas sem fins lucrativos, pessoas naturais e entes despersonalizados que atuem como controlador ou operador, **exceto** as que tratem dados de alto risco para os titulares, ou cujo faturamento próprio ou do respectivo grupo econômico ultrapasse o teto das empresas de pequeno porte ou das *startups*, conforme interpretação do art. 2º, I, c/c art. 3º da normativa.

Entre as adaptações, encontram-se:

a) flexibilidade de canais para a disponibilização de informações referentes ao tratamento de dados pessoais (art. 7º);

b) possibilidade de organização nas entidades representativas do se-

76 Nesse sentido: XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; Cf. BRASIL. **Lei 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília-DF, 15 de agosto de 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 ago. 2021.

tor para resolução de conflitos com titulares de dados (art. 8º);

c) simplificação no registro das operações de tratamento de dados pessoais (art. 9º);

d) flexibilidade e simplificação na comunicação de incidentes de segurança (art. 10);

e) a dispensa de indicação de encarregado de dados (também conhecido como DPO, sigla para *data privacy officer*), desde que disponibilize um canal de comunicação com os titulares (art. 11);

f) a aprovação de uma política simplificada de segurança da informação, com elementos de garantia mínima para problemas ordinários (art. 13);

g) a previsão de prazo em dobro para atendimento das demandas dos titulares, para comunicação à ANPD em caso de incidente de segurança, entre outros (art. 14)[77].

5. CONCLUSÃO

Diante das questões e das análises acima realizadas, verifica-se que os dados pessoais são, e serão por muito tempo, expressivos ativos econômicos no mercado digital, sendo incontáveis as possibilidades da sua utilização para atuais e novos negócios.

A LGPD tem a enorme e difícil tarefa não apenas em regulamentar o tratamento dos dados pessoais e de tornar possível a sua sindicabilidade, mas deve servir, ainda, como importante ferramenta de estímu-

77 ANPD (Autoridade Nacional de Proteção de Dados). Conselho Diretor. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília: ANPD, 2022.

lo e proteção constitucional à liberdade econômica e à garantia da livre concorrência.

Esta pesquisa configura-se como uma proposta inicial de abordagem do tema a partir de uma perspectiva do Direito Econômico. Não é papel da ANPD realizar a repressão do abuso do poder econômico, tarefa precipuamente atribuída ao Conselho Administrativo de Defesa Econômica (CADE). Contudo, enquanto entidade reguladora dos dados pessoais, considerados como as *commodities* do mercado global da primeira quadra do século XXI, e responsável pela regulamentação da LGPD através de seus normativos, a ANPD tem a importante missão de compor os interesses dos agentes econômicos envolvidos nesse mercado digital, estabelecendo regras que promovam a competição entre os agentes econômicos e os induzam de modo a evitar a concentração dos mercados e a criação de barreiras para o acesso de novos *players*.

Com efeito, esta pesquisa concentrou-se em um dos aspectos desse problema, a saber, o tratamento diferenciado em relação às microempresas e empresas de pequeno porte, princípio da ordem econômica que é corolário do princípio da livre concorrência. A atuação da ANPD, mormente com a edição da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, sugere a preocupação da entidade com os impactos econômicos que a LGPD pode trazer, no caso, com os impactos causados pelos custos de conformidade sobre as empresas.

As regras diferenciais trazidas pelo normativo denotam a atenção que a ANPD dá para buscar uma aplicabilidade efetiva da LGPD, sugerindo um escalonamento do nível de proteção exigida segundo o grau de risco do tratamento, ou a partir da relevância econômica do agente.

REFERÊNCIAS

ALVARENGA, Darlan; SILVEIRA, Daniel. PIB do Brasil despenca 4,1% em 2020. **G1**, Economia, 3 mar. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/03/03/pib-do-brasil-despenca-41percent-em-2020.ghtml. Acesso em: 31 ago. 2021.

ANPD (Autoridade Nacional de Proteção de Dados). Conselho Diretor. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.** Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília: ANPD, 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 31 jan. 2022.

ARTESE, Gustavo. Compliance digital e privacidade. In: CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI, Rodrigo; VENTURINI, Otavio. **Manual de Compliance**. 2. ed. Rio de Janeiro: Forense, 2020.

ARTHUR, Charles. Tech giants may be huge, but nothing matches big data. **The Guardian,** International edition, Technology, 23 ago. 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 31 ago. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 out. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 15 de agosto de 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 ago. 2021.

BRASIL. Supremo Tribunal Federal (Plenário). **ADI-MC 6.387/DF.** Relatora Min. Rosa Weber. Brasília, Df, 24 de abril de 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 13 out. 2020.

CARNEIRO, Felipe. O produto é você. **Veja**, Economia, 26 out. 2018. Disponível em: https://veja.abril.com.br/economia/o-produto-e-voce/. Acesso em: 31 ago. 2021.

CARVALHO, André Castro; ALVIM, Tiago Cripa; BERTOCCELLI, Rodrigo; VENTURINI, Otavio (Coord.). **Manual de Compliance**. 2. ed. Rio de Janeiro: Forense, 2020.

CASTELLS, Manuel. **A sociedade em rede**. v. I. 6. ed. São Paulo: Paz e Terra, 1999.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios (2ª Turma Cível). **Agravo de Instrumento nº 0749765-29.2020.8.07.0000**. Agravante: Ministério Público do Distrito Federal e Territórios. Agravado: SERASA S.A. Relator: Desembargador Cesar Loyola. Acórdão nº 1341840, julgado em 26 maio 2021. Disponível em: https://pje2i.tjdft.jus.br/consultapublica/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=f35858e977c68d5e59bd02e30a4790655fd187ddfe216ebe. Acesso em 25 ago. 2021.

DONEDA, Danilo. **Da privacidade à proteçao de dados pessoais**. 2. ed. São Paulo: RT, 2020.

EKBIA, Hamid R.; NARDI, Bonnie. **Heteromation, and other stories of computing and capitalism**. Cambridge: MIT Press, 2017.

ESTÊVES, Guilherme Mesquita. **Análise juseconômica da Lei Geral de Proteção de Dados Pessoais sob a ótica da eficiência na promoção de autodeterminação informativa**. Dissertação (Mestrado) – Universidade Federal de Ouro Preto, Ouro Preto, 2020.

FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas digitais e o negócio de dados: necessário diálogo entre o direito da concorrência e a regulação dos dados. **Direito Público,** v. 17, n. 93, o. 58-81, maio/jun. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3695. Acesso em: 2 set. 2021.

FREIRE, Ana Lucy Oliveira. O desenvolvimento do comércio e a produção do espaço urbano. **GeoTextos**, v. 6, n. 2, p. 11-32, dez. 2010. Disponível em: https://periodicos.ufba.br/index.php/geotextos/article/download/4829. Acesso em: 2 set. 2021.

HARARI, Yuval Noah. **Sapiens:** uma breve história da humanidade. L&PM, 2015.

JIMÉNEZ SERRANÍA, Vanessa; ABRUSIO, Juliana. Big data: uma análise sob a óptica das práticas abusivas no acesso e uso de dados massificados na economia de plataforma. **Revista de Direito Brasileira**, Florianópolis, v. 28, n. 11, p. 387-404, jan./abr. 2021. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/6819. Acesso em: 29 jul. 2022.

HUBERMAN, Leo. **História da Riqueza do homem**. 16. ed. Rio de Janeiro: Zahar, 1981.

KANTAR. **Kantar BrandZ:** 2021 most valuable global brands. London: Kantar Brandz, 2021. Disponível em: https://www.rankingthebrands.com/PDF/Brandz%20Most%20Valuable%20Global%20Brands%202021,%20Kantar.pdf. Acesso em 25 ago. 2021.

MACHADO SEGUNDO, Hugo de Brito. Algumas notas sobre a invocação do princípio da "livre concorrência" nas relações tributárias. **Nomos:** Revista do Programa de Pós-Graduação em Direito da UFC, Fortaleza, v. 28, n. 2, p. 61-81, jul./dez. 2008. Disponível em: http://periodicos.ufc.br/nomos/article/view/11754. Acesso em: 31 ago. 2021.

MAGALHÃES, Rodrigo Almeida; OLIVEIRA, Erika Cristina Rodrigues Nardoni. O direito à privacidade na era digital. **Revista Jurídica da Fa7,** Forta-

leza, v. 18, n. 1, jan./abr. 2021. Disponível em: https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1173. Acesso em: 25 ago. 2021.

MATIAS, João Luis Nogueira. **A função social da empresa e a composição de interesses na sociedade limitada.** Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

NORTH, Douglas C. **Instituições, mudança institucional e desempenho econômico.** Tradução de Alexandre Morales. São Paulo: Três Estrelas, 2018.

RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de dados pessoais e seus reflexos nas ralações de trabalho. **Scientia Iuris,** Londrina, v. 23, n. 2, p. 127-146, jul. 2019. Disponível em: http://www.uel.br/revistas/uel/index.php/iuris/article/view/35794. Acesso em: 09 out. 2020.

SILVEIRA, Sérgio A.; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc**, Rio de Janeiro, v. 12, n. 2, p. 217-230, nov. 2016. Disponível em: http://revista.ibict.br/liinc/article/view/3719. Acesso em: 26 ago. 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.

Open banking, sigilo bancário e LGPD: como resolver essa equação?

Open banking, bank secrecy and LGPD. how to solve that equation?

Micael Souza Borja

» Graduado em Direito pela Universidade Estadual de Santa Cruz. LLM em Direito Corporativo pelo Instituto Brasileiro de Mercado de Capitais (IBMEC). Advogado do Banco do Nordeste do Brasil S.A.

» E-mail: micaelsb@bnb.gov.br

REVISTA JURÍDICA DO BANCO DO NORDESTE

Recebimento: 29/09/2022
Aprovação: 27/10/2022

RESUMO

O presente artigo visa abordar, de forma resumida, a criação e implantação no Brasil do Sistema Financeiro Aberto, comumente chamado de "Open Banking" ou "*Open Finance*" e as suas implicações com a Lei Geral de Proteção de Dados (Lei n] 13.709/18) e a Lei do Sigilo Bancário (LC n. 105/2001). Instituído como parte da AGENDA BC# do Banco Central, a nova plataforma tem por objetivo o compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes. A solução para que o compartilhamento desses dados financeiros de clientes pessoa física esteja de acordo os ditames de sigilo e proteção de informações pessoais previstos na legislação adjacente e na Resolução Conjunta BACEN/CMN nº 1/2020 passam necessariamente pela figura jurídica do consentimento. Os mecanismos para que se obtenha o referido consentimento, todavia, não são simples e as sanções de natureza cível, administrativa e penal para o vazamento e o compartilhamento indevido de dados pessoais de clientes podem ser graves.

PALAVRAS-CHAVES

Open Banking. Lei Geral de Proteção de Dados. Sigilo Bancário. Consentimento. Dados pessoais.

ABSTRACT

The present article aims to briefly address the creation and implementation in Brazil of the Open Financial System, commonly called Open Banking or Open Finance and its implications with the General Personal Data Protection Law (Law n. 13.709 /2018) and the Bank Secrecy Law (Complementery Law n. 105/2001). Established as part of the BC#

AGENDA of the Central Bank, the new platform aims to share data, products and services by financial institutions and other authorized institutions, at the discretion of their customers. The solution for sharing these financial data of individual customers is in accordance with the dictates of secrecy and protection of personal information provided for in the aforementioned legislation and in Joint Resolution BACEN/CMN N. 1/2020 necessarily involves the legal form of consent. The mechanisms for obtaining that consent, however, are not simple and the civil, administrative and criminal sanctions for the leakage and improper sharing of personal data of customers can be serious.

KEYWORDS

Open Banking. General Data Protection Act. Bank Secrecy. Consent. Personal data.

SUMÁRIO

1. INTRODUÇÃO

O Banco Central do Brasil (BCB) vem, desde 2019, propondo grandes desafios aos bancos e demais instituições financeiras brasileiras.

Na onda desse movimento de maior abertura, avanço tecnológico e democratização do acesso aos serviços e produtos, o BACEN propôs a AGENDA BC# - Uma pauta para o sistema financeiro do futuro.

Diante de atrasos no cronograma original, que previa implantação completa em 12/2021, a plataforma está na quarta fase de sua implantação.

No final de 2020, como fruto dessa agenda, presenciamos o nascimento do PIX, que por sua praticidade e economia, vem fazendo grande sucesso e alterando fortemente a lógica dos meios de pagamento no sistema financeiro nacional.

Uma das propostas mais revolucionárias dessa Agenda BC# é a implantação do *Sistema Financeiro Aberto.*

*Nas palavras do BACEN, Open Banking "*é considerado o compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação, de forma segura, ágil e conveniente" (COMUNICADO BACEN n° 33.455, de 24 de abril de 2019).

Num primeiro momento, dada a tradição de um sistema bastante hermético, alguém poderia questionar se o compartilhamento de todos esses dados e informações não poderia resultar em quebra de sigilo de dados, regulado pela Lei nº 13.709 (Lei Geral de Proteção de Dados), e/ou até mesmo do sigilo bancário, regido pela Lei Complementar nº 105/2001 (Lei do Sigilo Bancário).

O presente artigo visa abordar essa aparente contradição entre o *Open Banking* e a proteção de dados financeiros pessoais, esclarecendo que o consentimento esclarecido do consumidor é a chave para a resolução do problema.

A forma de obtenção desse consentimento, os objetivos específicos para a sua concessão, a sua resolutividade e as consequências legais do vazamento e do compartilhamento indevido de dados pessoais, como veremos, apresentam desafios que serão objeto de apreciação pelo poder judiciário.

2. *OPEN FINANCE* E O COMPARTILHAMENTO DE DADOS FINANCEIROS PESSOAIS

Nos termos da Resolução Conjunta BACEN/CMN nº 1/2020, o modelo de sistema financeiro aberto a ser implantado no Brasil deve atender, no mínimo, aos seguintes dados, produtos e serviços:

> I – dados relativos aos produtos e serviços oferecidos pelas instituições participantes (localização de pontos de atendimento, características de produtos, termos e condições contratuais e custos financeiros, entre outros);
>
> II – dados cadastrais dos clientes (nome, filiação, endereço, entre outros);
>
> III – dados transacionais dos clientes (dados relativos a contas de depósito, a operações de crédito, a demais produtos e serviços contratados pelos clientes, entre outros); e
>
> IV – serviços de pagamento (inicialização de pagamento, transferências de fundos, pagamentos de produtos e serviços, entre outros).

E por qual motivo o cliente aceitaria autorizar que outros bancos/fintechs tenham acesso e possam tratar seus dados financeiros?

É aí que chegamos no grande atrativo da proposta *"Open"*. O cliente poderá ter acesso a uma plataforma com um número muito maior de

serviços bancários complementares ao já oferecido pela instituição financeira que ele é cliente.

Outra promessa da plataforma aberta é que com uma maior oferta de serviços, seja estimulada a competitividade e a inovação por parte das instituições financeiras, resultando em produtos e serviços mais baratos e/ou vantajosos para o consumidor.

A Resolução Conjunta BACEN/CMN nº 1/2020, com redação atualizada pela Rel. BACEN4/2022, explicita em seu art. 5º que constituem objetivos do *Open Finance:*

> I – incentivar a inovação;
>
> II – promover a concorrência;
>
> III – aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro; e
>
> IV – promover a cidadania financeira.

3. A APARENTE CONTRADIÇÃO ENTRE O OPEN BANKING E PROTEÇÃO DE DADOS PESSOAIS E O SIGÍLO BANCÁRIO

Mas, como conciliar esse compartilhamento de dados de natureza pessoal de clientes com as premissas e ditames de proteção de dados previstos na Lei Geral de Proteção de Dados (Lei n. 13/709/2018) e com as regras atinentes ao sigilo bancário (Lei Complementar n. 105/2001)?

A resposta para tal pergunta vem da própria lógica contida em ambas as leis, que preveem como exigência fundamental para acesso à informação o consentimento do cliente.

Tanto a lei do sigilo bancário quanto a LGPD preveem que não configura violação de sigilo o compartilhamento/tratamento de informação

mediante prévio e expresso consentimento do titular da informação.

> "Art. 1º. As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
>
> (...)
>
> § 3º Não constitui violação do dever de sigilo:
>
> (...)
>
> V – a revelação de informações sigilosas com o consentimento expresso dos interessados;" (Lei Complementar n. 105/2001).
>
> "Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I – mediante o fornecimento de consentimento pelo titular;" (Lei n. 13.709/2018).

No tocante a esse consentimento e as suas especificidades, verifica-se que a LGPD estabelece diversas exigências para que o tratamento/compartilhamento de dados pessoais tenha caráter legítimo e esclarecido.

O art. 7º, §7º da LGPD explicita que o controlador que obteve o consentimento do cliente e que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim.

O art. 8º da lei, por sua vez, é essencial para que sejam conhecidos os limites desse consentimento. Em breve resumo, a lei estabelece que o consentimento deve ser escrito ou por meio que demonstre claramente a vontade do titular do dado.

Se for por escrito, o consentimento deve estar contido em cláusula destacada das demais. Já a cláusula que trata do consentimento deve ainda conter de forma clara as finalidades determinadas para o seu uso (art. 8º, §1º e §4º).

Trata-se de ponto tão sensível da lei que o mesmo art. 8º estabelece que é vedado o tratamento de dado obtido por meio de vício de consentimento e que cabe ao controlador do dado o ônus da prova de que o mesmo foi obtido de acordo com a lei.

Por fim, a LGPD deixa claro que esse consentimento pode ser revogado a qualquer momento, por procedimento "gratuito e facilitado" (art. 7, §5º).

Para que não se tenha dúvidas nem mesmo sobre o conceito legal de consentimento, a própria lei, por meio do art. 5º, explicita que consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;".

Em termos voltados à regulação específica do *Open Finance,* a Resolução Conjunta BACEN/CMN nº 1/2020, buscando uma conformidade do sistema com as premissas da LGPD, além de endossar o contido na lei sobre o consentimento prévio, livre e esclarecido, detalha que o consentimento deve ser dado por meio eletrônico (art. 2º. VIII).

A Resolução Conjunta BACEN/CMN nº 1/2020 alerta ainda que é vedada a obtenção de consentimento por meio de contrato de adesão e/ou por meio de formulário com opção de aceite previamente preenchida e, também, de forma presumida, sem manifestação ativa da parte do cliente (art. 10, § 3º).

É preciso que as instituições financeiras estejam atentas aos detalhes e especificidades relacionadas ao consentimento.

4. CONSEQUÊNCIAS ADVINDAS DO COMPARTILHAMENTO ILEGAL DE DADOS PESSOAIS E EVENTUAL QUEBRA DE SIGÍLO BANCÁRIO

O "compartilhamento" indevido de dados de clientes da instituição e/ou de clientes que a instituição tenha obtido acesso por meio do *Open Banking* está sujeito às sanções administrativas previstas na LGPD, que vão da imposição de multa e suspensão temporária do tratamento de dados a até mesmo à proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 52, Lei nº 13.709/18).

Além das sanções administrativas, o compartilhamento indevido de dados pode estar sujeito também a reparações de natureza cível.

Vem sendo discutido na jurisprudência se o vazamento genérico de dados de cliente pode, por si só, configurar dano moral *in re ipsa* ou se deve ser comprovado pelo titular do dado que o vazamento do dado resultou em dano efetivo que deve ser objeto de reparação cível. Nesse sentido, decisão da 26ª Câmara da Seção de Direito Privado do TJ/SP:

> "COMPRA E VENDA DE BEM MÓVEL -AÇÃO DE INDENIZAÇÃO -VAZAMENTO DE DADOS DOCONSUMIDOR NO WEBSITE DA RÉ -VULNERABILIDADE DO SISTEMA – RESPONSABILIDADE OBJETIVA DA FORNECEDORA – DANOS MORAIS CONFIGURADOS – RECURSO PROVIDO PARA JULGAR A AÇÃO PARCIALMENTE PROCEDENTE". (TJSP – Rec. Apelação, proc. Nº1003122-23.2020.8.26.0157, 26 Cam. Dir. Privado, Rel. Des. Renato Sartorelli, j. 22/06/2021)

Mas além disso, alguns desses dados, à exemplo de saldo de conta bancária, extratos e relatórios de investimentos, por sua natureza, são resguardados também pelo sigilo bancário.

A quebra de sigilo bancário, por sua vez, ocorrendo fora das hipóteses legais permitidas pela LC 105/2001 – dentre elas a do consentimento

esclarecido – constitui ilícito penal e sujeita o(s) responsável(is) à pena de reclusão, de um a quatro anos, e multa (art. 10, LC 105/2001), além das possíveis reparações cíveis e/ou penalidades de natureza administrativa com base na LGPD.

Como visto, apesar de aparentemente simples, a resolução da equação que viabiliza a implantação do *open banking* no Brasil passa necessariamente pelas especificidades, que não são tão simples.

Os procedimentos para a colheita do consentimento devem ser claros, objetivos e seguros, de forma a não deixar margem para dúvidas tanto para o consumidor como também para o judiciário em caso de litígio envolvendo a questão.

Como ressaltado acima, a LGPD é clara no sentido de o ônus da prova sobre a não ocorrência de vício no consentimento é do futuro controlador do dado, que nesse caso é a instituição financeira que solicita o acesso aos dados financeiros do cliente.

O compartilhamento indevido desses dados pode, como visto, resultar em consequências graves. É preciso que haja uma cuidadosa aderência entre as práticas adotas pelas instituições participantes da plataforma e o disposto na legislação.

> "A conformidade aos princípios elencados acima, tanto na Resolução do Open Banking, quanto na LGPD, é condição basilar para que os participantes do open banking não gerem riscos aos clientes, às demais instituições e ao próprio setor. Significa dizer que cada instituição participante do open banking é responsável pela segurança e sigilo nas jornadas de autenticação do cliente, gestão dos consentimentos, uso e compartilhamento de dados, devendo adotar as melhores práticas para proteção dos dados dos clientes".

5. CONSIDERAÇÕES FINAIS

Todavia, a implantação do sistema *Open Finance,* em que pesem os riscos envolvidos, é de nítido interesse das instituições financeiras e segue tendência típica da chamada revolução 4.0, em que o domínio da informação configura diferencial competitivo em uma economia nitidamente baseada em dados.

Diante de seu caráter recente e da complexidade das questões envolvendo o manejo/compartilhamento desses dados, muitos pontos dos pontos tratados até aqui serão ainda submetidos ao crivo do judiciário.

Ao poder judiciário caberá a última palavra sobre os limites dessa plataforma *Open,* especialmente no tocante a questões consumeristas, tributárias e de tratamento de dados pessoas.

O que é certo, a nosso ver, é que além de alterar fortemente a lógica do sistema bancário brasileiro, o *Open Banking* irá demonstrar para o consumidor o quanto que seus dados financeiros são valiosos e devem usados em seu benefício. Caso contrário, que sejam usadas as salvaguardas legais previstas na LGPD e na LC 105/2001 para que sejam combatidos desvios e excessos.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BALTAZAR JÚNIOR, J.P. Sigilo bancário e privacidade. 1 ed. Porto Alegre: Livraria do Advogado, 2005.

BANCO CENTRAL DO BRASIL. Resolução Conjunta nº 1, de 4 maio de 2020 (Redação dada, a partir de 2/5/2022, pela Resolução Conjunta nº 4, de 24/3/2022.). disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v4_P.pdf

BLUM et TERADA. R.O e F. M. D.. Open banking e a Lei Geral de Proteção

de Dados. Disponível em: https://noomis.febraban.org.br/especialista/renato-opice-blum/open-banking-e-a-lei-geral-de-protecao-de-dados

BRANCO, M. Vazamento de dados gera direito a indenização por danos morais?. Disponível em: https://www.jota.info/justica/vazamento-de-dados--danos-morais-16082021.

BRASIL. LEI N. 13.709, de 14 de agosto de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. LEI COMPLEMENTAR N. 105, de 10 de janeiro de 2001. Lei do Sigilo Bancário

FRAZÃO, OLIVA, TEPEDINO. A. M. G. Lei geral de proteção de dados pessoais: e suas repercussões no direito brasileiro. 2 ed, 2021.

Proteção de dados pessoais, privacidade e ética na sociedade da informação: as lições da superinteligência artificial

Protection of personal data, privacy and ethics in the information society: the lessons of artificial super intelligence

Geralda Magella de Faria Rossetto

» Doutora em Direito pelo Programa de Pós-Graduação em Direito pela Universidade Federal de Santa Catarina (UFSC). Mestre em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS). Advogada, com ênfase em curadoria de dados. Pesquisadora do Núcleo de Estudos Jurídicos e Sociais da Criança e do Adolescente – NEJUSCA, do Núcleo de Pesquisa Direito e Fraternidade – UFSC e do DataLab – Laboratório de Desenvolvimento e de Pesquisa em Gestão de Dados – UFSC. Membro da Rede Universitária para Estudos sobre a Fraternidade (RUEF). Procuradora Federal da Advocacia Geral da União (AGU) aposentada.

» E-mail: geraldamagella@gmail.com

Endy de Guimarães e Moraes

» Doutoranda em Direito pela Fordham University (NY/EUA). Mestre em Direito pela Fordham University (NY/EUA). Professora

REVISTA JURÍDICA DO BANCO DO NORDESTE

convidada de cursos de graduação e pós-graduação. Advogada e Diretora do Centro de Estudos sobre a Religião, as leis e o trabalho dos advogados na Fordham University.

» Email: emoraes@law.fordham.edu

Isaac Nogueira de Almeida

» Mestrando em Planejamento e Políticas Públicas. Advogado. Especialista em Direito Tributário e em Direito Penal e Criminologia. Pesquisador no grupo de "Direito e Fraternidade", da Universidade Federal do Rio Grande do Sul. Participa da rede Internacional "Comunhão e Direito".

» E-mail: isaacnogueira.adv@gmail.com

Recebimento: 30/09/2022
Aprovação: 27/10/2022

RESUMO

Pretende-se analisar a proteção de dados, a privacidade e a ética tendo por parâmetro a inteligência artificial. O estudo elege alguns marcos jurídicos, especialmente a Lei Geral de Proteção de Dados, para examinar a proteção dos direitos ante algumas aplicações da inteligência artificial. Conclui-se que tais temáticas requerem a adoção de técnicas razoáveis de conformidade, seja com os dados pessoais, através de um padrão voltado à ética, seja com *privacy by design*, voltado a duas responsabilidades cardeais: *uma* baseada no diálogo universal acerca do impacto de novas tecnologias; *outra*, na qualidade de um mínimo indispensável, de finalidade e de razoabilidade, a dizer, legítimos interesses voltados à proteção dos direitos de todos. Elegeu-se o método dedutivo e a técnica de pesquisa a matriz bibliográfica e sua revisão, nacional e estrangeira disponível a respeito dos temas.

PALAVRAS-CHAVE

Proteção de Dados Pessoais; Privacidade; Ética; Inteligência Artificial.

ABSTRACT

This paper aims to analyze data protection, privacy, and ethics, having artificial intelligence as a parameter. The study elects some legal frameworks, especially the Brazilian General Data Protection Law, to examine the protection of rights before some artificial intelligence applications. It concludes that such themes require the adoption of reasonable techniques of compliance, whether with personal data, through a standard focused on ethics, or with privacy by design, focused on two cardinal responsibilities: one based on a universal dialogue about the impact of new technologies; the other, as a necessary minimum, of purpose and

reasonableness, i.e., legitimate interests aimed at protecting the rights of all. The research used the deductive method and a bibliographic review of national and foreign materials on the themes.

KEYWORDS

Personal Data Protection; Privacy; Ethics; Artificial Intelligence.

SUMÁRIO

1. INTRODUÇÃO

O presente estudo baseia-se em uma simples premissa, certamente muito conhecida pelos que atuam na esfera da tecnologia: o alimento da inteligência artificial consiste basicamente de dados. Consequentemente, dados e inteligência artificial (IA) são uma dupla inseparável, o que justifica a adesão relativa à privacidade, à ética e demais temas correlatos, como ocorre em relação à proteção de dados pessoais.

Não por acaso, os esforços de muitos para entender o que se processa com a evolução e a revolução das gerações de dados pessoais e a urgência com que as demandas voltadas à privacidade e a ética estão a acontecer. Mas é fato, os limites de proteção nem sempre se dão como esperado, a favor de um caminho ético, inclusivo e evolutivo, ou mesmo, no campo das leis, já se sabe de certas problemáticas que atravessam a regulação da internet e está indo além. *Uma* delas diz respeito ao valor dos dados pessoais – que precisa ser claro - cujo avanço mercadológico deve ser revisto ao longo do tempo visando conter a comercialização dos dados e a consequente violação de sua proteção em detrimento dos interesses do usuário. *Outro,* é sobre as redes e a importância da conexão que precisa acontecer dando ênfase à inclusão e à educação. Ainda, outra mais específica, que vai além daquela que compõe a rede de colaboração em busca de uma ideia fundamental, é a que diz respeito à inovação e a mudança, e tem a ver com a articulação da própria promoção e "defesa" dos dados, de modo que, rapidamente, num piscar de olhos, a proteção de dados pessoais se decompõe em uma falsa e inexistente proteção. A explicação(?). É comum apontar que o ansioso e forte mercado econômico mudou de tal forma que o lucrativo negócio dos dados pessoais entrou na seguinte escala: dados são vilipendiados, comercializados e vendidos, à mercê de seus titulares, que passam à categoria de usuários. O que fazer(?). Recorrer à inteligência artificial(?).

Retomando ao ponto zero, antes apresentado, dados e IA usufruem

de dependência recíproca. Aliás, o avanço desenfreado da IA, desacompanhada da proteção e de regulação de direitos, e do alto custo da comercialização daqueles (dados), realizada sem observação de salvaguardas e de demais processos educativos, leva a destacar os esforços de alguns países no desenvolvimento de uma cultura de dados. O Canadá, cujo admirável esforço do *Privacy by Design* oferece lições para o mundo todo, enquanto outros países, como ocorre com a União Europeia confere protagonismo de legislação específica, no caso a GDPR, cujo exercício de proteção de dados avança em discussão e desafios, e segue inspirando outros países a terem atitudes nesse sentido, como é o caso do Brasil, cuja Lei Geral de Proteção de Dados Pessoais, nasceu inspirada sob tal égide.

Com efeito, o ansioso mercado econômico e o atrasado mercado jurídico – da regulação e regulamentação e da fábrica de leis - necessitam mutuamente de um replanejamento político, legislativo e de "engenharia" organizacional voltada à IA. O intuito é uma "arquitetura" da proteção pessoal humana, uma espécie de conscientização máxima de seu código fonte, de dados, ponta a ponta, a conferir proteção aos dados pessoais. Ora, um bom código, um código limpo, não deve estabelecer um código confuso – ainda que tal se faça para funcionar – deve visar a dar garantias de privacidade e de ética à proteção de dados.

Exposta essa realidade, este estudo tem como proposta examinar a proteção de dados pessoais tendo como perspectiva a inteligência artificial e como pano de fundo apresentar as distintas e entrelaçadas funções que decorrem da privacidade e da ética nesse campo de atuação, tendo por escopo destacar a reafirmação que lhes cabe quanto ao desenvolvimento e os desdobramentos na árdua tarefa de proteção de dados pessoais.

A metodologia adotada para essa finalidade tem como pressuposto o desafio da construção dos saberes e, em tal razão, toma em empréstimo a crítica - tão própria em uma sociedade superconectada e cada vez mais

portadora de novidades, cujas mudanças acenam novas problemáticas para a educação e a ciência de modo a refletir e, consequentemente, expor um juízo a respeito do estado da questão proposta: dados pessoais e inteligência artificial, será mesmo uma inteligência que galga o reconhecimento de estar à frente da proteção dos direitos(?). No mais, para cumprir o objetivo proposto, se utilizará como método de abordagem o dedutivo e a técnica da pesquisa segue a matriz bibliográfica, incluindo sites, sobretudo, as referências decisivas para a pesquisa, priorizando a revisão da bibliografia nacional e estrangeira disponível a respeito dos temas.

Com o objetivo de facilitar a compreensão do trabalho, os aspectos suso indicados serão assim distribuídos, na seguinte ordem, além da *introdução* e das *considerações finais*: *primeiro*, a proteção de dados pessoais na sociedade da informação; *segundo*, a privacidade e a ética contrapostas e expostas no mundo tecnológico das superconexões; *terceiro,* a urgência da proteção dos dados pessoais frente a inteligência artificial – como lidar com uma inteligência que se apresenta – e se supõe - maior do que os humanos e que, pela primeira vez, começa a interagir concretamente com os humanos, como está a acontecer na Revolução 5.0.

2. UM MUNDO ANSIOSO POR PROTEÇÃO DE DADOS PESSOAIS

Trazidos para o espaço cotidiano, a categoria dos dados pessoais muito se aproxima do usuário consumidor. Distribuídos na sociedade globalizada, o tema se confunde com a informação e a comunicação. Conectados e transferidos, os dados ocupam outro processo, resultado de conexão, e se aproximam da sociedade da vigilância, cuja proximidade com o "capitalismo da vigilância" salta aos olhos, ainda que, nessa perspectiva, é evidente que entra em cena a informação.

Compreender o universo do usuário, da informação, da comunica-

ção, da conexão, da transferência e da vigilância requer uma tradução para o mundo dos dados pessoais e de sua respectiva proteção: tenhamos em conta que até recentemente, imperava a tendência humana de utilização da inovação tecnológica, independentemente de suas consequências.

Essa atitude de abertura ao mercado tecnológico e de criação e adoção das necessidades pode não ter limites, o que não mais se justifica à luz da finalidade, e, em tal razão, sublinha-se a importância de relacionar alguns mais princípios à tutela de proteção de dados, tais como, o da necessidade, pertinência, proporcionalidade, simplificação e harmonização.

Outro ponto que justifica a inscrição do dado pessoal ao mínimo indispensável, tem a ver com garantir a maior liberdade possível, sendo que essa tomada de posição, parece afetar a coleta de dados e a razão de sua finalidade. Em matéria de dados sensíveis e em questões envolvendo a criminalidade, as regras do jogo parecem ofertar propostas antagônicas, eis que, se de um lado, as mesmas devem ser objetivas e limitadas, a coleta de dados genéticos, por exemplo, compõe um mosaico desafiador: se de um lado, somente podem ser legítimas em relação a pessoas sobre as quais pese alguma suspeita, por outro, não são admissíveis testagens de massas ou coletivas. Essa balança, desde o "11 de setembro" carece de reparos, exatamente porque o terrorismo criou novas ruptura, acelerou a disrupção e estabeleceu novas agendas, de modo que, a conservação de qualquer dado pessoal e/ou amostra genética, segundo o ideal de amostras legitimamente recolhidas no interesse das autoridades, no caso de ação judicial, carece de ser submetidas ao arsenal interpretativo dos juízes e dos custodiares.

Mesmo que inerente a rastreabilidade dos dados em casos conforme os anteriormente relacionados, referida configuração implica em algo mais: dar conta de proteção da privacidade, cujo sentido alargado também leva à compreensão da imagem, da honra e da identidade da pessoa humana, e, portanto, muito próximo e contíguo em relação aos dados

pessoais e da condução da esfera ética. Exatamente por essas questões que o capitalismo da vigilância entra na cena econômica, segundo uma ordem de vigília, cujos traços são marcados pelas seguintes características, segundo a lição de Zuboff (2021, p. 15):

> **1.** Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; **2.** Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; **3.** Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; **4.** A estrutura que serve de base para a economia de vigilância; **5.** Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; **6.** A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; **7.** Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; **8.** Uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos.

Por mais que usufruam de sentidos específicos, tradutores de sua mensagem e identidade que lhes são inerentes, dado e informação dão conta de um recado: um dado é a informação potencializada, são fatos, de sorte que, segundo Mendes, se o dado assume a forma de uma palavra impressa ele é imediatamente compreendido como informação (2019, p. 55), de modo que, "O discurso sobre a privacidade cada vez mais gira em torno de questões relacionadas a dados pessoais e, portanto, sobre a informação. O papel da informação como ponto de referência de um grande número de situações jurídicas é flagrante" (DONEDA, 2019, p. 135).

Nesse prisma, dado e informação são categorias com matrizes conceituais particulares, de modo que, segundo revela a Profa. Laura Mendes (2019, p. 55): *i)* dados e informações embora distintos, guardam conceitos relacionados; *ii)* a informação é o resultado de uma ação in-

terpretativa e subordina-se ao contexto em que surge, o observador e o intérprete; *iii)* dados são símbolos ou sinais formais e bases potenciais de informação; *iv)* ambos podem ser armazenados e processados; *v)* quando o dado permite à associação, ele caracteriza-se como dado pessoal; *v)* detém um alto valor informativo.

Do universo normativo, são extraídos também três importantes conceitos, os quais mutuamente se alimentam, a dar conta de uma evolução jurídica da cultura de dados pessoais, a saber:

i) dados pessoais na Diretiva 95/46/CE, de 1995:

Dados pessoais são fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável, de modo que, na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 (DIRETIVA 95/46/CE, 2022), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, consta:

> Artigo 2º
>
> Definições
>
> Para efeitos da presente directiva, entende-se por:
>
> a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

ii) dados pessoais no GDPR (Regulamento Geral de Proteção de Dados da União Europeia):

O GDPR (2022) dispõe que:

> O termo 'dados pessoais' é a porta de entrada para a aplicação do Regula-

> mento Geral de Proteção de Dados (RGPD). Apenas se um tratamento de dados disser respeito a dados pessoais, aplica-se o Regulamento Geral de Proteção de Dados. O termo está definido no art. 4 (1). Os dados pessoais são quaisquer informações que estejam relacionadas com uma pessoa singular identificada ou identificável.

Há um variado conjunto de disposições presente na GDPR que levam ao conceito e a classificação dos dados pessoais, cuja expressão e referência, à própria pessoa natural (e não a pessoa jurídica), as regras dizem respeito.

Para tanto, são reputadas de pertinência os dispositivos seguintes, constantes da GDPR:

> [...] a lei estabelece que as informações para uma referência pessoal devem se referir a uma pessoa física. Em outras palavras, a proteção de dados não se aplica a informações sobre pessoas jurídicas como corporações, fundações e instituições. Já para as pessoas físicas, a proteção começa e se extingue com a capacidade jurídica. Basicamente, uma pessoa obtém essa capacidade com seu nascimento e a perde com sua morte. Os dados devem, portanto, ser atribuíveis a pessoas vivas identificadas ou identificáveis para serem considerados pessoais.

A respeito do alcance dos dados pessoais, uma vez que a definição inclui "qualquer informação", deve-se assumir que o termo "dados pessoais" deve ser interpretado da forma mais ampla possível, enquanto que, também não é esperado que os dados pessoais usufruam de objetividade tamanha que a sua própria especificidade dê conta por si mesmo[78]. Portanto, "Informações subjetivas como opiniões, julgamentos ou

78 A GDPR indica alguns exemplos relativos a informações menos explícitas, que poderiam emitir interpretação duvidosa, tais como "registros de horários de trabalho que incluam informações sobre o horário em que um funcionário começa e termina sua jornada de trabalho, bem como pausas ou horários que não caiam no horário de trabalho, como dados pessoais. Além disso, as respostas escritas de um candidato durante um teste e quaisquer observações do examinador sobre essas respostas são "dados pessoais" se o candidato puder ser identificado teoricamente. O mesmo também se aplica aos endereços IP. Se o responsável pelo tratamento tiver a faculdade legal de obrigar o prestador a fornecer informações adicionais que lhe permitam identificar o utilizador por detrás do endereço IP, isso também são dados pessoais" (GDPR, 2022).

estimativas podem ser dados pessoais. Assim, isso inclui uma avaliação da credibilidade de uma pessoa ou uma estimativa do desempenho do trabalho por um empregador" (GDPR, 2022).

No mais, há uma classificação de pertinência destacada pela GDPR (2022), relacionada a seguinte categorização: os *dados gerais*; e, também, as *categorias especiais de dados pessoais* denominados *dados pessoais sensíveis* - que são altamente relevantes porque estão sujeitas a um nível mais alto de proteção, tais como os *dados genéticos, biométricos e de saúde,* bem como *dados pessoais* que revelem a origem racial e étnica, opiniões políticas, convicções religiosas ou ideológicas ou filiação sindical.

Além da regulamentação, conforme anotado anteriormente, constante da GDPR, uma interessante consideração é apresentada por Laura Mendes a respeito da possibilidade de que "os dados se refiram a pessoas indeterminadas" (2019, p. 56). Nessa hipótese, são considerados dados anônimos e podem ser utilizados para fins estatísticos" (2019, p. 56), o que se encontra referendado pelo Regulamento Europeu[79], de modo que,

Após adquirirem a característica de anônimos, os dados não estão mais sujeitos à disciplina da proteção de dados pessoais, se tiverem sido tratados de modo a impossibilitar toda e qualquer identificação pessoal. Isso porque a tutela jurídica abrange apenas aqueles dados que se referam à pessoa identificada ou identificável. (MENDES, 2019, p. 57).

79 É o que dispõe a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, no "Considerando de nº 26": **"**Considerando que os princípios da protecção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável; que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa; que os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável; que os códigos de conduta na acepção do artigo 27º podem ser um instrumento útil para fornecer indicações sobre os meios através dos quais os dados podem ser tornados anónimos e conservados sob uma forma que já não permita a identificação da pessoa em causa". **(**DIRETIVA 95/46/CE, 2022).

iii) dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD), de 2019:

A Lei 13709, de 2018, assim define os dados pessoais, mediante a seguinte classificação (BRASIL, 2022):

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

A esse respeito, tem-se um pertinente posicionamento doutrinário:

> [...] a proteção de dados pessoais não se limita aos dados sensíveis, de modo que os níveis de proteção (e o correspondente rigor do escrutínio em termos de controle da legitimidade constitucional de alguma intervenção restritiva) são maiores quanto mais estiver em causa a esfera mais interna da privacidade designadamente, a intimidade. (SARLET, 2021, p. 33).

Tendo em vista a forte conexão entre conceitos e práticas, dado e informação ocupam a cena em muitos países em todo o mundo, com tamanha força e disposição a dar conta do alcance, dos limites e dos desafios da tutela jurídica em face dos dados pessoais e a dimensão de seu tratamento. Com mais frequência, os processos contemporâneos de proteção dos direitos envolvem o debate público e a consulta de partes interessadas para um debate que envolve especialistas e a sociedade como um todo, verdadeiro instrumento de reflexão produtiva sobre o papel da terminologia de melhorias significativas, em contextos regionais, nacionais e internacional.

Seja como for, repousa sobre os dados pessoais uma tarefa urgente, quer pela rastreabilidade do próprio dado, quer pelos desafios que inauguram uma nova tomada de consciência, tem-se inolvidável tarefa em face da gramática dos direitos de proteção de dados pessoais, tomados em sua expressão de privacidade e de desenvolvimento da personalidade da pessoa, dos quais a atualidade é testemunha, referentes à unidade e à diversidade da espécie humana. Para tanto, a lição de Tzvetan Todorov é um convite inescusável ao tema:

> Os seres humanos se parecem e diferem ao mesmo tempo: observação trivial que cada um pode fazer por si mesmo, já que as formas de vida divergem em todos os lugares e a espécie (biológica) é uma só. Tudo é questão de saber até onde se estende o território da identidade e onde começa o da diferença; que relações exatamente esses dois territórios mantêm. A reflexão sobre essas questões tomou, durante os séculos passados, a forma de uma doutrina das raças. (1993, p. 107).

Nestes tempos em que o campo teórico e o doutrinário, inclusive a pesquisa, sobretudo, com a chegada e a permanência da Covid-19[80], experimenta novas tecnologias, a proteção dos dados parece estar sendo substituída pela experiência e pela simulação, antes que pela evidência, a demonstração e o método, fazendo com que os dados ganhem espaço, a representar a consciência digital e o diálogo universal da sociedade informacional. Sua metodologia é o seu próprio tratamento; sua expressão, a imagem e o ícone; sua gramática, a informação em potencial: a linguagem, a técnica e o contrato; seu resultado é a leitura de si mesmo, os algoritmos que nos possibilitam a sua construção.

80 Em 2021, as iniciativas legislativas e políticas que abordam novas tecnologias centraram-se na gestão dos riscos que a crescente digitalização de todos os aspectos da vida criou. Dossiês fundamentais relacionados com a inteligência artificial (IA) e com a moderação de conteúdos em linha estiveram em destaque. Situações de emergência relacionadas com a gestão da pandemia testaram, na prática, os princípios de proteção de dados; o mesmo aconteceu com o desenvolvimento de medidas relacionadas com a segurança. (INFORMATIVO STF, 2022).

3. UM MUNDO MINADO: O QUE NOS PROPÕE E AGUARDA A PRIVACIDADE E A ÉTICA

O tema ora proposto (privacidade) é analisado em conjunto com a ética, e, com o objetivo de fornecer uma compreensão em face da proteção dos direitos, quase como descobrir o lado humano do ambiente digital. Para tanto, analisa-se a temática posta em contato com a internet e seus processos, seguindo uma tomada de proteção, por concepção e por padrão, ou, em outras palavras, em privacidade desde a concepção e privacidade por padrão, os quais correspondem respectivamente a *Privacy by Design* e *Privacy by Default.* Essas duas metodologias são fundamentais na cultura de dados pessoais, cujos significados tem a ver, o *primeiro*, com uma política de prevenção voltada à privacidade de ponta a ponta, desde a concepção e o planejamento, um *framework* em todas as etapas do processo, da prática, do produto e do serviço, a dar conta de uma reviravolta no modo de garantir a privacidade e a proteção de direitos e liberdade dos indivíduos.[81]; o segundo, tem como base a privacidade por padrão, de modo que, quando um produto ou serviço estiver a disposição do grande público, as configurações mais seguras de privacidade deverão ali constar, por padrão, dispensando a atuação do usuário final nesse aspecto, que também, deverão usufruir de dados pessoais protegidos dentro de uma realidade de uso mínimo ideal, mantido apenas no tempo necessário para dar conta da finalidade pretendida.

Traduzida de forma mais significativa, *Privacy by Design* e *Privacy by Default,* ambos, estão a provocar uma mudança substancial na forma como os dados pessoais dos indivíduos, estão sob responsabilidade na dinâmica dos negócios, dos serviços e dos mercados, fundindo vida

81 O conceito de Privacy by Design está previsto na LGPD, de 2018, artigo 46 §2º. Segundo Jardim (2022), "O objetivo é introduzir a privacidade e a proteção de dados desde a idealização. Dessa forma, não é necessário nenhum tipo de adequação e os riscos já são previstos e eliminados na concepção do próprio projeto."

real à digital. No dizer de Martins e Guariento (MIGALHAS, 2022):

> Nesse contexto, o conceito por trás do privacy by design é de que todo o processo de engenharia de um produto ou serviço que envolva o tratamento de dados pessoais deve garantir a proteção da privacidade, enquanto direito à intimidade. Na prática, impõe ao agente de tratamento de dados o dever de assegurar que a privacidade esteja incorporada ao sistema durante todo o ciclo de vida e em todos os elementos/etapas do produto ou serviço.

Em relação ao *Privacy by Default* referem os mesmos autores, Martins e Guariento:

> O *privacy by default*, por sua vez, pode ser considerado uma decorrência natural do privacy by design, pois incorpora a ideia de que o produto ou serviço seja comercializado com todas as salvaguardas de privacidade concebidas durante o seu desenvolvimento. (MIGALHAS, 2022).

Em uma larga medida, quando se refere à privacidade em contraponto com a ética, há um fio que os une. Trata-se da confiança, uma espécie de "it", um "quê" a nos mover perante as relações estabelecidas na esfera dos dados pessoais, e do qual também não podem ser desprezados a cibersegurança e o fator humano – ambos, no final das contas, são decisivos à engenharia social. Esse cenário, na esfera tecnológica e da IA, trata de "assegurar que os dados serão utilizados de forma ética, transparente e para finalidades benéficas para o usuário" (LEMOS e BRANCO, 2021, p. 449), verdadeiro referendo, uma medida fundamental para a dupla Privacy by Design e Privacy by Default.

Em se tratando do mundo digital, a questão das ameaças cibernéticas e segurança dos ambientes tem um valor inestimável à vida humana e sua organização. Ilustra essa questão, o fato de que, através do relatório "*The Global Risks Report*" (GRPS 2019), é apontado o ataque cibernético na qualidade de "o quarto maior risco à humanidade", enquanto o "*The Global Risks Report*" - GRPS 2022, quanto aos "esforços internacionais de mitigação de riscos" anui que a Inteligência Artificial, explora-

ção espacial, transfronteiriça, ciberataques e desinformação e migração e refugiados são as áreas em que o estado atual dos esforços de mitigação de risco cai aquém do desafio - ou seja, os esforços "não são iniciados" ou estão em "desenvolvimento inicial", abaixo de temas como o "comércio e facilitação", "crime internacional" e "armas de destruição", em que a grande maioria percebeu a mitigação do risco e os esforços para serem "estabelecidos" ou serem "efetivos. (GRPS, 2022, p. 7 e 45-46).

Resguardadas as diferenças, os riscos tecnológicos em suas múltiplas dimensões expõem a vida: de um lado a vida real e sua permanência, de outro, a fragilidade da vida digital em face do comportamento humano, a ofertar verdadeiras condições para o sofrimento digital "Digital Distress". Os números nesse sentido, apresentados pelo *The Global Risks Report (2022)* oferecem um breve retrato da situação exposta: 3 milhões são a lacuna em profissionais cibernéticos necessários em todo o mundo; US$ 800 bilhões é o número por trás do crescimento estimado no valor do comércio digital até 2024; enquanto 95% dos problemas de segurança cibernética são rastreados por erro humano (GRPS, 2022, p. 45).

Com efeito, frente a fusão da vida real e digital, o propósito deste estudo, apresenta a importância das estratégias e metodologias de privacidade, segurança e ética, desde a criação, concepção ou desenho, minimizando os riscos para a proteção dos direitos de dados das pessoas naturais, tendo em conta que, na esfera da ética e da privacidade, tanto por ocasião da definição dos meios de tratamento como no momento do próprio tratamento, medidas técnicas e organizacionais adequadas, cujas decisões que afetam as pessoas devem ser justas, transparentes e sujeitas à contestação, de forma que, as novas tecnologias possam nos ajudar a enfrentar os grandes desafios do mundo atual, desde a vertiginosa desigualdade, as crises ambientais, a comercialização desenfreada dos dados, o avanço do preconceito de gênero e etnia, ameaças significativas à privacidade, à dignidade especialmente em razão do transumanismo, os perigos de vigilância em massa e o aumento de tecnologias de IA não

confiáveis na aplicação da lei, para citar alguns exemplos, e, assim, evitar o avassalador crescimentos dos números nesse sentido.

Lançar mão do tema da privacidade e colocar referida categoria no centro do debate científico é mesmo uma tarefa que diz respeito a todos, porque se trata de uma proposição que ocupa o local, o regional, o nacional e pode ir além, até mesmo avançar e chegar ao campo da ética, de modo que, ao pretender examinar a privacidade e a ética em contraponto a questão dos dados pessoais, tendo por pano de fundo a inteligência artificial, é certo que se está a enfrentar o novo cenário de hiperconectividade, Internet das Coisas e os parâmetros que nortearão a sociedade, moldada pela tecnologia, de forma que, "o avanço das coisas inteligentes cada vez mais autônomas e simbióticas às relações sociais" (MAGRANI, SILVA e VIOLA, 2019, p. 116) podem fornecer uma melhor compreensão "do grau de influência que artefatos não humanos podem exercer sobre nós, incluindo nesta perspectiva as discussões sobre algoritmos e inteligência artificial, pensando sob um ponto de vista regulatório" (MAGRANI, SILVA e VIOLA, 2019, p. 116), cujo significado tem a ver com a privacidade, a ética e a inteligência artificial, cujos exemplos, podem ser encontrados nos vazamentos de dados pessoais, na exposição incontrolada de imagem e na violação de direitos, sendo que, as consequências imprevisíveis e incontroláveis, podem culminar com uma solução inesperada que pode tanto implicar em desativar o sistema de IA, quanto arruinar a identidade de uma pessoa e, ainda, colocar em perigo a vida humana.

A assunção da privacidade e da ética na temática tecnológica enseja a construção de padrões universais para fornecer respostas a essas questões. Também é tradutora de rupturas e disrupção, o que se encontra justificado em três níveis, conforme pode ser encontrado em Rodotá (2008, p. 125), a saber: *i)* pela difusão das coletas de dados pessoais, cada vez mais amplas e especializadas, cujos sujeitos tiveram o cuidado de deslocar o eu de cada pessoa para lugares diversos, indeterminados e intangíveis; *ii)* a unidade da pessoa partiu-se e, como tal, despontam as

pessoas eletrônicas, e tantas pessoas criadas pelo mercado quantos são os interesses que estimulam a coleta das informações, de modo que avançamos rumo a "abstrações no cyberspace", de indivíduos multiplicados, não por assunção de identidades múltiplas, mas por força das relações de mercado; *iii)* uma resposta a esse estado de coisas deve ser conferido pelo reconhecimento de um direito à autodeterminação informativa, do qual deriva a necessidade do fortalecimento de poderes exercidos por todos, o que depende da produção de regras e da arquitetura dos diversos sistemas.

Quanto a privacidade, não é difícil vislumbrar suas possibilidades de transpor fronteiras e margens, da mesma forma, em complemento aos seus muitos caminhos e significativos paradoxos, é possível que referida categoria seja examinada como fonte de integração, um sinal concreto, um "cânon"[82] a seguir. Recorre-se ao lugar comum pelo que se entende quanto ao cânon da privacidade – qual seja, o "mundo" que antecede ou é parelho ao público – e se desvela em um novo e fechado mundo onde é preciso uma lógica de resguardar o recôndito, o sagrado, o íntimo, a honra, a imagem, a identidade, a intimidade, como também, aquilo de que não quero falar, nem dizer, onde a palavra, a voz e a visão, por exemplo, não devem chegar.

Pertinente a privacidade e a importância que a categoria vem experimentando, recorre-se à(s) palavra(s) do ano com o propósito de verificar a adoção do tema pela sociedade e mais do que isso, a insistência com que essas palavras tem feito alusão e confirmado a preocupação com a cultura tecnológica, a dizer muito mais a exposição, o estar nas redes, e menos, a cultura do esquecimento e do cancelamento – especialmente essa última expressão que passa a funcionar como um "biomarcador' das redes, enquanto a privacidade insiste em ser lembrada ou, pelo menos,

82 As aspas no sentido que lhe empresta o texto, tem uma razão maior: além do próprio significado que o termo encerra e, nesse aspecto, vem a favor a intenção do texto.

em ter reconhecida sua relevância[83]. Os fatos e eventos que motivaram a escolha de tais expressões como as palavras do ano pelos principais dicionários certamente dão indícios da atualidade e importância do tema da pesquisa, conforme se demonstra a seguir.

Curiosamente, dentre as palavras do ano[84], eleitas nos dois últimos anos, em que pese os avanços da tecnologia e a prioridade que ela se converteu nos últimos tempos, com alta expressividade e presença tecnológica nas relações, no serviço, no mercado e no cotidiano, há pouca referência relativa ao tema, conforme se denota das expressões retiradas do Dicionário da Oxford, para 2020, (UTSCH, 2022), quais sejam, *Cancel Culture* (Cultura do Cancelamento), cujo termo refere-se à adoção junto as redes sociais para boicotar ou retirar o apoio a alguém; *unmute* (liberar o áudio) e *remotely* (remotamente), muito usadas na nova forma de trabalho adotada por milhões de pessoas no mundo, sendo que, na mesma linha, em 2018, o *Dictionary.com* escolheu *misinformation* como a palavra do ano[85], como, também, Fake News[86].

---

83 Ressalta-se que o objetivo, nesse momento, não é abordar com maior profundidade os casos indicados na sequência, mas apenas traçar os seus aspectos gerais, com o intento de justificar a atualidade e importância da temática. Consta a seguinte definição no Dicionário Collins (2022): "informação falsa, muitas vezes sensacionalista, disseminada sob o disfarce de reportagem de notícias".

84 Sobre a palavra do ano é de ser levado em conta que "A escolha `deve refletir o ethos, o estado de espírito e as preocupações´ e ter `o potencial para ser um termo com potencial duradouro". Já em 2021, a palavra escolhida foi "Vax", enquanto em 2013, foi "Selfie" e em 2016, "Pos-Truth". (Folha de S. Paulo, 2022).

85 Segundo o Dicionário, trata-se de "informações falsas que se espalham, independentemente de haver intenção de enganar". (*DICTIONARY.COM,* 2018).

86 Consta a seguinte definição no Dicionário Collins (2022): "informação falsa, muitas vezes sensacionalista, disseminada sob o disfarce de reportagem de notícias". Confirmada, por exemplo pela expressão *Fake News* escolhida em 2017 pelo *Collins Dictionary (2022).* De acordo com reportagem do *Independent,* "o uso do termo - que muitas vezes tem sido usado pelo presidente dos EUA, Donald Trump - aumentou 365% desde 2016" (tradução livre). *INDEPENDENT*, 2017. ***'Fake news' named Collins Dictionary's official Word of the Year for 2017.*** Disponível em: https://www.independent.co.uk/news/uk/home-news/fake-news-word-of-the-year-2017-collins-dictionary-donald-trump-kellyanne-conway-antifa-corbynmania-a8032751.html. Acesso em: 16 dez. 2021.
Sobre a palavra do ano é de ser levado em conta que "A escolha `deve refletir o ethos, o estado de

As escolhas levadas a termo funcionam como uma chave mestra, um confessionário público, revelador da atenção que os serviços, os mercados, os países e as instituições que se dedicam ao tema, mas bem pode traduzir uma outra realidade, a de "esquecimento' em relação a questões fundamentais da atualidade.

Diante desse cenário, está claro que a esfera tecnológica, inobstante sua presença incontestável nas relações humanas, parece ocupar o outro lado dessa mesa de negociação, sendo que, do lado de cá, está a vida que segue, do lado de lá as questões que precisamos levar em conta para uma organização adequada e em conformidade.

A menos que possamos refletir sobre esses desafios, e tomar sentido e consciência quanto as arestas que precisam ser aparadas e daquelas que haveremos de construir e, também, reconstruir, é bem possível que essa configuração pertence a um arranjo (talvez até um engodo) que precisa urgentemente ser corrigido, ou pelo menos tomado em real reconhecimento, sobretudo quando se pensa na alocação digital e exposição que está sendo levada a termo em razão da privacidade das pessoas, particularmente em relação à geração atual e a futura.

É que, em um mundo rodeado de tecnologias da mais alta e significativa conexão, e, também, habitado por homens, mulheres, crianças e jovens – nesse caso, seres humanos em dinâmica digital – cuja acessibilidade tecnológica assiste e integra a vida real à digital, e do outro lado da mesa – agora sim – estão sentadas as ameaças digitais. Contudo, esse "banquete" não parece corresponder razão para saudá-lo, a menos que novas metodologias venham em socorro desses processos.

Segundo a lição de Cathy O´Neil, as aplicações fomentando a eco-

espírito e as preocupações´ e ter `o potencial para ser um termo com potencial duradouro". Já em 2021, a palavra escolhida foi "Vax", enquanto em 2013, foi "Selfie" e em 2016, "Pos-Truth". (Folha de S. Paulo, 2022).

nomia dos dados foram baseadas em escolhas feitas por seres humanos falíveis, mesmo que com as melhores das intenções. Mas os que esses modelos cumpriam (ainda que às avessas), eles programavam preconceitos, equívocos e vieses humanos nos sistemas de *softwares* e, cada vez mais, passavam a gerir a vida, mesmo que essas decisões, fossem erradas ou danosas (2020, p. 8).

A consequência é que, por intermédio desses algoritmos – o caminho era mesmo de "destruição de massa" ou de "Armas de Destruição Matemáticas" conforme revela a autora (2020), e "tendiam a punir os pobres e oprimidos da sociedade enquanto enriquecia ainda mais os ricos" (O´-NEIL, 2020, p. 8). A esfera da privacidade em contato com a ética parece mesmo restar esquecida e há uma urgente recuperação e enaltecimento neste sentido.

Os fatos e eventos, e muito mais os cientistas, tem sido reveladores e confirmadores de um aspecto que este estudo pretende expor, ainda que de forma breve: justificar os indícios da atualidade e da importância do tema da privacidade na dimensão do mundo *on-line* e *off-line*.

4. UM MUNDO TECNOLÓGICO E EM CONSTRUÇÃO NA SOCIEDADE DA INFORMAÇÃO: DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL – O QUE ESPERAR DESSA GIGANTE INTELIGÊNCIA(?)

Como nossa dependência de tecnologias digitais cresce e a Internet 5.0 está prestes a se tornar realidade, esforços destinados a construir normas e definir regras de comportamento e de atuação no ambiente digital estão se intensificando a passos largos. A esse título e em uma construção evolutiva, revolutiva e disruptiva, alguns documentos foram cele-

brados visando a celebração de um diálogo global e o estabelecimento de padrões universais para fornecer uma resposta às questões da privacidade, da ética, da proteção de direitos relacionadas à inteligência artificial. Desse universo, "Em 24 de novembro de 2021, a **Recomendação sobre a Ética da Inteligência Artificial** foi adotada pela Conferência Geral da UNESCO em sua 41ª sessão" (UNESCO, 2022), o qual adveio de esforços da UNESCO originário de "um processo de dois anos para elaborar **este primeiro instrumento global de definição de padrões sobre a ética da inteligência artificial na forma de uma recomendação**, seguindo a decisão de sua Conferência Geral em sua 40ª sessão em novembro de 2019" (UNESCO, 2022).

Referida recomendação aborda questões éticas relacionadas a inteligência artificial, a dizer:

> Ela aborda a ética da IA como uma reflexão normativa sistemática, com base em um marco holístico, abrangente, multicultural e em evolução de valores, princípios e ações interdependentes que podem orientar as sociedades para que lidem de forma responsável com os impactos conhecidos e desconhecidos das tecnologias de IA sobre seres humanos, sociedades, meio ambiente e ecossistemas, oferecendo-lhes uma base para aceitar ou rejeitar essas tecnologias. Ela considera a ética como uma base dinâmica para a avaliação e a orientação normativa das tecnologias de IA, fazendo referência à dignidade humana, ao bem-estar e à prevenção de danos – como uma bússola e tendo como fundamento a ética da ciência e da tecnologia. (UNESCO, 2022).

Enquanto diálogos internacionais multissetoriais estão despertando parcerias e cooperações, documentos como este podem ajudar a fortalecer os vínculos entre os parceiros, enquanto cooperação entre organizações pode desencadear boas práticas que podem ser alcançar novos públicos e até serem replicadas no campo econômico e inovacional. Em tempos de tecnologias emergentes, tais como blockchain, *quantum,* inteligência artificial e metaverso.

A sociedade conectada não prescinde de um valoroso aspecto: trata-se da confiança digital cujo sentido revela a imprescindibilidade de um elo entre os governos, cujo sentido é o da cooperação, da comunicação e do diálogo, a afastar barreiras desfazer processos de colonização digital oriundos de monopólios dos sistemas digitais, cuja finalidade tem em sua base fins geopolíticos, evitando que ataque, interrupções se tornem um instrumento de opressão e evidente perda de confiança. É verdade que os governos, as empresas e as instituições poderão enfrentar o inconformismo da sociedade acaso sejam incapazes de reverter o cenário de constante negativa de inclusão e de governança na responsabilidade desses desafios.

De outro lado, as ameaças cibernéticas estão engrossando as fileiras de vazamento de dados pessoais e a menos que mantenhamos vigilância e o estabelecimento de regulamentos e medidas regulatórias entre os povos, os cidadãos e demais cadeias de fornecedores, é possível que os riscos se tornarão cada vez mais evidentes e precários, de forma que, quando ocorrer um ataque, as empresas serão obrigadas a se envolver com o pagamento de resgates cada vez mais sui generis e capciosos, além de sofrer pesada violação de imagem, e consequências reputacionais, legais e financeiras significativas.

Da mesma forma que o impacto de ataques cibernéticos disruptivos podem ser financeiramente devastador para aqueles que deixam de investir em mecanismos de proteção, de infraestrutura, de segurança e de formação educativa, de forma que, Tecnologias confiáveis, por sua vez, representam a base sobre a qual o andaime de um justo e coeso sociedade é construída. A menos que atuemos para melhorar a confiança digital com persistência, propósito e iniciativas de construção de confiança, o mundo digital continuará exposto e em risco, prejudicando a construção das dimensões do progresso humano. Nessa tarefa a própria inteligência artificial tem um papel preponderante pela capacidade e proposição do que consegue estabelecer, corrigir e destruir.

A seu respeito, há múltiplas definições, não sendo conveniente a proposição de uma definição única de inteligência artificial, inclusive porque se trata de temática em construção – que está em desenvolvimento – como, também, decorre com a proteção de dados pessoais e, também, o mesmo se pode considerar em relação a privacidade e a ética. Diante desse cenário, a Recomendação Ética da UNESCO fornece uma interessante abordagem, a qual considera "os sistemas de IA como sistemas que têm capacidade de processar dados e informações de uma forma que se assemelha ao comportamento inteligente e, normalmente, inclui aspectos de raciocínio, aprendizagem, percepção, previsão, planejamento ou controle" (UNESCO, 2022).

A título de eleger alguns aspectos definidores da IA, incluindo a internet das coisas, sistemas robóticos, robótica social e interfaces ser humano– computador, os quais podem ser ditos decisivos na proteção de direitos relacionados à proteção de dados pessoais, exatamente porque relacionados à abordagem ética e à própria privacidade, motivo pelo qual, recorre-se a alguns elementos decisivos para este estudo, tomados em empréstimo da Recomendação Ética da UNESCO (2022):

> Os sistemas de IA são tecnologias de processamento de informações que integram modelos e algoritmos que produzem a capacidade de aprender e realizar tarefas cognitivas, as quais levam a resultados como a previsão e a tomada de decisões em ambientes reais e virtuais. Os sistemas de IA são projetados para operar com vários graus de autonomia por meio da modelagem e da representação de conhecimento e pela exploração de dados e cálculo de correlações. Os sistemas de IA podem incluir vários métodos, tais como, mas não se limitando a: (i) aprendizado de máquina, incluindo aprendizado profundo e aprendizado por reforço; e (ii) raciocínio de máquina, incluindo planejamento, programação, representação de conhecimento e raciocínio, pesquisa e otimização. (UNESCO, 2022).

Na doutrina também é encontrado um posicionamento a respeito da IA, de modo que, a inteligência artificial na lição de Kelley K. H. et al, encontra-se definida porquanto um sistema de computador com sensi-

bilidade sobre o seu ambiente, dotado de compreensão, aprendizado e cognição. A ferramenta, passível de programação, confere reproduções voltadas às características humanas, visando executar tarefas de modo similar ou superior aos seres humanos, de que são exemplos, as principais formas de inteligência artificial, a *machine learning*, os carros autônomos, e as assistentes digitais (2018, p. 373).

Além do mais, Italo S. Vega (2019, p. 102) confirma que

> A IA é uma ciência e tecnologia baseada em disciplinas como ciência da computação, biologia, psicologia, linguística, matemática e engenharia. Um grande impulso da IA foi o desenvolvimento de funções computacionais normalmente associadas à inteligência humana, como raciocínio, aprendizado e solução de problemas.

De modo prático, os sistemas de IA envolve pesquisa, *design*, desenvolvimento implementação, uso, manutenção, operação, comércio, financiamento, monitoramento, avaliação, validação, desmontagem, término, controle, percepção e processamento dos dados coletados por sensores e a operação de atuadores no ambiente em que os sistemas de IA funcionam, enquanto que, na expressão dos profissionais envolvidos com a IA, o envolvimento dos mesmos ocorrem em relação a uma etapa do ciclo de vida do sistema de IA.

Nesse espírito, oferecemos uma lista de questões com relevância ética em **IA** e pertinentes à privacidade, que inclui mas não limita a proteção de dados pessoais, as quais afetam a tomada de decisões, e múltiplas outras áreas, tais como, a interação social, os meios de comunicação, o acesso à informação, a proteção ao consumidor, o meio ambiente, a democracia, o Estado de Direito, a segurança, o policiamento, o emprego, o trabalho, a assistência médica, a educação, a exclusão digital, os dados pessoais, os direitos humanos e as liberdades fundamentais – no caso, a liberdade de expressão, a privacidade e não discriminação, a liberdade de consciência.

É preciso levar em consideração os novos desafios éticos e os relacionados à privacidade, criados pela possibilidade de que os algoritmos de IA reproduzam e reforcem vieses existentes, como, também, podem estabelecer e até agravar outros mais, até aqueles previamente existentes, tais como, a discriminação e o preconceito. No médio e no longo prazo, a adoção de proteção de dados pessoais poderá reforçar os direitos da privacidade, mas a urgência com que os sistemas de IA parecem desafiar o sentido da experiência e da capacidade humana, está a conferir preocupações complementares, desde o valor da dignidade, e as questões de ordem cultural, social, ambiental, a autonomia, a autocompreensão humana, a capacidade de ação e a questão jurídica.

5. CONSIDERAÇÕES FINAIS

A tecnologia, especialmente a inteligência artificial, no conjunto de sua expressão é aquela que mais visivelmente incorpora o futuro. Ela se transforma, permite oportunidades, mas também lança novas vulnerabilidades. A seu respeito, não se pode negar ou afastar o que importa: a própria tecnologia, e, não a sua abominação, nem a confiança cega na tecnologia. Em face da mesma, em termos positivos ou negativos, convém bom senso.

Diante desse contexto, propôs-se examinar a proteção de dados, a privacidade e a ética na perspectiva da inteligência artificial disposta na sua própria historicidade, desde seus estudos iniciais, passando pelo planejamento, concepção, *design*, aplicação, conexão e comunicação, a IA requer a adoção de técnicas mínimas e razoáveis de conformidade, seja com a proteção de dados pessoais, com o estabelecimento de um padrão voltado à ética, cujo significado, em específico, é um só: dados, privacidade e ética precisam compor uma amálgama de justiça e de razoabilidade, a dizer, legítimos interesses voltados à proteção dos direitos de todos.

Essas características conferem aos sistemas de IA um novo e profundo papel nas práticas humanas e sociais, e na relação com o meio ambiente, criando com isso um novo contexto para as pessoas desenvolverem uma compreensão do mundo e de si mesmos, entenderem criticamente os meios de comunicação e as informações, e aprenderem a tomar decisões. Tudo isso sem escurar da importância da proteção dos direitos, sem os quais, a vida e suas relações poderão estabelecer tempos difíceis e sistemas de IA ingratos.

A inteligência artificial e as novas tecnologias e seus arranjos, estão transformando a sociedade rapidamente e devem continuar transformando nas próximas décadas. Essa transformação de ordem social, histórica, cultural, política e digital, terá impactos éticos profundos, podendo tanto melhorar como prejudicar a vida humana e suas relações. A IA, tanto quanto a **inteligência humana,** e a entrega inteligente de direitos, oferecem o que a humanidade é e vislumbra, tanto em sua medida de maldade e de bondade, como, também, em humanidade e inteligência. Haveremos de ter cuidado e lucidez para não alimentar o lado mais sombrio da nossa natureza, e zelar pelo protagonismo da inteligência artificial, sem desmerecer a memória, o testemunho, a experiência e a presença humana na própria história da humanidade.

6. REFERÊNCIAS

BRASIL. **Lei 13709**, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 set. 2022.

COLLINS DICTIONARY, 2018. **Fake News.** Disponível em: https://www.collinsdictionary.com/pt/dictionary/english/fake-news. Acesso em: 16 set. 2022.

DICTIONARY.COM, 2018. **Misinformation.** Disponível em: https://www.dictionary.com/browse/misinformation. Acesso em: 14 dez. 2018.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais:** elementos da formação da proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil - Revista dos Tribunais, 2019.

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 28 set. 2022.

Folha de S. Paulo. Disponível em: https://www1.folha.uol.com.br/mundo/2021/11/dicionario-oxford-elege-vax-neologismo-para-vacina-palavra-do-ano-na-lingua-inglesa.shtml. Acesso em 25 ago. 2022.

Reuters Brasil, 2019.

INFORMATIVO STF. Brasília: Supremo Tribunal Federal, Secretaria de Altos Estudos, Pesquisas e Gestão da Informação, n. 1068/2022. Disponível em: http://portal.stf.jus.br/textos/verTexto.asp?servico=informativoSTF. Data de divulgação: 23 de setembro de 2022.

JARDIM, Mário. LGPD: Privacy by Design não é frenesi. 22 novembro 2021.

Disponível em: https://www.convergenciadigital.com.br/Opiniao/LGPD%3A-Privacy-by-Design-nao-e-frenesi-58790.html. Acesso em: 29 set. 2022.

KELLEY,K . H., FONTANETTA, L. M.; HEINTZMAN, M., PEREIRA, N. **Artificial Intelligence: implications for Social Inflacion and Insurance -** Risk Management and Insurance Review., 2018, p. 373.

MAGRANI, Eduardo; SILVA, Priscila; VIOLA, Rafael. Novas perspectivas sobre ética e responsabilidade de inteligência artificial. In: FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial e Direito:** ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

MARTINS, Ricardo Maffeis. GUARIENTO, Daniel Bittencourt. **Privacy by design, by default e by redesign.** MIGALHAS. 21 de maio de 2021. https://www.migalhas.com.br/coluna/impressoes-digitais/345919/privacy-by-design-by-default-e-by-redesign. Acesso em: 30 set. 2022.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. 2ª. tiragem. São Paulo: Saraiva, 2019.

O´NEIL, Cathy. **Algoritmos de Destruição em Massa:** como o Big Data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham.1. ed., Santo André-SP: Editora Rua do Sabão, 2020.

Regulamento Geral de Proteção de Dados. Disponível em: https://gdpr-info.eu/. Acesso em: 25 set. 2022.

Rodotá, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro – São Paulo – Recife: Renovar, 2008.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados. In: MENDES, Laura Schertel et al. **Tratado de Proteção de Dados Pessoais.** 2. reimpressão. Rio de Janeiro: Forense, 2021.

The Global Risks Report 2019, 14th Edition. World Economic Forum. Disponível em:https://www.weforum.org/reports/the-global-risks-report-2019. Acesso em: 30 set. 2022.

The Global Risks Report 2022, 17th Edition. World Economic Forum. Disponível em: https://www.weforum.org/reports/global-risks-report-2022/. Acesso em: 30 set. 2022.

TODOROV, Tzvetan. **Nós e os Outros:** a reflexão francesa sobre a diversidade humana. Tradução Sérgio Goes de Paula. Rio de Janeiro: Jorge Zahar Editor, 1993.

UNESCO. Recomendação sobre a Ética da lnteligência Artificial. Aprovada em 23 de novembro de 2022. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 29 set. 2022

UTSCH, Sérgio. 23 novembro de 2020. Disponível em: https://www.sbtnews.com.br/noticia/mundo/154638-pela-primeira-vez-dicionario-oxford-escolhe--varias-palavras-do-ano. Disponível em: 20 ago. 2022.

VEGA, Italo S. **Inteligência Artificial e Direito:** ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

ZUBOFF, Soshana. **A Era do Capitalismo de Vigilância:** a luta por um futuro humano na nova fronteira do Poder. Tradução George Schlesinger. 1. edição. Edição digital. Rio de Janeiro: Editora Intrínseca Ltda, 2021.

Responsabilização civil na LGPD: novos dilemas ou desafios preexistentes na dogmática jurídica?

Civil liability on LGPD: new dilemmas or pre-existing challenges in legal dogmatic?

Jean Marcell de Miranda Vieira

» Advogado. Atualmente ocupa a função de Superintendente Jurídico do Banco do Nordeste do Brasil S/A. Pós-graduado em Direito Público e Privado pela Universidade Federal do Piauí (UFPI) e em Processo Civil pela Pontifícia Universidade Católica de São Paulo (PUC – SP).

» E-mail: jeanmarcellmv@gmail.com.

Bruno Leonardo Câmara Carrá

» Graduado em Direito pela Universidade Federal do Ceará (UFC); Mestre em Direito (Direito e Desenvolvimento) pela Universidade Federal do Ceará (UFC); Doutor pela Universidade de São Paulo (USP). Pós-Doutor pela *Scuola di Giurisprudenza*, da Universidade de Bolonha (Itália). Docente da graduação e da pós-graduação stricto sensu do curso de Direito do Centro Universitário 7 de Setembro (UNI7). É Juiz Federal no Tribunal Regional Federal da 5ª Região.

» E-mail: brunolccarra@gmail.com.

Recebimento: 30/09/2022
Aprovação: 27/10/2022

REVISTA JURÍDICA DO BANCO DO NORDESTE

RESUMO

A racionalidade jurídica que subjaz do regime de responsabilização civil delineado na LGPD foi, mesmo antes de sua entrada em vigor, pauta de inúmeras discussões, as quais estão no foco desta pesquisa, destinada justamente à realização de uma análise dos temas levantados pela comunidade jurídica. A partir de uma pesquisa bibliográfica e jurídica, pretende-se levantar quais são as discussões que permeiam a temática, a fim de se verificar se, de fato, os debates existentes entre os operadores do Direito afiguram-se como novos dilemas especificamente advindos da LGPD ou se, na verdade, os impasses são os mesmos oriundos dos grandes temas afetos à responsabilidade civil como um todo, independentemente das especificidades de uma norma ou outra que venha a prever parte específica para a responsabilização civil e, adicionalmente, radicando o olhar sobre um dos tópicos dessa discussão, verificar, por meio da seleção de algumas decisões judiciais, se o Judiciário brasileiro tem visualizado a natureza da responsabilidade como objetiva ou subjetiva, e como vem tratando a questão atinente à prescindibilidade ou não do liame causal entre a ação/omissão e o dano.

PALAVRAS-CHAVE

LGPD – Responsabilidade Civil – Novos dilemas – Desafios preexistentes – Dano *in re ipsa*

ABSTRACT

The legal rationality that underlies the civil liability regime outlined in the LGPD was, even before its entry into force, the agenda of numerous discussions, which are the focus of this research, aimed precisely at carrying out an analysis of the issues raised by the legal community.

From a bibliographical and legal research, it is intended to raise what are the discussions that permeate the theme, in order to verify if, in fact, the existing debates between the Law operators appear as new dilemmas specifically arising from the LGPD or if the impasses are the same arising from the major issues related to civil liability as a whole, regardless of the specifics of a rule or another that may provide a specific part for civil liability and, additionally, focusing on one of the topics of this discussion, to verify, through the selection of some judicial decisions, whether the Brazilian Judiciary has viewed the nature of responsibility as objective or subjective, and how it has been dealing with the issue regarding the dispensability or not of the causal link between the action/omission and the damage.

KEYWORDS

LGPD – Civil Liability – New dilemmas – Pre-existing challenges – In re ipsa damage

SUMÁRIO

INTRODUÇÃO

No Brasil, a despeito da existência de normas que, de algum modo, regulavam a proteção de dados pessoais (CDC[87], Marco Civil da *Internet*[88], Cadastro Positivo[89] etc.), foi editada norma específica para esse fim, a Lei n. 13.709/18, conhecida como Lei Geral de Proteção de Dados, cujo texto possui parte especificamente dedicada à responsabilização, delineando critérios e circunstâncias que podem dar vez à responsabilização dos agentes ali caracterizados.

Todavia, a racionalidade jurídica imanente ao regime trazido pela LGDP é objeto de inúmeras discussões nas searas teórica e jurídica, as quais serão objeto de levantamento neste artigo, cujo objetivo precípuo consistirá no levantamento dos principais debates na comunidade jurídica, para verificar: a) quais os grandes temas estão em voga e se eles são corolários diretos da própria LGDP ou se, ao fim e ao cabo, afiguram-se como velhos dilemas sobre os quais pairam dissenso quanto ao instituto da responsabilidade civil em si e seus elementos constituintes; b) por meio da seleção de algumas decisões judiciais, se o Judiciário brasileiro tem visualizado a natureza da responsabilidade como objetiva ou subjetiva; e c) como esse mesmo Judiciário vem tratando a questão atinente à prescindibilidade ou não da caracterização do liame causal entre a ação/omissão e o dano.

Para a persecução desse objetivo, lançar-se-á mão de uma linha emi-

87 BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>.

88 _____. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

89 _____. Lei n. 12.414, de 9 de junho de 2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>.

nentemente dogmática, em que se realizará pesquisa bibliográfica e de decisões judiciais que contribuam para a consecução da meta deste ensaio.

Inicialmente, reputa-se imprescindível trazer a lume quais são as bases da responsabilidade civil no Brasil, por meio de um curto histórico evolutivo, sem todavia analisar seus elementos, partindo-se do pressuposto de que o leitor deste artigo as conhece.

Subsecutivamente, a título de sedimentação dos conhecimentos prévios necessários à essência do estudo, apresentar-se-á a estrutura normativa da LGPD, com foco no extrato atinente ao sistema de responsabilização positivado nessa lei.

Por derradeiro, direcionando a pesquisa rumo ao seu cerne, levantar-se-ão os debates travados a partir do regime de responsabilização trazido da LGPD, bem como o conteúdo das dissensões levadas ao Judiciário nacional, visando mapear o seu teor e tentar identificar se as decisões da Comunidade de Justiça brasileira perfilham um entendimento objetivo ou subjetivo quanto à natureza da responsabilidade civil no âmbito da Lei Geral de Proteção de Dados, e como as decisões têm tratado especificamente a questão da prescindibilidade ou não de evidenciação do nexo causal entre ação/omissão e o dano para fins de responsabilização.

1. BREVE HISTÓRICO SOBRE A NATUREZA DA RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

Em geral, a responsabilidade decorre do inadimplemento de uma obrigação ou da inobservância de um preceito normativo (responsabilidade civil contratual/negocial ou responsabilidade civil extracontratual/

aquiliana, respectivamente).[90] [91]

Inicialmente prescindível, a comprovação da culpa passou, a partir da experiência romana, a ser regra, tendo em conta as situações desarrazoadas ensejadas pelo fato de a responsabilidade sem culpa ser regra até então.[92]

Todavia, o Direito Comparado (especialmente o francês), mitigando a força dessa regra, começou a admitir a modalidade sem culpa, que ganhou corpo especialmente a partir de discussões estimuladas pela teoria do risco e a responsabilização, perante a coletividade, dos que desempenhavam algumas atividades.[93]

O Direito Civil brasileiro, que erigiu a responsabilidade civil subjetiva como regra, também se viu influenciado por esse movimento, *v.g.*, a previsão de culpa presumida no tranporte ferroviário trazida pelo Decreto n. 2.681/1912[94], que imputou esse tipo de responsabilidade ao Estado

90 TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. Vol. 2. 17. ed. Rio de Janeiro: Forense, 2022. p. 357.

91 Segundo Carrá: "Fala-se em responsabilidade civil quando nasce para alguém o dever de reparar em virtude dos prejuízos que causou, se o dano adveio de uma ação ou omissão contrária ao ordenamento jurídico. Pode ainda alguém ser chamado a responder por ato de terceiro ou de fato de coisa quando a lei assim o determinar." (CARRÁ, Bruno Leonardo Câmara. Aspectos das modalidades subjetiva e objetiva no sistema atual de responsabilidade civil brasileiro. **Revista Esmafe**: Escola de Magistratura Federal da 5ª Região, Recife, n. 11, p. 187-209, dez. 2006. Disponível em: <https://revista.trf5.jus.br/index.php/esmafe/article/view/75/71>. Acesso em: 29. set. 2022.).

92 TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. *op. cit.* p. 357.

93 TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. Vol. 2. 17. ed. Rio de Janeiro: Forense, 2022. p. 358.

94 BRASIL. Decreto n. 2.681, de 7 de dezembro de 1912. **Regula a responsabilidade civil das estradas de ferro.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d2681_1912.htm>. Acesso em: 13. set. 2022.

pelos atos comissivos de seus agentes, e o CC/1916[95].[96]

Com a sobrevinda da sociedade de consumo em massa, a teoria do risco radicou-se, tanto no Direito Comparado quanto no nacional (anos 70 em diante), repercutindo na imputação da responsabilidade civil objetiva sobre fornecedores de produtos e serviços diante de danos causados aos consumidores, em virtude de sua presumida vulnerabilidade.[97]

Perfilhando a vertente objetivista, o ordenamento positiva norma ensejadora de defesa coletiva de direitos por instituições como o MP (Lei n. 7.347/85[98]), seguida da promulgação da "Constituição Cidadã"[99] em 1988, com diversos e relevantes dispositivos com com essa índole[100] e, como corolário de determinação contida no texto constitucional, o Código de Defesa do Consumidor em 1990, o qual perenizou a responsabilidade civil objetiva como regra para a tutela de seu público-alvo, os consumidores.[101]

Algum tempo depois, nessa mesma toada, o Código Civil de 2002 re-

95 _____. Lei n. 3.071, de 1º de janeiro de 1916. **Código Civil dos Estados Unidos do Brasil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l3071.htm>. Acesso em: 13. set. 2022.

96 TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. *op. cit.* p. 359.

97 *Idem*.

98 BRASIL. Lei n. 7.347, de 24 de julho de 1985. **Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm>. Acesso em: 13. set. 2022.

99 _____. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 13. set. 2022.

100 Segundo enumera Tartuce: "[...] a defesa dos consumidores como norma principiológica (art. 5.º, inc. XXXII), a reparação de danos imateriais ou morais (art. 5.º, incs. V e X), a função social da propriedade (art. 5.º, incs. XXII e XXIII), a proteção do Bem Ambiental (art. 225), a proteção da dignidade da pessoa humana como direito fundamental (art. 1.º, inc. III), a solidariedade social como preceito máximo de justiça (art. 3.º, inc. I) e a isonomia ou igualdade lato sensu (art. 5.º, *caput*)." (TARTUCE, Flávio. Direito Civil: Direito das Obrigações e Responsabilidade Civil. *op. cit.* p. 360.)

101 TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. *op. cit.* p. 360.

força a responsabilidade objetiva ao determinar que "[...] Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."[102]

Por essa lógica, o dever de indenizar subsume-se a uma relação de causa e consequência, a partir da observância de três nuances: ato ilícito, dano, e nexo de causalidade.

Para Tartuce:

> "[...] a responsabilização independente de culpa representa um aspecto material do acesso à justiça, tendo em vista a conjuntura de desequilíbrio percebida nas situações por ela abrangidas. Com certeza, afastada a responsabilidade objetiva, muito difícil seria, pela deficiência geral observada na grande maioria dos casos, uma vitória judicial em uma ação promovida por um particular contra o Estado, ou de um consumidor contra uma grande empresa."

Portanto, embora o CC/02 tenha adotado como regra geral a responsabilidade civil subjetiva, pautada na clássica concepção de que o dever de reparação pressupõe o dano, o nexo causal e a culpa do ofensor[103], não deixou de ser influenciado pela nova realidade, tornando prescindível a caracterização da culpa ao adotar, de modo subsidiário, a responsabilidade objetiva.[104] Assim:

---

102 BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. **Institui o Código Civil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 13. set. 2022.

103 *Ibidem*. "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."

104 A esse respeito, Carrá sopesa que: "Com efeito, nada obstante o fato de parte da doutrina ainda conceber a culpa como elementar na descrição desse fenômeno jurídico, impõe-se a constatação de que coexistem casos de responsabilidade objetiva no ordenamento brasileiro, os quais, como sabido, dispensam qualquer verificação anímica sobre a conduta." (CARRÁ, Bruno Leonardo Câmara. Aspectos das modalidades subjetiva e objetiva no sistema atual de responsabilidade civil brasileiro. **Revista Esmafe:** Escola de Magistratura Federal da 5ª Região, Recife, n. 11, p. 187-209, dez. 2006. Disponível em: <https://revista.trf5.jus.br/index.php/esmafe/article/view/75/71>. Acesso em: 29. set. 2022. p. 191.)

> "O ingresso, no mundo jurídico, da responsabilidade objetiva afasta a ne-cessidade de se continuar considerando a culpa como um dos elementos nucleares da responsabilização civil. Serão, agora, divididas as possibilidades: **de um lado os atos que continuam dependentes da verificação da culpa e, do outro, os fatos, humanos ou não, que causem dano independentemente da análise do aspecto volitivo da conduta.**"[105] (grifo nosso)

Hodiernamente, informa Tartuce, tem-se verificado o surgimento de novas teses, as quais não se estruturam a partir da discussão sobre o elemento culpa, transladando a análise para uma nova modalidade de responsabilização, chamada de pressuposta, segundo a qual, resume o doutrinador, "[...] deve-se buscar, em um primeiro plano, reparar a vítima, para depois verificar-se de quem foi a culpa, ou quem assumiu o risco."[106]

2. A LEI GERAL DE PROTEÇÃO DE DADOS E SEU REGIME DE RESPONSABILIZAÇÃO CIVIL

2.1. LGPD: Caracterização e Conceitos Relevantes

Inspirada no regulamento europeu GDPR (*General Data Protection Regulation*), e promulgada há 4 anos (com uma *vacatio legis* de 24 meses), a Lei Geral de Proteção de Dados brasileira foi criada com o intuito de "[...] proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo"[107], regulando o tratamento de dados pessoais no país por meio de um conjunto

105 *Ibidem*. p. 191.

106 TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. Vol. 2. 17. ed. Rio de Janeiro: Forense, 2022. pp. 360-361.

107 BRASIL. **Guia de Boas Práticas:** Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>. Acesso em: 16. set. 2022.

de determinações e princípios vocacionados à criação de um cenário de responsablidade proativa, em virtude do latente potencial de danos quando da coleta e do tratamento desses dados.

A norma tem incidência ampla[108], apresenta como figuras essenciais os agentes de tratamento (controlador[109] e operador[110]) e o encarregado[111], e assim define tratamento de dados:

> "[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;"[112]

Outrossim, esteia-se num conjunto de princípios, como boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, prestação de contas e, mais relevante para o objeto deste escrito, a responsabilização[113], a qual será melhor discriminada no item subsequente.

---

108 _____. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 16. set. 2022. "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados [...]"

109 *Ibidem*. "Art. 5º [...] VI – [...] pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;"

110 *Ibidem*. "Art. 5º [...] VII – [...] pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;"

111 *Ibidem*. "Art. 5º [...] VIII – [...] pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);"

112 BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 16. set. 2022. Art. 5º, X.

113 *Ibidem*. Art. 6º.

2.2. Responsabilização e Ressarcimento de Danos na LGPD

A LGPD dedicou seção específica[114] em seu texto para tratar da responsabilização e do ressarcimento de danos, não descartando, todavia, a eventual incidência de outras normas[115], de que é exemplo o CDC.

A partir de uma visão da legislação de proteção de dados como uma espécie de microssistema, que tem como cerne a LGDP, a responsabilidade dos agentes de tratamento (controlador e operador) está diretamente associada à atividade de tratamento de dados por eles realizada.

A interpretação conjunta dos artigos 42, *caput*[116]; 44, p. único[117]; e 46[118], todos da LGPD, permite estabelecer duas circunstâncias de responsabilização civil na lei, desde que, claro, a violação ocasione dano a uma pessoa ou à coletividade: "[...] violação de normas **jurídicas**, do microssistema de proteção de dados; e [...] de normas **técnicas**, voltadas

114 *Ibidem*. Seção III do Capítulo VI.

115 *Ibidem*. "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente."

116 *Ibidem*. "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

117 *Ibidem*. "Art. 44. [...] Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

118 *Ibidem*. "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução."

à segurança e proteção de dados pessoais."[119] (grifos do original).

Ademais, há previsão de responsabilização solidária do operador e do controlador, visando a garantia da efetiva indenização da vítima[120], bem como a previsão de inversão do ônus da prova[121], desde que presentes alguns dos requisitos já elencados pelo CDC[122], isto é, verossimilhança da alegação, hipossuficiência para produzir a prova ou excessiva onerosidade para fazê-lo.

Por derradeiro, vale a pena apresentar as excludentes de responsabilização trazidas pela lei, a qual isenta os agentes de tratamento desde que comprovem não ter realizado o tratamento de dados a eles reputado; ou que, malgrado o tenham feito, não violaram a legislação pertinente; ou, ainda, que o dano decorreu exclusivamente de culpa do titular dos dados ou de um terceiro.[123]

---

119 CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, ano 21, n. 53, pp. 163-170, jan-mar. 2020. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712>. Acesso em: 16. set. 2022.

120 BRASIl. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 16. set. 2022. "Art. 42. [...] § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei."

121 *Ibidem*. "Art. 42. [...] § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa."

122 BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Art. 6º, VIII.

123 _____. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. *op. cit.* Art. 43.

3. RESPONSABILIZAÇÃO CIVIL NA LGPD: NOVOS DILEMAS OU DESAFIOS PREEXISTENTES NA DOGMÁTICA JURÍDICA?

3.1. Responsabilidade Civil Objetiva ou Subjetiva?

Ao se pesquisar a respeito de responsabilização civil e LGPD, constatou-se que um dos grandes motes do debate se assenta na natureza jurídica da obrigação de indenizar prevista na lei, isto é, se seria ela subjetiva (e, portanto, analisada a partir do descumprimento de um dever por parte dos agentes de tratamento) ou objetiva e, portanto, amparada na noção do risco da atividade por eles desempenhada.

Uns entendem que a LGDP adotou o regime subjetivo, o que exigirá prova da culpa do agente de tratamento quando da ocorrência do dano, em decorrência de omissão na segurança ao tratar os dados e de desrespeito aos comandos legais.[124] Por isso, asseveram que "[...] o Capítulo VI da LGPD (artigos 46 a 54) - que trata de *standards* de conduta a serem seguidos pelos agentes de tratamento de dados para a segurança, sigilo, boas práticas e governança de dados - seria também o fundamento para o reconhecimento da responsabilidade subjetiva."[125]

Além disso, tendo-se em conta as excludentes de responsabilidade enumeradas no artigo 43 da lei, verifica-se que o agente de tratamento de dados será eximido de culpa, ainda que exista dano, se ele não tiver

124 GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, Término do tratamento de dados. In: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. São Paulo. Editora RT, 2019. p. 231.

125 MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**, 30. jun. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>. Acesso em: 14. set. 2022.

violado a LGDP, mais um indicativo de adoção da teoria da culpa.[126] Destarte, estará isento do dever de indenizar quando evidenciado que "[...] observou o *standard* esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa."[127]

Outros[128] defendem que a LGPD se alinha à teoria ativa/proativa, para a qual a obrigação de indenizar deve ser exceção e o foco deve estar na verificação da adoção, pelos agentes de tratamento, das medidas necessárias e bastantes para prevenir os danos, o que pode se verificar no art. 6º da lei sob enfoque, o qual vincula a responsabilização dos agentes à "demonstração [...] da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."[129]

No extremo oposto, a partir da premissa de que a LGPD está essencialmente vocacionada à diminuição de riscos de dano, há os que[130] vislumbram um risco imanente ao tratamento de dados, "[...] na medida em que há uma potencialidade danosa considerável em caso de violação desses direitos, que se caracterizam por sua natureza de direito personalíssimo e de direito fundamental." Portanto, em virtude desse risco e

126 *Idem*.

127 GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, Término do tratamento de dados. *op. cit.* p. 236.

128 MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. In: **Cadernos Adenauer**, vol. 3, Ano XX, 2019.

129 MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas,** 30. jun. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>. Acesso em: 14. set. 2022.

130 MENDES, Laura Schertel; DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, p. 555, 2018.

de sua latente capacidade de ensejar danos, entendem que a LGDP amoldou-se ao viés objetivo da responsabilidade civil.[131]

Não obstante, ao se utilizar de termos como "medidas, salvaguardas e mecanismos de mitigação do risco" (art. 5º, XVII), a norma deixa claro que o agente deve estar ciente dos riscos imanentes à atividade por ele desenvolvida e atuar efetiva e eficazmente na prevenção de danos, os quais, se ocorrerem, ensejarão a obrigação de reparar.[132]

Os que se alinham aos fautores de que a LGPD fundamentou-se na responsabilidade civil objetiva, aduzem que:

> "[...] a atividade desenvolvida pelo agente de tratamento é evidentemente **uma atividade que impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental.** Ademais, **tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves**, ao atingirem direitos difusos, **o que, por si só, já justificaria a adoção da responsabilidade civil objetiva**, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo."[133] (grifo nosso)

Como se percebe, não há consenso a esse respeito. No entanto, não é escopo deste artigo adentrar nas minúcias de cada linha de pensamento, tampouco analisá-las para formar uma opinião.

131 MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? *op. cit.*

132 *Idem*.

133 MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**, 30. jun. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>. Acesso em: 14. set. 2022.

3.2. Culpabilidade, Ônus da Prova, Obrigações de Meio e de Resultado

Conquanto alguns reconheçam que a maior discussão acerca da responsabilização na LGPD se concentre na natureza jurídica prevalente (subjetiva ou objetiva), e não refutem a importância do debate, não o veem como essencial, reputando ser necessário, ao invés disso, perscrutar sobre os elementos normativos restritivos ou alargadores da culpabilidade para essa responsabilização, já que, para eles, embora a LGPD tenha adotado o regime subjetivo, ela o fez com substancial redução das barreiras à ocorrência do dever de indenizar.[134]

No decorrer de sua exposição, expõem discussões decorrentes do regime jurídico de responsabilização na LGPD (ao seu sentir, orientado pela análise da culpa), permeado por elementos normativos que desaguam na necessidae de um juízo de valor sobre a culpa do agente, perceptível não somente no rol de excludentes de responsabilidade, mas na própria essência principiológica da norma.[135]

Ao se debruçarem sobre as hipóteses que podem dar azo à responsabilização civil (violações à legislação de proteção de dados pessoais e à segurança dos dados), trazem a lume a percepção da tentativa de sistematização dos referenciais para aferir culpa, que vão desde critérios sobre medidas de segurança idôneas para o tratamento/proteção dos dados até o da própria expectativa de segurança.[136]

---

134 BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilística.com**, v. 9, n. 3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em: 14. set. 2022.

135 *Idem*.

136 "Note-se que são critérios distintos. Para ficar apenas em um exemplo: o titular pode esperar que o tratamento forneça segurança maior ou menor que aquela garantida pela adoção das medidas de segurança aptas a proteger os dados pessoais. Os critérios geram questionamentos diferentes. De um lado, o que são medidas de segurança aptas? São aquelas que potencialmente garantem a segu-

Outra nuance recai sobre a compatibilização entre artigos da LGPD no que concerne ao ônus da prova, tendo-se em conta a previsão de uma presunção geral automática de alguns elementos da responsabilidade civil dos agentes de tratamento[137] e a possibilidade de inversão do ônus da prova em favor da vítima[138]:

> "É possível concluir, assim, que o regime jurídico da responsabilidade civil estabelecido pela LGPD traz uma erosão bastante significativa dos filtros da responsabilidade civil em favor do titular dos dados. Ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil."[139]

Partindo para outro aspecto associado ao tema, tendo em conta as obrigações imputadas aos agentes de tratamento, trabalham com a dicotomia entre obrigações de meio e de resultado, tecendo considerações sobre o fato de a responsabilidade dos agentes de tratamento de dados serem de meio ou de resultado para, ao final do raciocínio, concluir por uma provável ambiguidade na norma, cujo texto, ora indica aparente

---

rança, ou apenas aquelas que seguramente o fazem? De outro lado, quando a lei fala em "segurança que o titular dele pode esperar", o critério é subjetivo ou objetivo? Trata-se do que a pessoa do titular de dados do caso concreto pode esperar, devendo-se então levar em conta o seu nível especial de conhecimento ou ignorância? Ou critério objetivo, falando de um titular padrão?" (BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilística.com**, v. 9, n. 3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em: 14. set. 2022.)

137 "A partir das excludentes de responsabilidade estabelecidas no artigo 43 da LGPD, e em face de dano decorrente de tratamento de dados, presume-se: (i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; e (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento." (BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *op. cit.)*

138 BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *op. cit.*

139 *Idem*.

obrigação de resultado (*v.g.* o princípio da responsabilidade e da prestação de contas e as prescrições dele decorrentes) ora de meio (como no conceito de *privacy by design*[140]).

3.3. LGPD e Responsabilidade Civil no Judiciário Brasileiro

Conquanto o aspecto de responsabilização positivado pela LGPD tenha entrado muito recentemente em vigor, já é possível identificar algumas provocações ao Judiciário brasileiro, que lida com os consectários da indefinição legislativa da norma de proteção de dados a respeito da natureza jurídica da responsabilização civil por ela adotada.

O TJDFT, em sede de recurso inominado[141], reformou decisão da esfera *a quo*, retirando a incidência de danos morais por entender que a LGPD não dá azo à condenação por esse tipo de dano *in re ipsa*. Segundo o *decisum*, "[...] Ao contrário, a inteligência do art. 42 indica a necessidade de demonstração, em concreto, do dano causado pelo tratamento inadequado de dados."

No relatório que deu azo à decisão proferida no bojo de uma apelação cível no TJSP[142], o Relator do voto tratou de assunto ctiado em tópico

---

140 BRASIl. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 16. set. 2022. "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

141 BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Recurso Inominado n. 0739758-90.2021.8.07.0016**. 1ª Turma Recursal. Rel: Juiz Aiston Henrique de Sousa. Julgado em 1. jul. 2022. "RECURSO INOMINADO. DIREITO CIVIL. RESPONSABILIDADE CIVIL. LEI GERAL DE PROTEÇÃO DE DADOS. LGDP. EXPOSIÇÃO DE DADOS PESSOAIS EM SITE DA INTERNET. DADOS PESSOAIS NÃO SENSÍVEIS. EXCLUSÃO DE INFORMAÇÕES. **DANOS MORAIS. NÃO CABIMENTO**." (grifo nosso)

142 ESTADO DE SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação cível n. 1000331-**

anterior deste artigo, aderindo à nova linha de pensamento chamada responsabilidade ativa/proativa. Segundo o que expôs:

> "[...] não se trata mais, como antigamente, de aplicação das regras da responsabilidade subjetiva ou objetiva, mas sim do que adoutrina vem definindo como responsabilidade ativa ou proativa, hipótese em que, às empresas não é suficiente o cumprimento dos artigos da lei, mas será necessária ademonstração da adoção de medidas eficazes e capazes de comprovar a observância eo cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas."[143]

No que se refere ao ônus probatório, a celeuma não foge ao que já ocorria antes da LGPD. Em aresto do Sodalício paranaense[144], ao julgar

---

24.2021.8.26.0003. 27ª Câmara de Direito Privado. Rel.: Alfredo Attié. Julgado em: 16. nov. 2021. "LEI GERAL DE PROTEÇÂO DE DADOS PESSOAIS (LGPD) E DIREITO DO CONSUMIDOR. AÇÃO COM PRECEITOS CONDENATÓRIOS. Sentença de improcedência dos pedidos. Recurso de apelação do autor. Vazamento de pessoais não sensíveis do autor (nome completo, números de RG e CPF, endereço, endereço de e-mail e telefone), sob responsabilidade da ré. **LGPD. Responsabilidade civil ativa ou proativa.** Doutrina. Código de Defesa do Consumidor. **Responsabilidade civil objetiva**. Ausência de provas, todavia, de violação à dignidade humana do autor e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autor que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, houve a ocorrência de danos morais. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa. Precedentes. Ampla divulgação da violação já realizada. Recolhimento dos dados. Inviabilidade, considerando-se a ausência de finalização das investigações. Pedidos julgados parcialmente procedentes, todavia, com o reconhecimento da ocorrência de vazamento dos dados pessoais não sensíveis do autor e condenando-se a ré na apresentação de informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados, fornecendo declaração completa que indique sua origem, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados, conforme o art. 19, II, da LGPD. Determinação para envio de cópia dos autos à Autoridade Nacional de Proteção de Danos (art. 55-A da LGPD). RECURSO PARCIALMENTE PROVIDO." (grifo nosso)

143 ESTADO DE SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação cível n. 1000331-24.2021.8.26.0003.** 27ª Câmara de Direito Privado. Rel.: Alfredo Attié. Julgado em: 16. nov. 2021.

144 ESTADO DO PARANÁ. Tribunal de Justiça do Estado do Paraná. **Recurso Inominado Cível n. 0001894-56.2021.8.16.0033**. 2ª Turma Recursal dos Juizados Especiais. Rel.: Irineu Stein Junior. Julgado em: 10. jun. 2022. "RECURSO INOMINADO. MATÉRIA RESIDUAL. TENTATIVA DE CAPTAÇÃO DE CLIENTELA. AUSÊNCIA DE PROVA DE QUE OS DADOS FORAM REPASSADOS PELO CREDOR. **VIOLAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS. NÃO COLHIMENTO.** TERCEIRO QUE OBTÉM OS DADOS PESSOAIS E CONTRATUAIS E DA EXISTÊNCIA DE PROCESSO JUDICIAL PÚBLICO. **NEXO DE CAUSALIDADE. NÃO VERIFICAÇÃO.** FATO EXCLUSIVO DE

um recurso inominado, a parte irresignada teve seu pleito de inversão de ônus da prova mitigado, porque, ao sentir do julgador, não comprovou minimamente fato constitutivo de seu direito; o TJSP[145], por seu turno, em grau de apelação, pugnou pela necessidade da distribuição dinâmica desse ônus, mesmo diante da não comprovação mínima, pela vítima, da divulgação indevida de seus dados.

Numa rápida pesquisa, foi possível identificar que as discussões, com algumas exceções, continuam gravitando em torno dos assuntos explorados nos itens anteriores, concentrando-se na combinação desses temas com a legislação consumerista, versando sobre responsabilidade dos fornecedores, pleito por danos morais por exposição de dados, discussões sobre culpa etc.

Outrossim, a despeito das eventuais divergências encontradas nas decisões, algo lhes foi comum: a imprescindibilidade da caracterização do liame causal entre a ação/omissão e o dano verificado, afastando a possibilidade de incidência do dano *in re ipsa*.

TERCEIRO. **RESPONSABILIDADE OBJETIVA AFASTADA**. SENTENÇA REFORMADA. RECURSO CONHECIDO E PROVIDO." (grifo nosso)

145 ESTADO DE SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação n. 1010253-75.2020.8.26.0019.** 37ª Câmara de Direito Privado. Rel.: José Wagner Oliveira Melatto Peixoto. Julgado em: 1. fev. 2022. "TELEFONIA - Ação indenizatória – Sentença de improcedência – Preliminar de violação ao princípio da dialeticidade recursal, rejeitada – Preliminar de cerceamento de defesa decorrente da não inversão do ônus da prova que se confunde com o mérito, e com ele será analisada – Alegação de quebra de sigilo de dados a despeito da contratação do serviço de "verificação em duas etapas" – Relação de consumo – **Inversão do ônus da prova cabível, na aplicação do CDC, art. 6º VIII e art. 42, § 2º da Lei nº 13.709/18 (LGPD)**– Alteração de e-mail nos dados cadastrais da autora, pelo qual foi atendido pedido de envio de 2ª via de fatura com dados pessoais – Concessionária que não fez prova da autoria da alteração do e-mail no cadastro da consumidora, e nem de quem solicitou e de quem enviou fatura de consumo para o endereço eletrônico recadastrado, de ônus seu por ser a fornecedora dos sistemas e depositária neles de todos os registros de acesso - Reconhecimento da concessionária, perante à ANATEL, de encaminhamento de segunda via de conta de consumo para o e-mail recadastrado – Fatura que apresenta dados pessoais da consumidora, dado a conhecer a terceiros – Quebra de sigilo de dados – Configuração – Danos morais – Ocorrência – Indenização devida – Valor arbitrado de R$ 10.000,00 em consonância com o evento danoso – Correção monetária deste arbitramento (STJ, Súmula 362), e juros de mora da citação (CC, art. 405)- Decaimento da ré (STJ, Súmula 326)- Ação parcialmente procedente – Sentença substituída – Recurso parcialmente provido." (grifo nosso)

CONCLUSÃO

Este artigo foi dedicado ao levantamento das principais temáticas advindas do regime de responsabilização civil positivado pela Lei Geral de Proteção de Dados, no intuito de verificar se tais questões podem ser consideradas novas para a dogmática jurídica ou se, na verdade, não passam de velhos temas que apenas foram trasladados para o âmbito da LGPD, sem contudo deterem especificidades que permitam lhes imputar um caráter de novidade e, adicionalmente, à tentativa de verificar, por meio da seleção de alguns julgados, como o Judiciário tem se posicionado a respeito de duas questões nevrálgicas: qual é a natureza da responsabilidade civil (subjetiva ou objetiva) no âmbito do regime estatuído pela LGPD e sobre a prescindibilidade ou não da caracterização do liame causal entre a ação/omissão e o dano.

O primeiro capítulo permitiu rememorar o caminho perfilhado pela responsabilidade civil no Brasil, sem todavia, dissecar os seus elementos, dada a magnitude de uma missão como essa.

A segunda etapa revelou a estrutura normativa da LGPD, trazendo à baila alguns conceitos importantes e específicos da norma, além de delinear o regime de responsabilização ali contido, o qual, conforme defendido por alguns, denota a omissão legislativa quanto à indicação clara da natureza jurídica da responsabilização ali prevista.

A última etapa, núcleo da pesquisa, ensejou a constatação de que, tanto na comunidade jurídica como na judiciária, a despeito de algumas discussões específicas quanto ao conteúdo da lei (notadamente quanto ao alcance de algumas terminologias), as discussões centrais gravitam em torno dos mesmos temas que desafiam a dogmática jurídica na interpretação da responsabilidade civil como um todo. Destarte, ainda que decorrentes do regime perfilhado pela LGDP (que, por sinal, enseja as principais discussões), os debates e os casos levados à tutela jurisdicio-

nal estatal, ao fim e ao cabo, mantêm-se em torno de velhas discussões, tais como o regime ser de responsabilidade ser objetivo ou subjetivo, as dificuldades para interpretar os elementos da culpabilidade, os desafios quanto à distribiução do ônus da prova, a caracterização das obrigações ali contidas como de meio e de resultado etc.

Especificamente quanto à natureza da responsabilidade, notou-se que a omissão legislativa quanto a esse aspecto afigura-se como a grande fonte de discordâncias no campo teórico, as quais, por sua vez, como se verificou nas decisões selecionadas (e também em outras encontradas, mas não citadas neste estudo, que procurou apenas trazer alguns exemplos da utilização de cada corrente), reverberam diretamente no seio do Judiciário, não possibilitando concluir, ainda, pela predominância de uma das linhas de pensamento nos julgamentos, circunstância que, com o passar com tempo e a repetitividade dos casos, talvez possa compor futuros pronunciamentos qualificados, a partir dos instrumentos oriundos do microssistema de formação dessas espécies de manifestações pelo Poder Judiciário, visando à solução do impasse hermenêutico advindo da omissão legislativa.

A única avaliação comumente encontrada em todas se assentou na necessidade de caracterização do nexo causal entre a ação/omissão e o dano, descartando a possibilidade do dano *in re ipsa*.

REFERÊNCIAS

1. Legislação em Geral

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

_____. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

_____. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

_____. Lei n. 12.414, de 9 de junho de 2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>.

_____. Lei n. 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>.

_____. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>.

_____. Lei n. 7.347, de 24 de julho de 1985. **Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm>.

_____. Lei n. 3.071, de 1º de janeiro de 1916. **Código Civil dos Estados Unidos do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l3071.htm>.

_____. Decreto n. 2.681, de 7 de dezembro de 1912. **Regula a responsabilidade civil das estradas de ferro**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d2681_1912.htm>.

2. Precedentes Judiciais

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Recurso Inominado n. 0739758-90.2021.8.07.0016**. 1ª Turma Recursal. Rel: Juiz Aiston Henrique de Sousa. Julgado em 1. jul. 2022.

ESTADO DE SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação n. 1010253-75.2020.8.26.0019**. 37ª Câmara de Direito Privado. Rel.: José Wagner Oliveira Melatto Peixoto. Julgado em: 1. fev. 2022.

_____. **Apelação cível n. 1000331-24.2021.8.26.0003**. 27ª Câmara de Direito Privado. Rel.: Alfredo Attié. Julgado em: 16. nov. 2021.

ESTADO DO PARANÁ. Tribunal de Justiça do Estado do Paraná. **Recurso Inominado Cível n. 0001894-56.2021.8.16.0033**. 2ª Turma Recursal dos Juizados Especiais. Rel.: Irineu Stein Junior. Julgado em: 10. jun. 2022.

3. Livros, Artigos Científicos, Trabalhos Acadêmicos e Publicações em Geral

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilística.com**, v. 9, n. 3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>.

BRASIL. **Guia de Boas Práticas**: Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>.

CAVALIERI FILHO, Sergio. In: TARTUCE, Flávio. **Direito Civil**: Direito das Obrigações e Responsabilidade Civil. Vol. 2. 17. ed. Rio de Janeiro: Forense, 2022.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, ano 21, n. 53, pp. 163-170, jan.-mar. 2020. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712>.

CARRÁ, Bruno Leonardo Câmara. Aspectos das modalidades subjetiva e objetiva no sistema atual de responsabilidade civil brasileiro. **Revista Esmafe**: Escola de Magistratura Federal da 5ª Região, Recife, n. 11, p. 187-209, dez. 2006. Disponível em: <https://revista.trf5.jus.br/index.php/esmafe/article/view/75/71>.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro** Vol. 4: Responsabilidade Civil. 16. ed. São Paulo: Saraiva Educação, 2021.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, Término do tratamento de dados. In: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. São Paulo. Editora RT, 2019.

MACHADO, Cláudio Germando Sampaio; CARRÁ, Bruno Leonardo Câmara. **A responsabilidade civil dos agentes de tratamento de dados na Lei nº 13.709/2018**: Os entendimentos doutrinários e legislativos acerca de interpretação da responsabilidade civil na Lei Geral de Proteção de Dados.

MENDES, Laura Schertel; DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, p. 555, 2018.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. In: **Cadernos Adenauer**, vol. 3, Ano XX, 2019.

MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**, 30. jun. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>.

TARTUCE, Flávio. **Direito Civil:** Direito das Obrigações e Responsabilidade Civil. Vol. 2. 17. ed. Rio de Janeiro: Forense, 2022.

JURISPRUDÊNCIA

REVISTA
JURÍDICA
DO BANCO DO NORDESTE

REFERENDO NA MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.388 DISTRITO FEDERAL

RELATORA: MIN. ROSA WEBER

REQTE.(S): PARTIDO DA SOCIAL DEMOCRACIA BRASILEIRA

ADV.(A/S): FLAVIO HENRIQUE COSTA PEREIRA E OUTRO (A/S)

INTDO.(A/S): PRESIDENTE DA REPÚBLICA

PROC.(A/S)(ES): ADVOGADO-GERAL DA UNIÃO

REVISTA JURÍDICA
DO BANCO DO NORDESTE

EMENTA

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.

1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de **ADI 6388 MC-REF / DF** serviço público há de assegurar mecanismos de proteção e segurança desses dados.

3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não exces-

sivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (Artigo 45, § 2º, alíneas "b" e "d").

4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.

5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.

6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada.

8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a

responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.

9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na

10. Constituição.

11. *Fumus boni juris* e *periculum in mora* demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.

12. Medida cautelar referendada.

RELATÓRIO

A Senhora Ministra Rosa Weber (Relatora): 1. Submeto ao referendo do Plenário, nos moldes do **art. 21, IV e V, do RISTF, medida cautelar** por mim concedida a fim de evitar dano de incerta reparação e assegurar a eficácia da ulterior decisão do mérito.

Cuida-se de pedido de **medida cautelar** em ação direta de inconstitucionalidade proposta pelo **Partido da Social Democracia Brasileira - PSDB em face do art. 2º, caput, da Medida Provisória nº 954,**

de 17 de abril de 2020, que dispõe sobre "*o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020*".

A agremiação autora afirma, preliminarmente, a sua legitimidade para o ajuizamento da presente ação, nos moldes do **art. 103, VIII, da Constituição da República**.

Defende a **inconstitucionalidade material** do dispositivo impugnado, no que determina o repasse, à Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, das informações correspondentes ao nome, endereço e número de telefone de todos os cidadãos brasileiros usuários dos serviços de telefonia fixa e móvel, por afronta às cláusulas fundamentais assecuratórias da **inviolabilidade da intimidade**, da **vida privada**, da **honra** e da **imagem** das pessoas, bem como do **sigilo de dados** (**art. 5º, X e XII, da Constituição da República**).

Argumenta, nesse sentido, que "*os dados constantes dos cadastros das empresas de telefonia são elementos da vida privada e da intimidade da pessoa, não sendo lícito seu manejo da forma como normatizada pelo art. 2º, caput da Medida Provisória 954, de 2020*" e sustenta que "*o perigo latente da medida legislativa é de tamanha envergadura que (...) aproxima o ato de uma medida de exceção, típica dos Estados ditatoriais, ao despir o brasileiro de seus direitos fundamentais essenciais ao convívio em sociedade e à garantia de não sobreposição do Estado à sua condição humana*".

2. Requer a concessão de medida acauteladora *inaudita altera pars* e *ad referendum* do Plenário, para suspender imediatamente a

eficácia do **art. 2º, *caput*, da MP nº 954/2020** até o julgamento final da presente ação, e, por consequência, "*seja vedado o compartilhamento dos dados consistentes no nome, telefone e endereço de todos os cidadãos brasileiros pelas empresas de telecomunicações prestadoras de serviços telefônicos fixo comutado ou do serviço móvel pessoal*".

Afirma configurado o **perigo na demora** da prestação jurisdicional face à iminente concretização da apontada lesão a direitos fundamentais, tendo em vista o exíguo prazo de **sete dias** contados da publicação do ato disciplinador do procedimento de disponibilização, previsto no **art. 2º, § 3º, da MP nº 954/2020,** para que as empresas efetivem o compartilhamento.

3. No mérito, pugna pela procedência do pedido de declaração de **inconstitucionalidade material** do **art. 2º, *caput*, da Medida Provisória nº 954/2020** "*e, por consequência, seja declarado proibido ou nulo o ato de compartilhamento de dados consolidados de telefone, nome e endereço de todos os cidadãos brasileiros para a Fundação IBGE pelas empresas de telecomunicações prestadoras de serviços telefônicos fixo comutado ou do serviço móvel pessoal*".

4. O feito foi a mim distribuído em **20.4.2020**, na forma do **art. 77-B do RISTF,** por prevenção em relação à **ação direta de inconstitucionalidade nº 6387.**

5. Em **24.4.2020,** a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, o pedido de **medida cautelar** foi por mim **deferido**, *ad referendum* do Plenário desta Suprema Corte, para **suspender a eficácia da Medida Provisória nº 954/2020**, determinando - se, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstivesse de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tivesse feito, que sustas-

se tal pedido, com imediata comunicação à(s) operadora(s) de telefonia.

Na ocasião, determinei que a tramitação conjunta do presente feito com as **ações diretas de inconstitucionalidade nºs 6387, 6389, 6390 e 6393**, que igualmente impugnam a validade constitucional da **Medida Provisória nº 954/2020**.

É o relatório.

VOTO

A Senhora Ministra Rosa Weber (Relatora): 1. Senhor Presidente, renovo minhas saudações a todos, cumprimento e agradeço aos que fizeram uso da palavra em sustentações orais que pluralizam e enriquecem o debate, permitindo maior e melhor reflexão sobre tema tão delicado. Obrigada, Dr. José Levi, gaúcho como eu, pelas palavras gentis.

Submeto ao referendo deste E. Plenário a decisão que proferi, em sede cautelar, **suspendendo a eficácia da Medida Provisória nº 954/2020**, com o consequente comando ao **Instituto Brasileiro de Geografia e Estatística – IBGE** para se abster de requerer a disponibilização, pelas operadoras de telefonia, em meio eletrônico, dos dados de que trata e que dizem com os **nomes, números de telefone e endereços de todos os seus usuários, pessoas físicas e jurídicas.**

Como relatei, foram a mim distribuídas cinco ações diretas de inconstitucionalidade que impugnam a higidez constitucional da **Medida Provisória nº 954**, a primeira ajuizada pelo **Conselho Federal da Ordem dos Advogados do Brasil,** e as subsequentes, por quatro partidos políticos: **PSDB, PSB, PSOL** e **PCdoB.**

A ADI da OAB, como disse, é a mais ampla, abarcando o objeto das demais, e nela se afirmam presentes, na MP, os vícios da **inconstitucionalidade formal e –** pelo não atendimento dos requisitos da relevância

e urgência, impostos pelo art. 62 da CF, para a edição de medida provisória -, e da **inconstitucionalidade material,** ao argumento principal de violação das regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa, albergados nos **arts. 1º, inciso III, e 5º, incisos X e XII da nossa Lei Fundamental.**

Colho da fundamentação que exarei os aspectos decisivos, na minha visão, para a concessão da liminar – considerada a urgência da medida, sob pena do comprometimento do resultado útil do processo – quanto a este tema sensível e polêmico relativo aos dados pessoais, que perpassa conhecidas obras da literatura universal – como o clássico 1984, de George Orwell, publicado ainda em 1949 – e do cinema, e aqui lembro o documentário Privacidade Hackeada.

"**Vistos etc.**

1. Cuida-se de pedido de **medida cautelar** em ação direta de inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, que dispõe sobre "*o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020*".

2. Para a adequada compreensão da controvérsia constitucional, transcrevo o inteiro teor do ato normativo questionado:

'Art. 1º Esta Medida Provisória dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE.

Parágrafo único. O disposto nesta Medida Provisória se aplica durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão **disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.**

§ 1º Os dados de que trata o *caput* serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

§ 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o *caput*.

§ 3º Os dados deverão ser disponibilizados no prazo de:

I - sete dias, contado da data de publicação do ato de que trata o § 2º; e

II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes.

Art. 3º Os dados compartilhados:

I - terão caráter sigiloso;

II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e

III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968.

§ 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o *caput* do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos.

§ 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no *caput* do art. 2º foram utilizados e divulgará **relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.**

Art. 4º Superada a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), nos termos do disposto na Lei nº 13.979, de 2020, as informações compartilhadas na forma prevista no *caput* do art. 2º ou no art. 3º serão eliminadas das bases de dados da Fundação IBGE.

Parágrafo único. Na hipótese de necessidade de conclusão de produção estatística oficial, a Fundação IBGE poderá utilizar os dados pelo prazo de trinta dias, contado do fim da situação de emergência de saúde pública de importância internacional.

Art. 5º Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 17 de abril de 2020; 199º da Independência e 132º da República.'

3. A parte autora afirma presentes os vícios da inconstitucionalidade formal, por inobservância dos requisitos constitucionais para edição de medida provisória, e da inconstitucionalidade material, ao argumento principal de violação das regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa (**arts. 1º, III e 5º, X e XII, da Constituição da República**).

4. Conforme assinala, a inconstitucionalidade formal diz com a inobservância do **art. 62, *caput*, da Constituição Federal**, na medida em que não demonstrados os requisitos da urgência e da relevância material a autorizar a edição de medida provisória. À alegação da inconstitucionalidade formal, defende a possibilidade de sindicância jurisdicional, a despeito da jurisprudência construída, no período do regime militar, no sentido de sua inviabilidade quanto a atos de natureza política. Nesse sentido, reporta-se à **ADI-MC 162,** à **ADI 2213** e à **ADI 4029**, em que reformulado o fundamento da legitimidade de controle constitucional dos pressupostos do exercício do poder extraordinário de legislar outorgado ao Presidente da República como instrumento de tutela do preceito fundamental da separação de poderes.

   Segundo argui, a MP n. 954/2020 não evidencia a importância superlativa da pesquisa estatística que embasa a solicitação de compartilhamento dos dados, tampouco explicita a forma como esta pesquisa contribuirá na formulação das políticas públicas de enfrentamento da crise sanitária, uma vez não informados os tipos de pesquisas a serem realizadas. Noutro espectro, destaca

não esclarecido o motivo para o compartilhamento de dados, já informado pelo IBGE o adiamento do Censo Demográfico para o ano de 2021.

5. Busca seja assentada a inconstitucionalidade material da MP n. 954/2020. Para tanto, assevera a necessidade de tutela do direito fundamental à proteção de dados pessoais, a teor do **art. 5º, XII, da CF**, que assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ressalvada a relativização, nessa última hipótese, mediante ordem judicial e para fins de persecução penal.

   Argumenta com o direito fundamental à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (**art. 5º, X, CF**), como fundamento do indivíduo para determinar e controlar, frente ao Estado, a utilização dos seus dados. Seguindo essa linha discursiva, aponta para a existência, no desenho constitucional brasileiro, de um direito fundamental à proteção de dados, na concepção de um direito à autodeterminação informativa, em que fundamenta, inclusive, a edição da Lei Geral de Proteção de Dados (Lei n. 13.709/2018).

   Ainda nessa perspectiva e para ilustrar, invoca a decisão do Tribunal Constitucional Federal Alemão que reconheceu, em 1983, forte no direito geral da personalidade, o direito fundamental à autodeterminação sobre dados pessoais, diante de intervenções estatais.

   Conforme argumenta "*a autodeterminação individual pressupõe – mesmo sob as condições da moderna tecnologia de processamento de informação – que, ao indivíduo está garantida a liberdade de decisão sobre as ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão*". Alega necessá-

ria, no ponto, a explicitação do postulado da proporcionalidade para as hipóteses de relativização do afirmado direito fundamental à autodeterminação informativa.

Ou seja, articula que a atividade legislativa será constitucional se observar a proporcionalidade nos critérios a embasar a intervenção estatal na coleta, no compartilhamento e no uso dos dados pessoais, conduta não adotada no ato normativo contestado. Isso porque a MP n. 954/2020 não explicita a finalidade do uso da pesquisa estatística, não demonstra a forma pela qual adequados e necessários os dados nem delimita o campo de proteção na operação de processamento de dados. Importa registrar a indicação do precedente formado no RE 1055941, sobre o compartilhamento de dado pelo COAF/UIF ao Ministério Público.

Em suas palavras: "*A Medida Provisória em análise viola o sigilo de dados dos brasileiros e invade a privacidade e a intimidade de todos, sem a devida proteção quanto à segurança de manuseio, sem justificativa adequada, sem finalidade suficientemente especificada e sem garantir a manutenção do sigilo por uma Autoridade com credibilidade, representatividade e legitimidade, a exemplo daquela prevista pela Lei Geral de Proteção de Dados, Lei Federal 13.709*."

6. Frente ao cenário argumentativo descrito, requer a concessão de medida cautelar, *ad referendum* do Plenário, na forma do art. 10, § 3º, da Lei nº 9.868/1999, para suspender imediatamente a eficácia do inteiro teor da MP n. 954/2020 até o julgamento final da presente ação, bem como para reconhecer o "*direito fundamental à autodeterminação informativa, a ensejar tutela jurisdicional quando sua violação não for devidamente justificada por motivo suficiente, proporcional, necessário e adequado e com proteção efetiva do sigilo perante tercei-*

ros, com governança que inclua o Judiciário, o Ministério Público, a Advocacia e entidades da sociedade civil".

7. Justifica presente o requisito da plausibilidade do direito, à evidência da não configuração dos requisitos constitucionais autorizadores da edição de medidas provisórias (**art. 62, *caput*, CF**), e da necessidade de tutela dos direitos fundamentais à privacidade, à intimidade, à proteção de dados pessoais, à dignidade da pessoa humana e à autodeterminação informativa. Igualmente, destaca configurado o perigo da demora na prestação jurisdicional face à urgência reconhecida no exíguo prazo de três dias estipulado no **art. 2º, §2º, da MP n. 954/2020** para a disciplina do procedimento de disponibilização de dados, a partir da oitiva da Agência Nacional de Telecomunicações. Após a regulamentação, abre-se o prazo de sete dias para as empresas oferecerem os dados solicitados. Afirma, portanto, "*no mais tardar, dia 27 próximo todos os dados dos brasileiros já deverão estar disponibilizados, nos termos da MP*".

8. No mérito, pede a procedência do pedido de declaração de inconstitucionalidade da **Medida Provisória n. 954/2020**, em sua integralidade, bem como o reconhecimento do direito fundamental à autodeterminação informativa.

9. Considerada a relevância da matéria constitucional objeto da ação, bem como a urgência caracterizada da tutela jurisdicional, solicitei informações prévias à Fundação Instituto Brasileiro de Geografia e Estatística - IBGE e à Agência Nacional de Telecomunicações - ANATEL, bem como abri vista para manifestação do Procurador-Geral da República e do Advogado-Geral da União, no prazo comum de 48 (quarenta e oito) horas.

10. Em 23.4.2020, o autor peticionou informando que no curso do prazo de 48 (quarenta e oito) horas concedido para a juntada das informações, foi publicada, em 22.4.2020, a "*Instrução Normativa IBGE 2/2020, que regula de maneira genérica e precária o procedimento de compartilhamento direto de dados, sob responsabilidade de sua Diretoria de Informática*" **(doc. n. 24867/2020)**.

    Nas suas palavras, conforme o ofício anexo, "*devidamente desidentificado pela remetente para não apresentar informações sensíveis, o IBGE já começou a oficiar as operadoras de telefonia móvel e fixa para que enviem os dados pessoais sob sua guarda à fundação pública.*"

11. À alegação de que algumas operadoras de telefonia já receberam o ofício encaminhado pelo IBGE, com fundamento na Instrução Normativa 2/2020, para a transferência imediata dos dados, a despeito do prazo de sete dias fixados pela Medida Provisória n. 954/2020, e o prazo de 48 horas fixado por este Supremo Tribunal Federal, **reitera o pedido de urgência a justificar a medida liminar requerida.**

12. Em 24.4.2020, o Advogado-Geral da União manifestou-se pelo indeferimento da medida cautelar, em arrazoado assim ementado:

    'Medida Provisória nº 954/2020. Compartilhamento de dados por empresas de telecomunicações com a Fundação IBGE. Legitimidade formal. A relevância e a urgência da medida encontram fundamento na necessidade de permitir, em contexto de distanciamento social, a continuidade e o enriquecimento do diagnóstico estatístico oferecido pelo IBGE. Conhecimento relevante para a formulação cientificamente adequada de políticas públicas de combate às consequências do Covid-19. Legitimidade material. Ausência de *fumus boni iuris*. Ausência de violação à privacida-

de e à intimidade (artigo 5º, incisos X e XII, da Constituição da República). Essa Suprema Corte já decidiu que a 'transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo' não ofende o direito à intimidade e à privacidade. ADI nº 2859. O acesso aos dados pessoais na forma da MP nº 954/2020 contempla finalidade (pesquisa estatística) e condicionantes consentâneos com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Obrigação de conservação do sigilo e posterior eliminação dos dados coletados. Indispensabilidade do prosseguimento do levantamento estatístico da PNAD. Subsídios necessários, entre outros fins, para servir de base ao cálculo do Fundo de Participação dos Estados. Proporcionalidade da MP nº 954/2020. Ausência de p*ericulum in mora*. Presença de perigo de demora inverso, em face da urgência na formulação de políticas públicas eficazes no combate à pandemia. Manifestação pelo indeferimento do pedido cautelar.'

Na mesma data, foram apresentadas informações pelo **Instituto Brasileiro de Geografia e Estatística – IBGE** e pela **Agência Nacional de Telecomunicações - ANATEL.**

13. Relatado o essencial, decido.

14. Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.

    A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (**art. 5º, X**). O assim chamado

direito à privacidade (*right to privacy*) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.

A fim de instrumentalizar tais direitos, a Constituição prevê, no **art. 5º, XII,** a **inviolabilidade do "*sigilo* *da correspondência e das comunicações telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal*".

15. O **art. 2º da MP n. 954/2020** impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de **nomes, números de telefone e endereços** de seus consumidores, pessoas físicas ou jurídicas.

    Tais informações, relacionadas à **identificação – efetiva ou potencial – de pessoa natural**, configuram **dados pessoais** e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (**art. 5º, *caput***), da privacidade e do livre desenvolvimento da personalidade (**art. 5º, X e XII**). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

    Decorrências dos direitos da personalidade, o respeito à **privacidade e à autodeterminação informativa** foram positivados, no **art. 2º, I e II, da Lei nº 13.709/2018** (Lei Geral de Proteção de Dados Pessoais), como **fundamentos** específicos da disciplina da **proteção de dados pessoais.**

No clássico artigo *The Right to Privacy*, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Em seus dizeres, "*a invasão injustificada da privacidade individual deve ser repreendida e, tanto quanto possível, prevenida*".

16. **Cumpre, pois, equacionar se a MP n. 954/2020 exorbitou dos limites traçados pela Constituição ao dispor sobre a disponibilização dos dados pessoais de todos os consumidores dos serviços STFC e SMP, pelos respectivos operadores, a entidade integrante da Administração indireta.**

17. Observo que o único dispositivo da **MP n. 954/2020** a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o **§ 1º do seu art. 2º**. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados.

    Já o **art. 1º, parágrafo único, da MP n. 954/2020** apenas dispõe que o ato normativo terá aplicação durante a situação de

emergência de saúde pública de importância internacional decorrente da COVID-19. Ainda que se possa associar, por inferência, que a estatística a ser produzida tenha relação com a pandemia invocada como justificativa da edição da MP, tal ilação não se extrai de seu texto.

Nessa ordem de ideias, não emerge da Medida Provisória n. 954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, consideradas a necessidade, a adequação e a proporcionalidade da medida. E tal dever competia ao Poder Executivo ao editá-la.

Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua **adequação e necessidade**, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (**art. 5º, LIV, da Lei Maior**), em sua dimensão substantiva.

18. De outra parte, o **art. 3º, I e II, da MP n. 954/2020** dispõe que os dados compartilhados "*terão caráter sigiloso*" e "*serão utilizados exclusivamente para a finalidade prevista no § 1º do art. 2º*", e o **art. 3º, § 1º**, veda ao IBGE compartilhar os dados disponibilizados com outros entes, públicos ou privados. Nada obstante, **a MP n. 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida**, seja na sua transmissão, seja no seu tratamento. Limita-se a delegar a ato do Presidente da Fundação IBGE o procedimento para compartilhamento dos dados, sem

oferecer proteção suficiente aos relevantes direitos fundamentais em jogo. Enfatizo: ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando o caso, o anonimato dos dados compartilhados, a MP n. 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros.

Essas considerações são corroboradas pela manifestação trazida aos autos pela Agência Nacional de Telecomunicações – ANATEL, que destacou necessária "*a observância de extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações*". E recomendou a adoção de medidas visando a adequar a medida à garantia dos princípios estabelecidos na Constituição Federal, na Lei Geral das Telecomunicações e na Lei Geral de Proteção de Dados, de modo a assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações, mediante:

> *'a) a sólida instrumentalização da relação jurídica que será estabelecida entre o IBGE e cada uma das prestadoras de serviços de telecomunicações demandadas; b) a delimitação específica da finalidade do uso dos dados solicitados; c) a limitação das solicitações ao universo de dados estritamente necessários para o atingimento da finalidade; d) a delimitação do período de uso e da forma de descarte dos dados; e e) a aplicação de boas práticas de segurança, de transparência e de controle.'*

19. Não bastasse, a ausência de garantias de tratamento adequado e seguro dos dados compartilhados parece-me agravada pela circunstância de que, embora aprovada, ainda não está em vigor a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018),

definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais.

20. Verifico, ainda, que na mesma data da publicação da MP n. 954/2020 foi editada a Instrução Normativa n. 2, de 17 de abril de 2020, que *estabelece procedimentos para disponibilização de dados de empresas de telecomunicações prestadoras de serviço telefônico fixo ou móvel ao Instituto Brasileiro Geográfico e Estatística -IBGE, para fins de suporte à produção de estatística oficial, durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus.*

    A referida Instrução Normativa teria embasado o envio, em 22.4.2020, segundo noticiado nos autos, de ofícios da Fundação IBGE às empresas de telefonia fixa comutada ou móvel pessoal, solicitando, com urgência, o compartilhamento imediato de dados, não obstante o prazo de sete fixados pela Medida Provisória 954/2020 e a determinação deste Supremo Tribunal Federal para a prestação de informações acerca do conteúdo deste ato normativo **(doc. 24 do processo eletrônico)**.

21. Saliento, também, que a análise da tramitação do projeto de lei de conversão da Medida Provisória 954/2020 revela terem sido apresentadas, até o momento, 344 propostas de emenda. Em significativo número, propugnada a restrição da norma aos dados estritamente necessários, bem como a necessidade de elaboração de relatório de impacto de segurança da informação anterior à coleta e uso dos dados (e não posterior, como veiculado), além da maior transparência na definição da finalidade e do uso dos dados compartilhados.

22. Presente, à luz do exposto, o ***fumus boni juris***, tenho por satisfeito igualmente o ***periculum in mora***, uma vez que a determinação do imediato compartilhamento de dados leva à eficácia plena do ato normativo questionado.

    Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição.

23. Reforço, em cumprimento ao dever de justificação decisória, no âmbito de medida liminar, que 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.

24. Nesse contexto, e a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, **defiro** a medida cautelar requerida, *ad referendum* do Plenário desta Suprema Corte, para **suspender a eficácia da Medida Provisória n. 954/2020**, determinando, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia.

25. Por fim, considerando que as ações diretas de inconstitucionalidade nºs 6388, 6389, 6390 e 6393, a mim distribuídas por

prevenção (art. 77-B, RISTF), igualmente impugnam a validade constitucional da Medida Provisória n. 954/2020, determino a tramitação conjunta dos feitos, com a reprodução desta decisão nos autos respectivos."

2. Acresço, neste momento, Senhor Presidente, algumas ponderações ao quanto exarado na decisão concessiva da liminar. Anoto que na segunda-feira passada, **04.5.2020**, o **IBGE** noticiou no seu sítio eletrônico (**www.ibge.gov.br**) ter dado início, em parceria com o Ministério da Saúde, à **PNAD Covid**, versão da **Pesquisa Nacional por Amostra de Domicílios Contínua** voltada à quantificação do alastramento da pandemia da Covid-19 e seus impactos no mercado de trabalho brasileiro.

Segundo a notícia veiculada no **Portal do IBGE**, "*cerca de dois mil agentes do IBGE já começaram a telefonar para 193,6 mil domicílios distribuídos em 3.364 municípios de todos os estados do país. Para definir a amostra da nova pesquisa, o IBGE utilizou a base de 211 mil domicílios que participaram da PNAD Contínua no primeiro trimestre de 2019 e selecionou aqueles com número de telefone cadastrado*".

Tal fato seria suficiente por si só para evidenciar a **desnecessidade** e o **excesso** do compartilhamento de dados tal como disciplinado na **MP nº 954/2020** para a **finalidade invocada** pelo IBGE como sua justificativa, qual seja a realização da PNAD. O objetivo alegado não só pode, como está sendo realizado de forma menos intrusiva à privacidade. Assim, **se a PNAD é realizada com uma amostra de pouco mais de duzentos mil domicílios, questiono: por que compartilhar duas centenas de milhões de números de telefone, com os riscos intrínsecos à manipulação desses dados?** Somado tal fato ao adiamento do **Censo 2020** para o próximo ano, parece-me que sua eloquência reverbera.

3. O **art. 1º, parágrafo único, da MP nº 954/2020** afirma circunscrita a aplicação à "*situação de emergência de saúde pública de*

importância internacional decorrente do coronavírus (covid19)". Essa premissa normativa atrai a incidência do **Regulamento Sanitário Internacional (RSI 2005)**, acordado na 58ª Assembleia Geral da **Organização Mundial de Saúde**, em 23 de maio de **2005**, incorporado ao direito pátrio por meio do **Decreto Legislativo nº 395/2009** e finalmente promulgado pelo **Decreto nº 10.212, de 30 de janeiro de 2020.**

Nele são fixadas balizas a serem observadas pelos Estados parte no tocante ao tratamento de dados pessoais nas hipóteses em que isso seja **essencial para os fins de avaliação e manejo de um risco para a saúde pública**, devendo se **garantir** que os dados pessoais sejam, a teor do seu **artigo 45, § 2º**:

> "(a) processados de modo justo e legal, e sem outros processamentos desnecessários e incompatíveis com tal propósito;
>
> (b) adequados, relevantes e **não excessivos em relação a esse propósito;**
>
> (c) acurados e, quando necessário, mantidos atualizados; todas as medidas razoáveis deverão ser tomadas a fim de garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e
>
> (d) **conservados apenas pelo tempo necessário**."

Nesse contexto, não bastasse a **coleta de dados** se revelar **excessiva**, repito, ao permitir que, pelo prazo de trinta dias **após a decretação do fim da situação de emergência de saúde pública**, os dados coletados ainda sejam utilizados para a produção estatística oficial, o **art. 4º, parágrafo único, da MP nº 954/2020** permite a conservação dos dados pessoais, pelo ente público, por tempo **manifestamente excedente ao estritamente necessário** para o atendimento da sua finalidade declarada, que é a de dar suporte à produção estatística oficial "***durante*** *a situação de emergência de saúde pública de importância interna-*

cional decorrente do coronavírus (covid19)" (destaquei).

Destaco, ainda, que a **desproporcionalidade** no tocante ao universo dos dados a serem disponibilizados com base na **MP nº 954/2020**, em cotejo com as finalidades declaradas para o seu uso, se agrava pela ausência de previsão, no ato normativo, de cuidados mínimos para a sua **anonimização** ou **pseudonimização**, procedimentos técnicos pelos quais os dados perdem a capacidade de identificar, direta ou indiretamente, o indivíduo a que originalmente se refere[146], sendo certo que em momento algum a **identificação** dos indivíduos titulares dos dados foi reivindicada como necessária ao relevante trabalho desenvolvido pelo IBGE.

4. Certamente há quem ainda se lembre de que há poucas décadas, antes da ubiquidade da telefonia móvel, era comum a edição de listas telefônicas impressas contendo nomes, telefones e endereços dos assinantes residenciais e comerciais dos serviços de telefonia em uma dada localidade. Além de ser facultado aos usuários dos serviços de telefonia optarem pela exclusão dos próprios dados dessas listas, é crucial ter presente que o que podia ser feitos a partir da publicização de tais dados pessoais não se compara ao que pode ser feito no patamar tecnológico atual, em que poderosas tecnologias de processamento, cruzamento e filtragem de dados permitem a formação de perfis individuais extremamente detalhados.

5. Outro ponto para o qual chamo a atenção é que, apesar de prevista a exclusividade do uso dos dados coletados pelo IBGE, **a Medida Provisória 954 não (contempla) garantia alguma que assegure o seu tratamento de forma segura.** Não há a previsão de auditoria externa e tampouco de responsabilização por eventual acesso indevido ou mau uso dos dados coletados.

146 Os conceitos jurídicos de anonimização e pseudonimização de dados foram incorporados ao ordenamento brasileiro pelos arts. 5º, XI, e 12, § 4º, da Lei nº 13.709/2018.

6. Quero enfatizar, por fim, que não questiono, em momento algum, a relevância, a seriedade e a legitimidade do trabalho desempenhado pelo IBGE, desde a sua fundação na década de 1930, ao produzir dados e informações estatísticas com reconhecida qualidade técnica. Não estou a afirmar que de modo algum os dados objeto da **Medida Provisória nº 954/2020** possam ser compartilhados com o IBGE. O que explicito, neste juízo perfunctório, é que **não se pode fazê-lo de uma forma que não garanta mecanismos de proteção compatíveis com as cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)**.

Assim como o exigir que automóveis sejam providos de freios, *airbags* e espelhos retrovisores não significa criar obstáculos para a indústria automobilística, o exigir que normas que envolvam direitos fundamentais e da personalidade observem requisitos mínimos de adequação constitucional tampouco pode ser lido como embaraço à atividade estatal.

Observo, por outro viés, que o adiamento para **03.5.2021**, operado pela **Medida Provisória nº 959, de 29 de abril de 2020,** do início da vigência da **Lei Geral de Proteção de Dados Pessoais** (a **Lei nº 13.709,** sancionada em **14 de agosto de 2018** com previsão para entrar em vigor em **16.08.2020), também deve ser anotado com um dado da realidade que, fragilizando o ambiente de proteção de dados pessoais no Brasil, obriga sejam medidas como a implementada na MP nº 954/2020 escrutinadas com maior cuidado, sob pena de se permitir que milhões de indivíduos sejam lesionados em suas esferas de direitos.**

Nos países citados pelo eminente **Procurador-Geral da República,** diversamente do que ocorre no Brasil, já há um marco legal vigente de proteção de dados, o que aqui, ao contrário, ainda não ocorre, pois adia-

da, por medida provisória, a vigência da lei aprovada pelo Congresso. Anoto igualmente que a adesão a serviços, por exemplo, de mensagens telefônicas em caso de desastres, incêndios etc. depende da aquiescência do indivíduo.

7. Situações de crise, como a deflagrada pela pandemia global da COVID-19 e marcada pelas medidas excepcionais que têm sido adotadas para o seu enfrentamento, tendem a favorecer o enfraquecimento de direitos, especialmente porque as instituições que em outro momento estariam menos permeáveis a tais investidas tornam-se, em momentos tais, menos vigilantes ou aderem às narrativas que visam a justificá-las a partir da crise posta. Tais movimentos têm sido objeto da literatura jurídica internacional, em que identificada, na pandemia de COVID-19 em curso "*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*"[147].

Em recente publicação, - volume *Law in the Time of COVID-19* (em tradução livre: O Direito no tempo da COVID-19), professores da Faculdade de Direito de Columbia reuniram análises acadêmicas acerca dos efeitos da pandemia em curso sobre diversas áreas do Direito, desde os direitos humanos ao direito falimentar, passando pelo direito eleitoral, pela execução penal, imigração, direitos LGBT direito ambiental, entre outros. Em inspirado artigo dedicado a abordar os desafios apresentados pela pandemia para a **privacidade**, a Professora **Clarissa Long** adverte:

> "a história nos ensina que uma vez estabelecidos, é improvável que poderes governamentais de vigilância e coleta de dados de seus cidadãos e residentes 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.

147 LONG, Clarissa; *Privacy and Pandemics* In PISTOR, Katharina. **Law in the time of COVID-19**. Columbia Law School Books, 2020.

(...)

> Sempre haverá a próxima pandemia em algum momento no futuro, senão 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."[148]

8. Reafirmando, assim, os fundamentos justificadores da concessão da medida cautelar, submeto-os à consideração dos eminentes pares.

É o voto.

ACÓRDÃO

Vistos, relatados e discutidos estes autos, acordam os Ministros do Supremo Tribunal Federal, em, por maioria, referendar a medida cautelar deferida para suspender a eficácia da Medida Provisória nº 954/2020, nos termos dos votos proferidos, vencido o Ministro Marco Aurélio, em sessão Plenária (realizada inteiramente por videoconferência - Resolução 672/2020/STF), presidida pelo Ministro Dias Toffoli, na conformidade da ata do julgamento.

Brasília, 7 de maio de 2020.

Ministra Rosa Weber

Relatora

O Acórdão, na íntegra, pode ser acessado em

https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357772

148 Idem.

AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.649 DISTRITO FEDERAL

RELATOR: MIN. GILMAR MENDES

REQTE.(S): CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL – CFOAB

ADV.(A/S): FELIPE DE SANTA CRUZ OLIVEIRA SCALETSKY E OUTRO(A/S)

INTDO.(A/S): PRESIDENTE DA REPÚBLICA

PROC.(A/S)(ES): ADVOGADO-GERAL DA UNIÃO

AM. CURIAE.: ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA

ADV.(A/S): BRUNO RICARDO BIONI

ADV.(A/S): MARIANA MARQUES RIELLI

ADV.(A/S): RAFAEL AUGUSTO FERREIRA ZANATTA

ADV.(A/S): IZABEL SAENGER NUNEZ

AM. CURIAE.: LABORATÓRIO DE POLÍTICAS PÚBLICAS INTERNET LAPIN

ADV.(A/S): JOSÉ RENATO LARANJEIRA DE PEREIRA

ADV.(A/S): PAULO HENRIQUE ATTA SARMENTO

AM. CURIAE.: INSTITUTO MAIS CIDADANIA

ADV.(A/S): LUIZ GUSTAVO DE ANDRADE

ADV.(A/S): ROOSEVELT ARRAES

VOTO

(Conjunto ADI 6649 e ADPF 695)

O SENHOR MINISTRO GILMAR MENDES (RELATOR): Trata-se de Ação Direta de Inconstitucionalidade e de Arguição de Descumprimento de Preceito Fundamental que, sob diferentes perspectivas, endereçam a controvérsia relativa aos limites, ao âmbito de proteção e à dimensão axiológica dos direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade, especificamente no que diz respeito ao tratamento de dados pessoais pelo Estado brasileiro.

Inicialmente, saúdo as sustentações orais que antecederam o debate da causa, todas fundadas em substanciosos argumentos de índole constitucional e em um profundo diálogo com os precedentes desta Corte. Registro que a verticalidade das manifestações e as diferentes concepções que existem sobre a matéria apenas comprovam a indiscutível necessidade de submeter a controvérsia ao escrutínio do Tribunal Pleno.

Não há dúvidas quanto ao assento constitucional da matéria ventilada nas ações de controle concentrado. É o que se conclui por meio de rápida incursão na jurisprudência do Supremo Tribunal Federal, que, ao ser provocado, não se eximiu de enfrentar, em mais de uma ocasião, a constitucionalidade de atos de coleta, armazenamento, transferência e divulgação de dados pessoais por agentes públicos.

Faço referência, pela relevância do precedente, ao memorável julgamento da Ação Direta de Inconstitucionalidade 6.387, de relatoria da EMINENTE MINISTRA ROSA WEBER, em que o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais na ordem jurídico-constitucional brasileira. A decisão é importante por diversos aspectos.

Primeiro, por contribuir para a construção de uma dogmática consti-

tucionalmente adequada para o que se tem chamado de era digital, berço de uma sociedade fundada no desenvolvimento tecnológico e no intercâmbio de informações digitais. Segundo, pela enunciação dos vetores interpretativos e do substrato axiológico que devem orientar a compreensão e a aplicação de toda a legislação existente sobre o tema.

Aqui também, nos casos ora em julgamento, surge outra auspiciosa oportunidade para que a Corte, no contexto das relações entre os gestores públicos e os titulares de dados pessoais, examine o âmbito de proteção do direito à autodeterminação informativa, mais precisamente os limites e as salvaguardas institucionais que se aplicam ao compartilhamento de informações entre órgãos e entidades da administração pública federal.

Pois bem. Examino inicialmente as preliminares ao mérito suscitadas pela Advocacia-Geral da União na Ação Direta de Inconstitucionalidade 6.649 e na Arguição de Descumprimento de Preceito Fundamental 695.

Em seguida, adentro a controvérsia constitucional que compõe a essência das ações de controle concentrado, debruçando-me sobre as teses deduzidas pelo Conselho Federal da Ordem dos Advogados do Brasil e pelo Partido Socialista Brasileiro (PSB).

Ao apreciar as ações de controle concentrado, avalio se é legítimo o compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, examinando a compatibilidade do Decreto 10.046/2019 com o regime de proteção de dados estabelecido pela ordem constitucional brasileira.

1. Admissibilidade

Em manifestação escrita na ADI 6.649, a Advocacia-Geral da União alega o não cabimento da ação direta de inconstitucionalidade para impugnação de regulamentos ou atos normativos que exorbitam do poder

regulamentar. Afirma, em síntese, que o Decreto 10.046/2019 constitui ato normativo estritamente subordinado, dependente de lei, de modo que as teses deduzidas pelo autor não caracterizariam ofensa direta ao texto constitucional.

Com a devida vênia, entendo que não prospera a preliminar articulada na manifestação da AGU, pelas razões que passo a expor.

A propósito do tema, a jurisprudência do Supremo Tribunal Federal realmente se consolidou no sentido de não se admitir ação de controle concentrado de atos normativos secundários, quando as razões que inspiram a ação direta pressupõem prévio confronto entre o regulamento administrativo e a legislação infraconstitucional. A esse respeito, são ricas as considerações feitas pelo eminente Ministro Celso de Mello, na ADI 1.347/DF:

> [...] o eventual extravasamento, pelo ato regulamentar, dos limites a que se acha materialmente vinculado poderá configurar insubordinação administrativa aos comandos da lei. Mesmo que desse vício jurídico resulte, num desdobramento ulterior, potencial violação da Carta Magna, ainda assim estar-se-ia em face de uma situação de inconstitucionalidade meramente reflexa ou oblíqua, cuja apreciação não se revela possível em sede de jurisdição concentrada.

As razões que inspiram essa orientação jurisprudencial são evidentes. Prevalece na doutrina que controlar a constitucionalidade significa aferir a compatibilidade de determinada interpretação ou aplicação de leis ou atos normativos em face do texto constitucional.

Como anota Jorge Miranda, a constitucionalidade e a inconstitucionalidade designam conceitos de relação, isto é, "a relação que se estabelece entre uma coisa – a Constituição – e outra coisa – um comportamento – que lhe está ou não conforme, que com ela é ou não compatível, que cabe ou não no seu sentido" (Manual de Direito Constitucional, Coimbra: Coimbra Editora, 1983, pp. 273-274).

São justamente essas premissas que orientaram a jurisprudência do Supremo Tribunal Federal acerca do não cabimento do controle abstrato, quando a articulação da tese de inconstitucionalidade pressupõe prévio exame de dispositivos infraconstitucionais. Por isso, a Corte tem repelido ações diretas fundadas exclusivamente na alegação de insubordinação do poder regulamentar aos comandos da lei, nelas identificando uma situação de ofensa meramente reflexa ou oblíqua que escapa dos limites do controle concentrado de constitucionalidade.

Por outro lado, não são poucos, tampouco isolados, os precedentes em que o Tribunal conheceu de ações diretas de inconstitucionalidade ajuizadas contra decretos editados pelo Poder Executivo, sobretudo quando se trata de regulamento com perfil autônomo ou de decreto que, a pretexto de dar fiel execução à lei, exorbita flagrantemente do âmbito do poder regulamentar (ADI-MC 2.155/PR, Rel. Min. Sydney Sanches, DJ 1º.6.2001; ADI-MC 1.435/DF, Rel. Min. Francisco Rezek, DJ 6.8.1999; ADI 1.969-MC, Rel. Min. Marco Aurélio, DJ 5.3.04; e ADI 2.950-AgR, Rel. Min. Marco Aurélio, redator para acórdão Min. Eros Grau).

No presente caso, é evidente que o decreto editado pelo Poder Executivo não se esgota na mera regulamentação de dispositivos da Lei 12.527/2011, que dispõe sobre o acesso à informação na administração pública, e da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais.

Em diversos aspectos, o Decreto 10.046/2019 parece ter força normativa própria, introduzindo alterações na ordem jurídica vigente. É o que ocorre, à guisa de exemplo, com a instituição do Cadastro Base do Cidadão, que reúne, em uma base unificada, informações biográficas que constam nas diferentes bases temáticas que atualmente compõem o acervo de dados da Administração Pública Federal (art. 16). Chama a atenção, ainda, a criação do Comitê Central de Governança de Dados (art. 21), com poder de (i) deliberar sobre a exata extensão dos dados bio-

gráficos que constarão do Cadastro Base do Cidadão (incisos VII e VIII); (ii) definir as hipóteses de compartilhamento amplo, restrito e específico; e (iii) fixar regras e parâmetros para o compartilhamento de dados entre órgãos da Administração Pública Federal (incisos I e II).

Convém ressaltar que o próprio Presidente da República reconheceu que, ao editar o Decreto 10.046/2019, operava com relativa margem de liberdade, e não apenas com a finalidade de dar fiel execução às leis. Não por outra razão, invocou tanto a prerrogativa prevista no art. 84, caput, IV, da Constituição Federal quanto aquela prevista no inciso VI, alínea "a", do mesmo dispositivo, que assegura ao Chefe do Poder Executivo o poder de expedir decretos de perfil não regulamentar, cujo fundamento de validade repousa diretamente na Constituição.

Examino as preliminares suscitadas pela Advocacia-Geral da União na ADPF 695, designadamente as alegações de ausência de indicação precisa do ato do Poder Público, de inobservância do requisito de subsidiariedade e de ausência do interesse de agir.

De início, reputo que a lesão a preceitos fundamentais por ato do Poder Público – compartilhamento de dados da Carteira Nacional de Habilitação entre o SERPRO e a ABIN – parece estar suficientemente indicada na peça inicial, sendo comprovada pelos documentos colacionados aos autos, que indicam (i) a transmissão da informação por veículo de mídia; e (ii) a confirmação desta em manifestação das autoridades. Em um primeiro juízo, tais documentos mostram-se suficientes para a comprovação do ato concreto, em consonância ao art. 3º, II, da Lei 9.882/99.

No mais, intimada, a União juntou aos autos acervo probatório complementar – em especial a Portaria 15/2016, do DENATRAN, e o Termo de Autorização 07/2020, emitido pelo DENATRAN em favor da ABIN, documentos que contribuem para a compreensão dos exatos contornos do ato do Poder Público impugnado na ADPF.

Afasto, ainda, a alegação de ausência de impugnação adequada de todo o complexo normativo em que a medida administrativa está inserida. Dos documentos já ressaltados e dos fundamentos da exordial é possível aferir com perfeição tanto os parâmetros de controle quanto o ato do Poder Público impugnado pelo requerente, sendo isso suficiente ao conhecimento da ADPF.

Também não vislumbro desrespeito ao requisito da subsidiariedade. Importa destacar, a princípio, que a Lei 9.882/99 impõe que a arguição de descumprimento de preceito fundamental somente será admitida se não houver outro meio eficaz de sanar a lesividade (art. 4º, § 1º).

Uma leitura apressada do dispositivo poderia conduzir à compreensão de que o cabimento da arguição de descumprimento de preceito fundamental se restringe às hipóteses de absoluta inexistência de qualquer outro meio capaz de tutelar a ordem constitucional.

Uma leitura mais cuidadosa, porém, revela que, na análise sobre a eficácia da proteção de preceito fundamental, deve predominar enfoque objetivo ou de proteção da ordem constitucional objetiva. Em outros termos, o princípio da subsidiariedade – inexistência de outro meio eficaz de sanar a lesão – há de ser compreendido no contexto da ordem constitucional global.

O caráter enfaticamente objetivo do instituto, assim, enseja a interpretação no sentido de que o meio eficaz de sanar a lesão parece ser aquele apto a solver a controvérsia constitucional relevante de forma ampla, geral e imediata.

No âmbito da ADPF, o ajuizamento da ação e sua admissão estão vinculados, muito provavelmente, ao significado da solução da controvérsia para o ordenamento constitucional objetivo, e não à proteção judicial efetiva de uma situação singular. Assim, o juízo de subsidiariedade há de ter em vista, especialmente, a lógica já consolidada dos processos objetivos

no sistema constitucional (ADPF 33, de minha Relatoria; ADPF 79, Rel. Min. Cezar Peluso, 4.8.2005; ADPF 99, Rel. Min. Ricardo Lewandowski, 8.3.2010; e ADPF 76, da minha relatoria, 13.2.2006).

Ante a inexistência de outro processo de índole objetiva apto a solver, de uma vez por todas, a controvérsia constitucional, afigura-se integralmente aplicável a arguição de descumprimento de preceito fundamental. É que as ações originárias e o próprio recurso extraordinário não parecem, as mais das vezes, capazes de resolver a controvérsia constitucional de forma geral, definitiva e imediata.

No presente caso, a potencial lesão a preceitos fundamentais consuma-se tão logo ocorra o compartilhamento de dados pessoais pretendido pelas autoridades do Poder Público. Dessa forma, mesmo que fosse cabível o manejo de instrumentos processuais ordinários, não haveria tempo hábil para uma resposta jurisdicional apta a sanar, de modo eficaz, o risco de grave comprometimento de valores essenciais contemplados pelo texto constitucional.

Rememoro também a fórmula da relevância do interesse público para justificar a admissão da arguição de descumprimento – explícita no modelo alemão –, que está implícita no sistema criado pelo legislador brasileiro, tendo em vista o caráter marcadamente objetivo que conferiu ao instituto.

Assim, o Supremo Tribunal Federal poderá, ao lado de outros requisitos de admissibilidade, emitir juízo sobre a relevância e o interesse público contido na controvérsia constitucional, podendo recusar a admissibilidade da ADPF sempre que não vislumbrar relevância jurídica na sua propositura.

O caso concreto tem a necessária relevância. Tem por fim evitar a lesão ao direito fundamental à dignidade da pessoa humana, à intimidade e à vida privada, na esteira do reconhecimento, em julgamento recente do

Tribunal Pleno, da proteção de dados pessoais como direito fundamental autônomo (ADI 6.387, Rel. Min. Rosa Weber).

Enfim, por qualquer ângulo que se aprecie a matéria, não me parece razoável impedir o escrutínio do tema pelo Supremo Tribunal Federal, seja pela relevância das teses invocadas na ADPF, que se relacionam diretamente com o regime constitucional de proteção de dados pessoais, seja pelo risco de afetação da privacidade de milhares de brasileiros.

O presente julgamento franqueia ao Tribunal Pleno a possibilidade de se debruçar sobre o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público. Põe em perspectiva, portanto, uma questão de crucial importância para qualquer sociedade democrática contemporânea, qual seja, o alcance, os limites e a fisionomia do direito à autodeterminação informativa.

Assim, com a devida vênia, entendo que seria temerário subtrair essa questão do controle abstrato de normas pelo Supremo Tribunal Federal, relegando-a a instrumentos processuais que não oferecem meios de solver a controvérsia constitucional de forma ampla, geral e imediata.

Por tudo, a arguição de descumprimento de preceito fundamental não apresenta óbices intransponíveis a impedir a apreciação das teses articuladas na inicial (art. 4º da Lei 9.882/1999).

2. Mérito

Não há como negar que existem razões fundadas para as preocupações externadas pelo requerente. Infelizmente, ainda há autoridades públicas que insistem no mau vezo de inverter a hierarquia das normas, acreditando menos na Constituição e nas leis do que em regulamentos editados pelo Poder Executivo. E, o que é pior, não raras vezes essa postura se ampara em leituras distorcidas do próprio texto do ato regula-

mentar, cujos limites semânticos não dão margem para a interpretação ilegítima proposta pelo administrador (também comum, nessa seara, é a tentação de fraudar a jurisdição deste Supremo Tribunal Federal mediante o achamboado expediente de revogações de atos infralegais às vésperas de sessão de julgamento).

Os exemplos são os mais variados e falam por si. Sem grandes digressões, temos aqui, em julgamento na ADPF 695, uma tentativa obscura de compartilhamento massivo dos dados pessoais de 76 milhões de brasileiros com órgãos integrantes do Sistema Brasileiro de Inteligência. Causa perplexidade que, ao se manifestar nos autos, a União pretendeu amparar essa prática manifestamente inconstitucional em permissões supostamente conferidas pelo Decreto 10.046/2019, ignorando os princípios mais comezinhos do regime constitucional de proteção de dados.

Além disso, todos nós conhecemos – porque a controvérsia desaguou neste Tribunal – a tentativa de edição da Medida Provisória 954/2020, que determinava que as operadoras de telefonia disponibilizassem ao IBGE, em meio eletrônico, os nomes, números de telefone e endereços de milhões de usuários de serviços de telecomunicação. O caso foi conduzido com excelência pela EMINENTE MINISTRA ROSA WEBER, que não hesitou em apontar a flagrante inconstitucionalidade da medida provisória e o risco que ela oferecia a liberdades públicas consagradas pelo regime democrático (ADI 6.387).

Também é grave a notícia trazida pelo Laboratório de Políticas Públicas e Internet de que o Comitê Central de Governança de Dados, no exercício de suas atribuições regulamentares, recomendou que dados pessoais fossem submetidos ao nível de compartilhamento restrito. Segundo cartilha elaborada pelo Comitê, pertenceriam a essa categoria as seguintes informações biográficas: nome completo, endereço, números de identificação (CPF, NIS e título eleitoral), situação civil, data de nascimento, telefone e endereço de e-mail (disponível em https://www.gov.br/

governodigital/pt-br/governanca-dedados/formulario_regras-de-compartilhamento_modelo-v1-0.pdf).

O evento preocupa, na medida em que, por definição, o nível de compartilhamento restrito engloba dados que, apesar de sigilosos, podem ser livremente acessados por todos os órgãos e entidades da Administração Pública Federal. Cuida-se, assim, de categoria que almeja impedir o acesso do público externo a dados cujo sigilo seja imprescindível à segurança da sociedade e do Estado, sem obstaculizar o livre fluxo das informações entre os diferentes órgãos que compõem o aparelho estatal.

Por permitirem ampla difusão de dados sensíveis entre entidades governamentais, os limites impostos pelo nível de compartilhamento restrito oferecem proteção inadequada para a tutela dos valores estruturantes da LGPD. Salta aos olhos, portanto, o manifesto equívoco cometido pelo Comitê Central de Governança de Dados, ao editar recomendação que encerra grave risco de malversação de dados pessoais e de violação da privacidade dos usuários do serviço público.

Tudo isso reforça a premente necessidade de exercermos com extremo rigor o controle de políticas públicas que possam afetar substancialmente o direito fundamental à proteção de dados pessoais. No caso específico do Decreto 10.046/2019, diante dos excessos praticados pela Administração Pública Federal, impõe-se uma correção de rumos, com o objetivo de imunizar o texto normativo contra leituras desviantes da Constituição Federal.

Para tanto, afigura-se adequada solução que, preservando ao máximo a autoridade do Chefe do Poder Executivo e o espaço de conformação que é inerente ao exercício do poder regulamentar, empreenda interpretação do Decreto 10.046/2019 que o coloque em conformidade com a Constituição Federal.

Nessa senda, cumpre que indaguemos, antes de mais nada, se a in-

terpretação conforme à Constituição tem lugar para o caso em apreço. A resposta para tanto passa pela devida contextualização da interpretação conforme à Constituição no quadro mais geral das fórmulas decisórias intermediárias.

A expansão de tarefas e papéis atribuídos ao poder público, mormente após a segunda metade do século XX, importou em novo modelo de organização política, o "Estado Social", cuja realização dependia de um incremento (tanto no campo temático como no grau de intensidade) das atividades legislativa e administrativa. (FORSTHOFF, Ernst. "Begriff und Wesen des sozialen Rechtsstaates". In: Rechtsstaat im Wandel. Verfassungsrechtliche Abhandlungen, 1950-1964. Stuttgart: W. Kohlhammer, 1964, p. 38; ALEXY, Robert. Theorie der Grundrechte. Frankfurt: Suhrkamp, 1986, p. 395 e ss.).

Ao Estado foram imputados deveres até então inéditos e, de seu descumprimento, originaram-se expedientes inconstitucionais também singulares, frente aos quais a jurisdição constitucional teve que aprender a lidar. Tal como a chamada omissão parcial. Nela, como leciona Hartmut Maurer, a inconstitucionalidade se materializa em uma disciplina normativa diferenciada (Unterschiedlichkeit der Regelung), que vulnera o princípio da isonomia. (MAURER, Hartmut. "Zur Verfassungswidrigerklärung von Gesetzen". In: Im Dienst an Recht und Staat: Festschrift fur Werner Weber. Berlim: Dunker und Humbolt, 1974, p. 345).

Assim, diz Jörn Ipsen, a inconstitucionalidade não é imputável a uma regra jurídica isoladamente considerada: o que se tem é a inconstitucionalidade de uma chamada relação normativa (verfassungwidrige Normrelation) (IPSEN, Jörn. Rechtsfolgen der Verfassungsidrigkeit von Norm und Eizelakt. Baden-Baden: Nomos Verlag, 1980, p. 213 e ss.)

Nesse sentido, o Tribunal Constitucional Alemão, já em 1958, no caso Teuerungszulage, lavrou ensinamento jurisprudencial destinado a fazer fortuna no constitucionalismo contemporâneo: em se tratando de

omissão parcial, não obstante a inconstitucionalidade da norma, uma consequente declaração de nulidade "causaria uma situação na qual a ordem constitucional seria respeitada ainda menos". (BVerfGE 8, 1, Primeiro Senado, em 11 de junho de 1958).

O tratamento dogmático e jurisprudencial da omissão parcial foi apenas o primeiro passo. Desde então, os tribunais constitucionais desenvolveram amplo leque de fórmulas decisórias intermediárias, expressão pela qual Gustavo Zagrebelsky e Valeria Marcenò agrupam estilos de decisões e técnicas processuais cujo traço comum está em conferir, à jurisdição constitucional, possibilidades outras que não o binário "lei constitucional e portanto válida" versus "lei inconstitucional e, portanto, nula". Técnicas essas funcionalmente orientadas para preservar a utilidade das decisões dos Tribunais Constitucionais naqueles casos em que – pontifica Zagrebelsky – "a eliminação pura e simples da lei não remediaria a inconstitucionalidade, mas concorreria, paradoxalmente, a produzir resultados de inconstitucionalidade ainda mais grave". (ZAGREBELSKY, Gustavo e MARCENÒ, Valeria. Giustizia Costituzionale. Bolonha: il Mulino, 2012, p. 338).

A interpretação conforme à Constituição insere-se plenamente nesse marco. Filia-se ao gênero das técnicas decisórias intermediárias, porquanto seu uso pressupõe e orienta-se pela função primordial de afastar a produção de resultados inconstitucionais. Para assim fazê-lo, a interpretação conforme à Constituição se vale da diferença entre texto e norma, nisso compreendidas distinções correlatas, como disposição e norma, texto legislativo e programa normativo etc. Pressuposto hermenêutico este que, de resto, fundamenta técnicas decisórias intermediárias congêneres, como a declaração parcial qualitativa de inconstitucionalidade.

É em conformidade com esses pressupostos que a técnica da interpretação conforme consegue evitar a solução radical de operar o expurgo total ou parcial de texto normativo. Trata-se de solução que observa aque-

la “exigência de gradualidade” que se espera das intervenções de um Tribunal quando em jogo atos normativos produzidos pelos demais Poderes.

Daí o acerto de Zagrebelsky ao pontificar que “a inconstitucionalidade da lei é a falência da interpretação”. Sim, porque a adoção de “soluções menos incidentes”, como a interpretação conforme e demais técnicas intermediárias, não é algo desejável apenas por motivos de ordem prática, e sim postura que se espera do julgador por razões de ordem constitucional (ZAGREBELSKY, Gustavo e MARCENÒ, Valeria.

Giustizia Costituzionale. Bolonha: il Mulino, 2012, p. 385 e 401). Razões como a cláusula da separação dos poderes e demais princípios que a desenvolve, como o princípio da conformidade funcional (MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 14ª ed. São Paulo: Saraiva, 2019, p. 94).

Nesse marco, deixo expressamente assentado que o primeiro critério que servirá de norte para o manejo da interpretação conforme à Constituição no caso em apreço, é aquele que homenageia a função precípua dessa técnica de decisão intermediária: a de afastar a produção de resultados inconstitucionais extremos.

Explicito, também, um segundo critério.

É bem verdade que é mais simples divisar uma dimensão negativa da interpretação conforme à Constituição. Assim se dá quando, por exemplo, o Tribunal delibera pela exclusão de interpretações consideradas inconstitucionais. Mas nem só de efeitos cassatórios vive a interpretação conforme à Constituição. As Cortes Constitucionais também se valem dessa técnica para colmatar lacunas, em atividade de otimização constitucional, mediante a qual, preleciona Christoph Gusy, se procede à construção normativa por analogia, redução, ou por derivação de premissas normativas da Constituição (GUSY, Christoph.

Parlamentarischer Gesetzgeber und Bundesverfassungsgericht. Ber-

lim: Duncker und Humblot, 1985, p. 214; ZIPPELIUS, Reinhold. "Verfassungskonform Auslegung von Gesetzen". In: Bundesverfassungsgericht und Grundgesetz. Vol. 2. Tübingen: Mohr Siebeck, 1976, p. 121).

É assim porque, há tempos, a atuação da jurisdição constitucional não mais se resume àquela função negativa, relacionada à eliminação de normas contrárias à Constituição descrita pela figura do "legislador negativo". Desempenha também funções positivas de "recomposição interpretativa" e de "integração normativa" do ordenamento jurídico. (ZAGREBELSKY, Gustavo e MARCENÒ, Valeria. Giustizia Costituzionale. Bolonha: il Mulino, 2012, p. 338).

Coerente a esse marco, o Professor Emérito da Universidade de Roma "La Sapienza" e Juiz da Corte Constitucional da Itália, Franco Modugno, ensina que da interpretação conforme à Constituição não se espera, apenas, a função negativa de invalidação de normas oriundas da interpretação de um dispositivo, mas também a função positiva de promover a coerência do ordenamento jurídico, obstando que a legislação infraconstitucional faça "sistema em si mesma", no exato instante em que promove a integração desta com o plexo normativo superior. (MODUGNO, Franco. "Metodi ermeneutici e Diritto Costituzionale". In: Scritti sull'Interpretazione Costituzionale. Nápoles: Editoriale Scientifica, 2008, p. 68 e ss.)

Não poderia ser diferente, uma vez que a interpretação conforme à Constituição traduz espécie, variante ou subdivisão da interpretação sistemática (SPANNER, Hans. "Die verfassungskonforme Auslegung in der Rechtsprechung des Bundesverfassungsgerichts". In: Archiv des öffentlichen Rechts. Vol. 91, n. 4. Tübingen: Mohr Siebeck, 1966, p. 503;

HAAK, Volker. Normenkontrolle und verfassungskonforme Gesetzesauslegung des Richters. Eine rechtsvergleichende Untesuchung. Bonn: Roehrscheid, 1963, p. 259; EBSEN, Ingwer. Das Bundesverfassungsgericht als Element gesellschaftlicher Selbstregulierung. Eine pluralistische Theorie der Verfassungsgerichtsbarkeit im demokratischen Ver-

fassungsstaat. Berlim: Duncker und Humblot, 1985, p. 91).

Precisamente por isso, a interpretação que busque garantir a supremacia da Constituição requer que a superioridade da norma constitucional ocorra não apenas negativamente. A Constituição não pode ser reduzida à função de fornecer um limite ao direito infraconstitucional, exatamente porque o texto maior é algo que se realiza no tempo, e não um dado inerte:

> "Não é um dado 'inerte' que possa ser tomado como critério fixo para determinar um ponto exato dentro de uma banda de oscilação de significados normativos possíveis de uma disposição legislativa. Em outras palavras, interpretar uma disposição com base em outras significa realizar uma interpretação sistemática, isto é, construir uma norma compatível com todas." (CHESSA, Omar. "Non manifesta infondatezza versus interpretazione adeguatrice?". In: D'AMICO, Marilisa; RANDAZZO, Barbara (orgs.). Interpretatzione conforme e tecniche argomentative. Turim: Ed. Giappichelli, 2009, p. 272) (grifou-se).

Daí ser premente a valorização do componente positivo da superioridade da Constituição, que conduz à transformação dos dispositivos interpretados em normas consoantes à Constituição. Exsurge, com isso, o segundo critério que orientará o uso da técnica decisória requerida: uma interpretação adequada das normas infralegais ora impugnadas não há de se contentar com o simples cotejo da literalidade do texto de decretos com padrões normativos superiores (Lei Geral de Proteção de Dados, Constituição Federal). Antes, exige reconstrução normativa sistemática.

Atento a essas premissas, assinalo que, no caso vertente, a declaração de inconstitucionalidade de todo o panorama normativo, esvaziando todo o seu alcance, acabaria por destituir os órgãos do Poder Executivo de normas operacionais necessárias ao compartilhamento de dados no interesse da eficiente prestação de serviços públicos. Nesse sentido, a extirpação pura e simples da norma impugnada poderia acarretar, fundamentalmente, a formação de vácuo regulamentar numa área relevante e

sensível para o gestor público, com impactos nocivos para a eficiência e segurança da atividade administrativa.

Em um outro cenário, caso se entenda pela repristinação do Decreto 8.789/2016, revogado pelo atual regulamento, o resultado seria ainda mais nocivo à proteção de privacidade. A norma anterior estabelecia que os dados cadastrais sob gestão dos órgãos públicos federais seriam "compartilhados entre as bases de dados oficiais, preferencialmente de forma automática, para evitar novas exigências de apresentação de documentos e informações e possibilitar a atualização permanente e simultânea dos dados".

Dado o obsoletismo do texto anterior, é lícito concluir que o efeito repristinatório da declaração de inconstitucionalidade causaria ainda mais insegurança e instabilidade, na medida em que os dispositivos revogados não apenas impunham o compartilhamento automático de informações cadastrais entre todos os órgãos públicos federais, como também silenciavam completamente a respeito da adoção de salvaguardas institucionais para proteção de dados pessoais.

Evidencia-se, a não mais poder, a necessidade de adoção da técnica decisória intermediária da interpretação conforme à Constituição.

Com efeito, por qualquer ângulo que se observe a matéria, parece-me mais adequado, no contexto do equilíbrio que deve existir entre os Poderes, preservar o programa normativo contido no decreto presidencial em tudo aquilo que estiver alinhado com a Constituição Federal. E, como visto, são muitas as possibilidades de tratamento legítimo de dados pessoais por órgãos e entidades governamentais.

Por tudo o quanto foi dito, adianto que o objeto desta fiscalização em abstrato de constitucionalidade, o Decreto 10.046/2019, pode ostentar sentido compatível com o texto constitucional. Ante a polissemia da norma, que conduziu a eventos recentes de grave descumprimento de

preceitos fundamentais, é dever do Tribunal atuar diligentemente para, empregando a técnica decisória adequada, subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais.

Passo a fazê-lo, atento, em primeiro lugar, ao papel que a jurisdição constitucional tem assumido, no direito comparado, para a criação de mecanismos de salvaguarda de posições jurídico-fundamentais em face do desenvolvimento tecnológico. Após, discorro sobre o âmbito de proteção e perfil do direito fundamental em jogo (autodeterminação informacional), bem como sua concorrência com princípios formais como o da supremacia do interesse público. Realizado esse percurso, obteremos o parâmetro adequado, acredito, para conformar o programa normativo do Decreto 10.046/2019 à Constituição Federal.

2.1 Inovação jurídica como contraface da inovação técnica: a permanente abertura da ordem constitucional à transformação tecnológica por obra da jurisdição constitucional comparada.

A discussão travada nestes autos testa as possibilidades e os limites da proteção constitucional do direito à privacidade (art. 5º, inciso X, da CF), vis-à-vis os riscos desencadeados pelo constante avanço tecnológico que caracteriza a nossa sociedade da informação.

Na era digital, as novas tecnologias de comunicação se tornaram condição necessária para a realização de direitos básicos – como se faz evidente no campo da liberdade de expressão, de manifestação política e de liberdade religiosa. Contudo, verifica-se que esses mesmos avanços tecnológicos suscitam riscos generalizados de violação de direitos fundamentais básicos.

Como muito bem destacado por Wolfgang Hoffmann-Riem, é necessário que, diante das ameaças geradas pelo desenvolvimento da tecnolo-

gia, a jurisdição constitucional atue como instrumento de inovação jurídica, visando à constante atualização da tutela dos direitos fundamentais:

> As tecnologias oferecem um enorme potencial, e não é exagero referir-se às oportunidades decorrentes da sociedade da informação. Na maioria dos aspectos da vida diária, os cidadãos são hoje obrigados a utilizar as novas tecnologias para não serem social e economicamente marginalizados. Mas as novas tecnologias também trazem consigo um potencial de perigo: não só o de terceiros, incluindo o Estado, penetrando na esfera privada, mas também o desenvolvimento de um poder de comunicação e de poder econômico que impõe seus interesses seletivamente através de manipulação ou por outros meios (tradução livre) (HOFFMANN-RIEM, Wolfgang.
>
> "Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información". In: ReDCE, n. 22, 2014).

O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. O crescimento exponencial das atividades de coleta, tratamento e análise de dados pessoais possibilita que governos e empresas utilizem algoritmos e ferramentas de data analytics, promovendo classificações e estereotipações discriminatórias de grupos sociais na tomada de decisões estratégicas para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham.

Alguns exemplos nesse sentido são dignos de nota. Nos Estados Unidos, por exemplo, uma ferramenta de gerenciamento automatizado do sistema prisional chamada de Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tem sido utilizada para avaliação do risco de reincidência dos egressos. Essa ferramenta funciona a

partir de árvore decisória, que classifica os detentos em um espectro de risco que varia de um a nove, sendo nove o mais alto e um o mais baixo.

Em 2017, a Suprema Corte de Wisconsin manteve a condenação de um réu que foi acusado de fugir da polícia ao dirigir um carro anteriormente utilizado em um tiroteio. Ele havia sido condenado previamente por agressão sexual e, após uma avaliação do algoritmo, considerou-se que havia alto risco de reiteração delitiva, a justificar a imposição da pena privativa de liberdade de seis anos.

Todo esse panorama nos indica que, em certas áreas, o processo artesanal de tomada de decisões críticas para o Estado de Direito tem sido progressivamente substituído por soluções automatizadas. Em decorrência dessas transformações, é inequívoco que, sob o influxo da dimensão objetiva dos direitos fundamentais, surge um dever estatal de proteção dos valores estruturantes do regime democrático, por meio da criação de salvaguardas institucionais que preservem a essência da cidadania.

É por isso que, diante dos riscos inerentes à sociedade da informação, cabe ao Tribunal, de um lado, reconhecer que a disciplina jurídica do processamento e da utilização de dados pessoais acaba por afetar o sistema de proteção de garantias individuais como um todo e, de outro, proceder a uma releitura de mecanismos clássicos de defesa das liberdades públicas e do Estado Democrático de Direito.

Esse ambiente faz com que os Tribunais Constitucionais tenham que proceder a uma constante reafirmação da força normativa da Constituição, de modo a preservar garantias individuais que constituem a base do regime democrático e que, hoje, são diretamente ameaçadas pelo descompasso entre o poder de vigilância e os mecanismos de proteção da intimidade.

Os riscos inerentes à era digital devem ser considerados na leitura e na aplicação da Constituição Federal de 1988. Aliás, ousaria dizer que

nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica. Dentro da tradição do judicial review norte-americano, por exemplo, mesmo os juristas partidários do originalismo constitucional reconhecem que a inovação naturalmente levanta questões sobre como a Constituição se aplica aos novos fenômenos sociais. Como advertiu o professor Lawrance Lessig, em 1996, no contexto da disseminação da internet:

> "Os Founding Fathers deram ao povo uma Constituição para um mundo onde a tecnologia era imperfeita. Nesse mundo, a liberdade reinava, não tanto porque a lei positiva a criava; mas porque as tecnologias imperfeitas se submetiam à justiça. Quando as tecnologias daquele mundo mudam, nós nos confrontamos com uma escolha. Podemos permitir que a ideia de eficiência tecnológica impere nesse novo espaço digital, fazendo com que as liberdades protegidas pela Constituição se esvaziem; ou podemos recriar as esferas de liberdade para superar àquelas pensadas em um contexto de imperfeição tecnológica" (tradução livre) (LESSIG, Lawrence. "Reading The Constitution in Cyberspace". In: Emory Law Review, v. 45, p. 869–910, 1996, p. 41).

Essa visão, a propósito, foi muito bem simbolizada no voto dissidente do Juiz Louis Brandeis, em 1928, no caso United States v. Olmstead. O processo envolvia discussão acerca do alcance normativo da Quarta Emenda da Constituição norte-americana, que garante a inviolabilidade da pessoa, da sua casa, de seus documentos e de seus bens contra a realização de buscas e apreensões ilegítimas (unreasonable searches and seizures). Havia dúvida sobre a incidência dessa garantia no caso de interceptação telefônica realizada por meio da instalação de equipamento de escuta em cabos telefônicos localizados na via pública. O voto majoritário considerou que, como ouvir uma conversa telefônica privada não exige invasão física do espaço privado do cidadão – o interior da residência –, não seria necessária a prévia autorização judicial.

A divergência inaugurada pelo Juiz Brandeis, por outro lado, reconheceu o caráter fundamental do direito à privacidade, encarado por ele como pedra angular do regime de liberdades assegurado pela Constituição americana ("the most comprehensive of rights and the right most favored by civilized men"). Partindo dessa premissa, sustentou que, mesmo nos casos em que não ocorre a invasão do domicílio, a realização de interceptação telefônica dependeria de prévia autorização judicial.

Entre os fundamentos de seu voto, o Juiz da Suprema Corte reconheceu a necessidade de conferir às garantias constitucionais uma capacidade de adaptação aos novos fenômenos sociais. Alertou ainda que:

> "(...) assim como as limitações gerais aos poderes de governo, como as incorporadas na cláusula do devido processo legal, não podem proibir o Estado de legislar sobre fenômenos modernos que um século atrás, ou mesmo meio século atrás, provavelmente seriam considerados arbitrários, (...) da mesma forma, as normas jurídicas que garantem ao indivíduo proteção contra abusos de poder específicos também devem ter uma capacidade de adaptação a um mundo em constante mudança" (tradução livre) (Olmstead v United States 277 US 438, 472, 1928, Voto Dissidente do Juiz L. Brandeis).

Essa abertura da jurisdição constitucional à transformação tecnológica enquanto instrumento de preservação dos direitos fundamentais também é consolidada na tradição continental. No icônico precedente da Lei do Censo alemã, julgado em 1983 (BVerfGE 65, 1), cuja análise será aprofundada neste voto, resta evidente que o avanço das técnicas de coleta e processamento de dados foi tomado como válvula de reconfiguração da proteção jurídica à personalidade. A decisão baseou-se principalmente no diagnóstico de que, a partir da coleta e cruzamento de dados do censo, "seria possível a criação de um quadro abrangente e detalhado da respectiva pessoa - um perfil de personalidade -, mesmo na área íntima; o cidadão torna-se uma verdadeira 'pessoa transparente'".

Desse modo, em linha com todas essas experiências históricas, as-

sento que o espírito hermenêutico que deve guiar o Tribunal no tratamento da matéria em exame deve ser o de renovar o compromisso de manter viva a força normativa da Constituição Federal de 1988, nela encontrando caminhos, e não entraves, para a proteção jurídica da intimidade enquanto garantia básica da ordem democrática.

2.2 Direito fundamental à proteção de dados pessoais: da proteção à intimidade à consagração no texto constitucional (EC n. 115/2022)

Dentro da teoria jurídica moderna, a compreensão histórica do direito à privacidade é comumente vinculada – com todas as possíveis e necessárias ressalvas – à publicação do seminal artigo "The Right to Privacy", escrito por Samuel Warren e Louis Brandeis ainda no final do século XIX (Warren, S., & Brandeis, L. (1890). "The Right to Privacy". Harvard Law Review, 4(5), p. 193-220). Esse texto revelou-se paradigmático por ter possibilitado, a partir de precedentes da tradição do common law, a identificação de um direito de privacidade de natureza pessoal independente da estrutura da tutela da propriedade.

Nessa concepção tradicional, o direito à privacidade pressupunha uma dicotomia entre as esferas pública e privada, de maneira que o núcleo de sua proteção jurídica se esgotava no direito de ser deixado só ("the right to be left alone"). Em sentido fortemente individualista, a proteção atribuída ao direito à privacidade voltar-se-ia, portanto, a reconhecer uma posição estática e absenteísta do Estado: o direito do titular de retrair aspectos de sua vida do domínio público (BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Editora Gen, 2019, p. 95).

Entre nós, estudos voltados à identificação da autonomia do Direito à Privacidade parecem ter-se vinculado inicialmente a essa abordagem formal de um direito negativo de não intervenção. Tal abordagem foi reproduzida em artigo clássico do professor Tércio Sampaio Ferraz Júnior

intitulado “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado”, publicado em 1993 (FERRAZ JÚNIOR, Tércio. “Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado”. In: Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, 1993, p. 430-459).

Como corolário imediato da compreensão do direito à privacidade como uma proteção de caráter essencialmente negativo, eclodiu nos Tribunais brasileiros orientação jurisprudencial restritiva quanto ao âmbito de proteção do art. 5º, inciso XII, da Constituição da República. A título exemplificativo, reporto-me ao entendimento firmado no RE 418.416, Rel. Min. Sepúlveda Pertence, DJ de 10.05.2006, em que a Corte referendou o acesso de órgãos policiais a dados armazenados em discos rígidos (hard disks) apreendidos a partir de busca e apreensão autorizada pelo Poder Judiciário.

Naquela assentada, fazendo expressa referência à fórmula consagrada pelo professor Tércio Ferraz, o eminente Ministro Relator assentou que a proteção a que se refere o art. 5º, inciso XII, da Constituição Federal alcançaria apenas a comunicação de dados, e não os dados em si mesmos. Dessa forma, seria lícita a extração, no interesse da Justiça Criminal, de dados armazenados em equipamentos de informática apreendidos na sede da empresa investigada, desde que, evidentemente, a busca e apreensão tenha sido autorizada pela autoridade judicial competente.

Essa concepção do direito à privacidade como uma garantia individual de abstenção do Estado na esfera privada individual, todavia, passou por profundas transformações no decorrer do século XX. Devido ao próprio avanço das tecnologias da informação, assistiu-se a uma notória transformação do sentido e do alcance do direito à privacidade. Nas palavras de Stefano Rodotà vivenciamos verdadeiro “processo de inexorável reinvenção da privacidade” (RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15).

Tal processo de reinvenção do direito à privacidade é analisado com esmero e profundidade em seminal monografia do professor Danilo Doneda. Ao examinar as sucessões geracionais das leis de proteção de dados a partir da década de 1970, bem como o espraiamento da proteção jurídica da privacidade em tratados internacionais ao longo do século XX, o autor assevera que:

> "A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto sua adequação às novas tecnologias da informação. Não basta pensar a privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma 'predileção' individual, associada basicamente ao conforto e comodidade. (...)
>
> Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais em importância: passa a ser um pressuposto para que ela não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada e inviabilizariam o livre desenvolvimento da sua personalidade.
>
> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos" (grifos nossos) (DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 141-142).

A construção de uma nova dogmática constitucional acerca da tutela da privacidade coincide com o reconhecimento, em 1983, do direito à autodeterminação informacional (die informationelle Selbsstbestimmung) pelo Tribunal Constitucional Alemão.

A característica especial do direito à autodeterminação informativa não é resultante de um invencionismo episódico, mas sim de "*várias linhas de argumentação da jurisprudência do Tribunal, que já na decisão do microcenso, com recurso à sua jurisprudência sobre a dignidade humana, atribuiu ao cidadão individual uma esfera inviolável da vida privada, da qual se supõe que a influência da autoridade pública deve ser removida*" (FRANZIUS, Claudio. "Das Recht auf informationelle Selbstbestimmung". Zeitschrift für das juristische Studium. Gießen, 2015, p. 262).

No paradigmático Volkszählungsurteil (BVerfGE 65, 1), de 1983, o Tribunal declarou a inconstitucionalidade da chamada Lei do Censo alemã (Volkszählunsgesetz), que possibilitava que o Estado realizasse o cruzamento de informações sobre os cidadãos para mensuração estatística da distribuição especial e geográfica da população. Nesse julgado, a Corte Constitucional redefiniu os contornos do direito de proteção de dados pessoais, situando-o como verdadeira projeção de um direito geral de personalidade para além da mera proteção constitucional ao sigilo.

A partir da leitura ampliativa do artigo 2.1, em conjunto com o artigo 1.1. da Grundgesetz, o Tribunal Constitucional reconheceu a existência de um direito constitucional de personalidade que teria como objeto de proteção o poder do indivíduo de "decidir sobre a divulgação e o uso dos seus dados pessoais" („selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"), de "decidir sobre quando e dentro de quais limites os fatos da sua vida pessoal podem ser revelados" („zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden") e ainda "de ter conhecimento sobre quem sabe e o que sabe sobre si, quando e em que ocasião" („wissen können, wer was wann und bei welcher Gelegenheit über sie weiß"). (FRANZIUS, Claudio. "Das Recht auf informationelle Selbstbestimmung". Zeitschrift für das juristische Studium. Gießen, 2015, p. 259).

No caso concreto, o Tribunal entendeu que o processamento automatizado dos dados, possibilitado pela Lei do Censo de 1983, colocaria em risco o poder do indivíduo de decidir por si mesmo sobre se, e como, ele desejaria fornecer seus dados pessoais a terceiros. A situação de risco identificada pelo Tribunal referia-se à possibilidade concreta de, por meio de sistemas automatizados, as informações fornecidas sobre profissões, residências e locais de trabalho dos cidadãos serem processadas de modo a se formar um "perfil completo da personalidade".

Essa nova abordagem revelou-se paradigmática, por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso.

Como bem destacado na decisão, a identificação de um constante avanço tecnológico demanda igualmente a afirmação de um direito de personalidade que integre o contexto das "condições atuais e das futuras circunstâncias do processamento automático de dados" ("*heutigen und künftigen Bedingungen der automatischen Datenverarbeitung*").

É justamente essa reconfiguração que possibilita a afirmação do direito à autodeterminação informacional como contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo. Nas palavras ilustres de Stefano Rodotà, a privacidade também passa a ser definida como "o direito de manter o controle sobre suas próprias informações e de determinar como a privacidade é alcançada e, em última instância, como o direito de escolher livremente o seu modo de vida" (tradução livre) (RODOTÀ, Stefano. In diritto di avere. Roma: Laterza, 2012, p. 321).

Essa nova abordagem também engloba uma proteção abrangente que desloca o eixo da proteção de dados para as possibilidades e finalidades de seu processamento. Como bem destacado por Laura Schertel

Mendes, é decisivo para a concepção do direito à autodeterminação "*o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados", de modo que "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato de quão sensíveis ou íntimos eles são)*" (MENDES, Laura Schertel. "Autodeterminação informativa: a história de um conceito". In: Revista Pensar, Vol. 25, n. 4, pp. 1-18, 2020).

A abertura do texto constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados pode ser identificada na própria jurisprudência do Supremo Tribunal Federal. Ao apreciar o tema 582 da sistemática da repercussão geral, o Tribunal Pleno reconheceu o direito de acesso do contribuinte a banco de dados da Receita Federal que armazena informações de interesse da arrecadação federal (RE 673.707, Rel. Min. Luiz Fux, Tribunal Pleno, DJe 30.9.2015).

No julgamento, o voto proferido pelo EMINENTE MINISTRO LUIZ FUX reforçou o dever qualificado de proteção que é inerente ao armazenamento de informações pessoais em bancos de dados de entidades governamentais ou de caráter público geridos por entidades privadas. Contribuindo decisivamente para a gênese da jurisprudência atual sobre o regime constitucional de proteção de dados, o eminente Relator ressaltou que o art. 1º da Lei 9.507/97, que disciplina o habeas data, institui restrições para a divulgação de informações pessoais armazenadas em bancos de dados públicos, limitando "*a divulgação a outros órgãos, que não o detentor das informações, ou a terceiros, que não o titular dos dados registrados*".

Essa evolução jurisprudencial culminou, recentemente, no reconhecimento pelo Tribunal de que a proteção de dados pessoais e a autodeterminação informacional são direitos fundamentais autônomos, dos quais

decorrem tutela jurídica específica e dimensão normativa própria (ADI 6.387, Rel. Min. Rosa Weber). Em eloquente manifestação, o colegiado afirmou a necessidade de instituição de um controle efetivo e transparente da coleta, armazenamento, aproveitamento, transferência e divulgação de dados pessoais, ao mesmo tempo que reforçou a importância de a Corte exercer com extremo rigor o controle de políticas públicas que possam afetar substancialmente o direito fundamental à proteção de dados.

A partir de leitura abrangente do texto constitucional, especialmente do direito à privacidade e ao livre desenvolvimento da personalidade, o voto da EMINENTE MINISTRA ROSA WEBER suspendeu a eficácia da Medida Provisória 954/2020, editada em decorrência da pandemia da COVID-19, que determinava que as operadoras de telefonia disponibilizassem ao IBGE, em meio eletrônico, os nomes, números de telefone e endereços de milhões de usuários de serviços de telecomunicação.

Na ocasião, o Tribunal assentou três balizas constitucionais relevantes que devem informar qualquer espécie de incursão sobre o tema. Primeiro que, embora não exista no ordenamento jurídico uma proibição absoluta para o tratamento de dados por entidades públicas, a dogmática constitucional contemporânea impõe que a privacidade dos usuários só possa ser afastada a partir de uma justificação minudente e exaustiva das finalidades atribuídas ao tratamento de dados.

Segundo, estabeleceu-se que a incidência do princípio da transparência impõe que a Administração Pública garanta ao titular dos dados um nível de controle suficiente para a verificação prospectiva da licitude do tratamento de dados. Isso se desdobraria, de acordo com a decisão, em um dever de publicidade que seja capaz de fornecer ao cidadão condições mínimas de proceder a um controle da forma como o Estado lida com dados pessoais.

Por fim, que a intervenção estatal na esfera privada deve (i) envolver apenas o universo de dados estritamente necessário para o alcance das

finalidades eleitas; e (ii) ser acompanhada do incremento dos protocolos e mecanismos de segurança do sistema de informação, de acordo com o grau de risco gerado pela relativização do direito fundamental à autodeterminação informativa.

Como se vê, tais diretrizes partem do pressuposto de que o princípio da proporcionalidade desempenha relevante papel de aferição da constitucionalidade das interferências no regime constitucional de proteção de dados, inspirando-se nas premissas assentadas no julgamento da Lei do Censo, em 1983, pelo Tribunal Constitucional alemão.

A esse respeito, conforme destacado no voto do EMINENTE MINISTRO LUIZ FUX, a relativização do direito fundamental somente será legítima se "*(i) atender a propósitos legítimos, específicos, explícitos e informados; (ii) limitar a coleta ao mínimo necessário para a realização das finalidades normativas; (iii) estabelecer medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados; (iv) prevenir a ocorrência de danos, consoante os parâmetros desenhados no direito comparado e no art. 6º da Lei Geral de Proteção de Dados*".

A partir desse julgado paradigmático, o Plenário também superou a falsa ideia de que existem dados que a priori dispensam proteção constitucional. Em seu voto, o EMINENTE MINISTRO RICARDO LEWANDOWSKI explicou que informações aparentemente triviais, como o número de inscrição no CPF ou de uma linha celular, "*servem de chave de identificação e de acesso a um universo de plataformas eletrônicas, como bancos, supermercados, serviços públicos e redes sociais, todas elas detentoras das mais variadas informações sobre o titular*".

Nesse passo, de acordo com a orientação fixada pelo Tribunal, o regime constitucional de proteção de dados dispensaria considerações sobre a natureza ostensiva ou reservada dos dados pessoais. A rigor, os gatilhos

que acionam o direito à autodeterminação informática relacionam-se mais propriamente com o grau de sensibilidade das informações e com o risco de malversação dos dados pessoais, tornando estéril qualquer tentativa de abrandar o nível de proteção dispensado pela ordem jurídica sob o pretexto da simplicidade ou trivialidade das informações envolvidas.

No âmbito do direito positivo, entre nós, há mais de duas décadas já se ensaia a evolução do conceito de privacidade a partir da edição de legislações setoriais que garantem a proteção de dados pessoais, tais como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet – que assegura aos usuários da internet, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações e dos dados armazenados (art. 7º, II e III) – e, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Em razão da importância da LGPD para o desfecho da controvérsia, faço breves considerações sobre o alcance e a fisionomia desse diploma normativo, destacando a posição de centralidade por ele ocupada no sistema de proteção de dados brasileiro.

A Lei 13.709/2018 dispõe sobre os princípios e procedimentos para o tratamento de dados pessoais e estabelece critérios para responsabilização dos agentes por eventuais danos ocorridos em virtude dessas atividades. Conforme lecionam Valter Shuenquener e Daniel Calil, a Lei 13.709/2018 "*teve como um de seus principais propósitos incentivar a criação de um costume institucional de proteção de dados e, especialmente por meio da Autoridade Nacional de Proteção de Dados, a preocupação de garantir a efetividade no cumprimento das normas acerca da temática* (ARAÚJO, Valter Shuenquener e CALIL, Daniel Couto dos Santos. Inovações Disruptivas e a Proteção de Dados Pessoais: novos desafios para o Direito, no prelo).

Com vistas a instituir uma nova cultura de gestão de dados, a LGPD

parte da premissa básica de que a disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e à autodeterminação informativa (art. 2º, incisos I e II).

Assim, dispõe que as atividades de tratamento de dados pessoais deverão observar os seguintes princípios: (i) eleição de propósitos legítimos, específicos, explícitos e informados ao titular; (ii) compatibilidade, ou adequação, do tratamento com as finalidades informadas ao titular; (iii) limitação do tratamento ao mínimo necessário para a realização das atividades; (iv) garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; e (v) utilização de medidas técnicas de segurança aptas a proteger os dados pessoais de acessos não autorizados ou de situações ilícitas de alteração, comunicação ou difusão.

Quanto aos órgãos governamentais, a lei prevê um rol taxativo de hipóteses em que se considera legítimo o tratamento de dados por pessoas jurídicas de direito público: (i) *execução de políticas públicas* (arts. 7º e 11); e (ii) *cumprimento de atribuições institucionais*, como a execução de competências ou atribuições legais do serviço público (art. 23). A lei também exige que os agentes públicos informem *as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos* (art. 23, inciso I).

Dessa forma, percebe-se que a LGPD parece ter limitado o tratamento de dados pelo Poder Público às atividades principais e acessórias de provisão de serviços públicos. Uma interpretação dessa lei alinhada ao princípio constitucional da legalidade impõe, ainda, que essas finalidades conexas à prestação de serviços públicos estejam, ao máximo possível, amparadas em previsões legais específicas.

Essa trajetória de fortalecimento da tutela da privacidade culminou, recentemente, com a promulgação da Emenda Constitucional 115, de 10 de fevereiro de 2022, em que o poder constituinte derivado alçou a proteção de dados pessoais a uma autêntica condição de direito fundamental autônomo, insculpido no art. 5º, inciso LXXIX, da Constituição Federal.

Mas não só. As alterações promovidas pelo Congresso Nacional não apenas trasladaram essa garantia para o rol dos direitos fundamentais, como também atribuíram à União (i) competência material para organizar e fiscalizar a proteção e o tratamento de dados pessoais (art. 21, inciso XXVI); e (ii) competência privativa para legislar sobre proteção e tratamento de dados pessoais (art. 22, inciso XXX).

Examinando o assunto pela perspectiva da evolução do conceito de privacidade na jurisprudência do Supremo Tribunal Federal e pelo progressivo reconhecimento, em diversas legislações setoriais, do dever estatal de tutela de informações relacionadas ao cidadão, compreende-se que a Emenda Constitucional 115/2022 teve o mérito de consolidar, de uma vez por todas, o status constitucional inerente ao direito de proteção de dados pessoais, dirimindo quaisquer dúvidas que pudessem pairar sobre o tema.

Todo esse panorama legislativo, doutrinário e jurisprudencial fornece uma visão holística a respeito do compromisso assumido pela ordem constitucional brasileira com a proteção de dados pessoais, fornecendo parâmetros seguros para a apreciação das controvérsias que assomam ao Plenário. Assim, é sob essa ótica de afirmação da autonomia do direito fundamental à proteção de dados pessoais que serão examinadas as alegações de inconstitucionalidade deduzidas nas ações em julgamento.

2.3 Tratamento de dados pessoais pelo Poder Público: princípios constitucionais aplicáveis e rejeição ao isolamento do interesse público.

A discussão jurídica travada nas presentes ações de controle concentrado assume contornos próprios em relação ao debate promovido pela Corte na análise da ADI 6.389, de relatoria da EMINENTE MINISTRA ROSA WEBER. Isso se deve principalmente às complexidades que permeiam o tratamento de dados no âmbito interno da Administração Pública.

É inegável que as relações mantidas entre o Estado e os cidadãos comportam particularidades que desaconselham um simples translado do regime jurídico de proteção de dados aplicável às relações privadas. Isso se torna ainda mais evidente quando se percebe que, devido ao dinamismo das sociedades contemporâneas, a coleta, o processamento e o compartilhamento de informações biográficas constituem ferramentas indispensáveis para a verificação da eficácia e da adequação das políticas públicas que, em dado momento, compõem a agenda governamental.

Reconhecendo a essencialidade dos dados pessoais para prestação de serviços públicos, em um contexto em que a sociedade exige soluções efetivas e céleres, a professora Miriam Wimmer afirma que "*o tratamento de dados pessoais pelo Estado é imprescindível para o desempenho do seu mandado constitucional*". (WIMMER, Miriam. "Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público". In: DONEDA, Danilo; SARLET, Ingo Wolgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional. Rio de Janeiro, Editora Forense, 2021, pp. 271-288).

Nesse sentido, ao lembrar que as funções do Estado recebem o influxo dos postulados inerentes ao regime jurídico de Direito Público, a autora pondera que as normas protetivas concebidas para o tratamento de dados em atividades privadas não devem ser automática e irrefletidamente aplicadas no âmbito dos órgãos estatais.

Como ressalta Miriam Wimmer, seria inimaginável, por exemplo, que entendêssemos que "*qualquer cidadão teria o direito de requerer ao Poder Público a portabilidade de seus dados constantes de uma determinada base de dados governamentais, ou que alguém pudesse se dirigir a um cartório para solicitar a eliminação dos seus dados pessoais ou ainda que se pretendesse negar consentimento para que a Receita Federal processasse determinada declaração de imposto de renda*" (ibidem).

Essas questões são ainda mais sensíveis no campo da segurança pública ou no das atividades de inteligência, como se discute na ADPF 695. Não faria sentido, por exemplo, condicionar a utilização de informações pessoais por órgãos de investigação ao prévio consentimento de agentes envolvidos na prática de infrações penais. Nesses casos, tornase de fato discutível em que medida a utilidade pública envolvida no tratamento desses dados poderia impor a flexibilização das limitações previstas na legislação protetiva.

Em um contexto de rápido desenvolvimento de novas tecnologias de informação, entidades internacionais como a Organização para a Cooperação e Desenvolvimento (OCDE) têm reconhecido que a modernização da Administração Pública, mediante a instituição de um modelo de *Data Driven Public Sector*, constitui importante passo na direção da concretização de direitos sociais (OCDE. The Path to Becoming a Data-Driven Public Sector. OECD Publishing: Paris, 2019).

É assente na literatura estrangeira o reconhecimento de que países comprometidos com uma agenda de um governo digital podem aprimorar os resultados de gestão utilizando novas tecnologias de forma responsiva, protetiva e transparente. Nesse aspecto, o tratamento de dados torna-se importantíssima ferramenta para o desenho, implementação e monitoramento de políticas e de serviços públicos essenciais.

Nos últimos anos, o Governo brasileiro tem buscado seguir essa

agenda de digitalização da Administração Pública. Conforme será discutido adiante no presente voto, esse movimento tem sido buscado na edição de atos normativos, como o que institui o chamado Cadastro Base do Cidadão, e em programas como a Estratégia Brasileira para a Transformação Digital (e-Digital).

Dentro desse contexto, não há dúvidas de que relevantes postulados constitucionais estão em jogo quando se discutem os limites do tratamento de dados pelo Poder Público, a exemplo do princípio da eficiência da Administração Pública (art. 37, CF). Conforme destacado pela União, em sua manifestação nos autos, o compartilhamento efetivo de dados entre os órgãos e entidades da Administração Federal é, sem dúvida, pressuposto de uma gestão pública eficiente.

Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais.

Como bem destacado por Gillian Black e Leslie Stevens, pesquisadores britânicos dedicados a essa temática, "*se a privacidade for tratada simplesmente como um direito ou interesse individual, sempre será possível para o setor público controlar dados para suas finalidades públicas, já que isso será sempre reputado como necessário e proporcional*" (tradução livre) (BLACK, Gillian e STEVENS, Leslie. "Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest". In: Scripted. Vol. 10, n. 1, 2013, p. 95).

Nesse sentido, assentam os autores a necessidade de se conferir uma abordagem comunitária e institucional ao direito à proteção de dados pessoais, evitando-se que este valor sempre sucumba diante da invocação do interesse público.

A consciência de que os governos devem tratar o regime jurídico de privacidade como um objetivo coletivo de estruturação dos regimes democráticos, e não como um valor contraposto de proteção de interesses individuais, é corolário do próprio reconhecimento da autonomia do direito fundamental à proteção de dados pessoais.

Como destaca Daniel Solove: "*a privacidade não é algo que indivíduos automatizados possuem no estado de natureza e que sacrificam para se unir ao pacto social. Estabelecemos proteções à privacidade por causa de seus profundos efeitos sobre a estrutura de poder e de liberdade na sociedade como um todo*" (SOLOVE, Daniel. J. Understanding Privacy. Cambrigde: Harvard University Press, 2008, p. 93). Desse modo, assenta o autor, "*a proteção da privacidade nos protege contra prejuízos a atividades que são importantes tanto para os indivíduos quanto para a sociedade*" (Idem).

É justamente por isso que instituições como a própria OCDE têm defendido que a confiança da sociedade e a garantia de parâmetros éticos no tratamento de dados pela Administração Pública são elementares para uma boa governança dos governos digitais.

Como ressaltado pela OCDE, diversos países passaram recentemente a adotar critérios formais, definidos em legislação própria, para proteger os cidadãos no processo de coleta, armazenamento, compartilhamento e processamento de dados pelos órgãos do Estado. Em patamares de proteção mais elevados, a OCDE observa que as limitações normativas devem visar a garantir que o cidadão tenha o controle sobre: (i) quais dados as organizações governamentais têm sobre eles, (ii) quais organizações públicas têm o direito de acesso a seus dados, (iii) quais organismos públicos fizeram uso de seus dados e para que fins, (iv) que organizações públicas fizeram um inquérito sobre seus dados e (v) o direito de concordar ou recusar permissão para que os dados que fornecem a uma instituição pública sejam compartilhados e reutilizados por outras (tradução

livre) (OCDE. The Path to Becoming a Data-Driven Public Sector. OECD Publishing: Paris, 2019, p. 113).

Os parâmetros apontados pela OCDE parecem estar sendo constantemente perseguidos pelas nações democráticas estrangeiras. De fato, colhe-se da experiência internacional diversos modelos institucionais voltados à garantia desse patamar ético.

Uma das opções consiste na criação de entidade independente vocacionada a apoiar as entidades governamentais no gerenciamento dos dados que elas possuem sobre os cidadãos, facilitando o acesso e o compartilhamento de informações a partir de *standards* e metodologias definidos. Essa experiência tem sido concretizada em países como Irlanda, Portugal, Canadá e Nova Zelândia. Na Nova Zelândia, a propósito, o Governo instituiu um Grupo de Aconselhamento Ético para o tratamento de dados pessoais.

Outro caminho que tem sido explorado pelas nações democráticas é o estabelecimento de guias vinculantes em relação ao próprio Estado, limitando o processamento dos dados dos cidadãos. No Reino Unido, por exemplo, observa-se que as disposições da Lei Nacional de Proteção de Dados (*Data Protection Act*) são concretizadas, em múltiplos níveis, com guias e documentos orientativos, como o *Digital Economy Act*, que determina que cada Ministro expeça um código de conduta para compartilhamento de informações no âmbito de suas atribuições; e o *Data Ethics Framework*, que traz orientações bastante pragmáticas para serem utilizadas no dia a dia dos servidores públicos.

Trazendo essas considerações para a esfera local, conclui-se que compete ao Poder Público a delicada missão de delimitar adequado âmbito de proteção do direito à autodeterminação informativa, harmonizando os objetivos do Estado com os interesses legítimos dos titulares dos dados pessoais. Sobre esse ponto, destaca-se mais uma vez o escólio de Miriam Wimmer:

> "A aplicação da legislação de proteção de dados no tratamento de dados pelo Poder Público – tanto no caso de atos individuais e concretos como também na edição de atos normativos – traz, portanto, o desafio de conciliação entre os princípios tradicionalmente aplicáveis à Administração Pública e aqueles contidos na própria LGPD, sem que se determine a precedência *prima facie* de um interesse público abstratamente caracterizado e reconhecendo também a importância da proteção de dados pessoais para além da sua dimensão individual. A eficiência demandada da Administração Pública e o interesse público tutelado pelo Estado devem, portanto, ser compreendidos no contexto de um conjunto mais amplo de princípios e com elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais". (WIMMER, Miriam. "Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público". In: DONEDA, Danilo; SARLET, Ingo Wolgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional. Rio de Janeiro, Editora Forense, 2021, pp. 271288).

Convém destacar que essa visão de compatibilização dos interesses da Administração Pública com a defesa de garantias individuais na temática da proteção de dados pessoais não é de todo estranha à jurisprudência do STF. Em pelo menos duas ocasiões, o Tribunal impôs limitações a um modelo de fluxo multidirecional e irrestrito de compartilhamento de dados entre instituições públicas.

Nesse sentido, rememoro decisão proferida pela EMINENTE MINISTRA CÁRMEN LÚCIA na Suspensão de Liminar 1.103 MC, na qual determinou que o IBGE se abstivesse de fornecer ao Ministério Público Federal dados reputados necessários à identificação de 45 (quarenta e cinco) crianças domiciliadas no município de Bauru/SP, que, de acordo com o Censo realizado em 2010, não teriam sido regularmente registradas nos Cartórios de Registro Civil de Pessoas Naturais. Nessa decisão, a então Presidente do Supremo Tribunal Federal afirmou a necessidade de conciliação dos valores constitucionais em jogo ao pontuar:

> "O dever de sigilo proporciona segurança a quem presta as informações e contribui para a confiabilidade das pesquisas efetuadas. Recepção das normas que estabelecem o sigilo das informações colhidas pelo IBGE (art. 2º, § 2º, do Decreto-lei n. 1.611/1967 e parágrafo único, do art. 1º, da Lei no 5.534/1968) pela Constituição Federal de 1988. IV. Quando princípios fundamentais da Constituição conflitam entre si, a questão deve ser analisada tendo em vista o caso concreto, respeitados os valores supremos consagrados na ordem constitucional. Com base no juízo de ponderação, busca-se identificar em qual dimensão deve um direito fundamental preponderar quando contraposto a outro direito também fundamental. Para isso, deve-se recorrer aos princípios instrumentais da razoabilidade e da proporcionalidade, implícitos na Constituição, e sopesar os valores protegidos pelas normas em conflito. Não se trata de eliminar um direito para fazer predominar exclusivamente outro, mas sim de conciliar os bens jurídicos em conflito e harmonizá-los com os princípios consagrados no sistema jurídico constitucional". (SL 1.103 MC, Rel. Min. Cármen Lúcia, julgado em 5.2.2017, DJe 8.5.2017).

No mesmo sentido, destaco decisão proferida pelo EMINENTE MINISTRO LUÍS ROBERTO BARROSO nos autos do Mandado de Segurança 36.150 MC, na qual cassou determinação do Tribunal de Contas da União (TCU) que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM, com o fim de realizar auditoria do Programa Bolsa Família.

Nessa importante decisão, o eminente relator dialogou profundamente com a noção de finalidade aqui discutida, apontando risco de subversão da autorização concedida pelos titulares dos dados pessoais no ato de coleta. Destaco trecho da referida decisão:

> "7. É certo que o art. 71, IV, da Constituição confiou ao TCU a competência para a realização de inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial nos órgãos e entidades da Administração. A atribuição dessa competência, por óbvio, supõe o reconhecimento dos meios necessários ao cumprimento desse encargo. Isso inclui a prerrogativa de requerer aos responsáveis pelos órgãos e

> entidades as informações necessárias à instrução de processos de auditoria e inspeção. No caso, no entanto, as informações que se quer acessar foram prestadas para uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo do INEP quanto às informações pessoais. 8. Nesse aspecto, a transmissão a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade. De igual modo, é plausível a alegação de que a franquia desses dados quebra a confiança no órgão responsável pela pesquisa por violação do sigilo estatístico. Há, pois, risco à própria continuidade das atividades desempenhadas pelo INEP, com efetivo prejuízo ao monitoramento das políticas públicas de educação". (MS 36.150 MC, Rel. Min. Roberto Barroso, julgado em 10.12.2018, DJe 13.12.2018).

Assim, é clara a necessidade de temperar os valores constitucionais da eficiência da Administração Pública com o regime constitucional de tutela dos direitos individuais, particularmente as garantias de autodeterminação informativa e de proteção dos dados pessoais (art. 5º, caput e incisos X, XII e LXXIX, da Constituição Federal).

2.4 Objeto da ADPF 695. Compartilhamento de dados pessoais para realização de atividades de inteligência

Considero apropriado iniciar pelo exame do ato de compartilhamento impugnado na Arguição de Descumprimento de Preceito Fundamental 695. Assim o faço porque as distorções e irregularidades identificadas da ação administrativa impugnada na ADPF auxiliam na constatação do quadro geral de insegurança que deriva do regulamento editado pelo Poder Executivo, o Decreto 10.046/2019.

Na ADPF 695, o Partido Socialista Brasileiro (PSB) requer seja sanada grave lesão a preceitos fundamentais, consistente no "*compartilhamento de dados pessoais (...) pelo Serviço Federal de Processamento de Dados (SERPRO) à Agência Brasileira de Inteligência*

(ABIN), com suposto lastro normativo no Decreto 10.046, de 9 de outubro de 2019". Sustenta, em síntese, que a "*transferência massiva e indiscriminada dos dados pessoais de todos os portadores de CNH no país para a Agência Brasileira de Inteligência*" viola os direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa.

Atento ao risco de violação massiva à proteção de dados pessoais de 76 milhões de brasileiros, requeri, no dia 22.6.2020, a apresentação da ADPF 695 em mesa para apreciação do pedido de concessão da medida cautelar. Em homenagem ao princípio da colegialidade, pretendi submeter a controvérsia ao crivo do Tribunal Pleno, visando promover um debate plural acerca da compatibilidade do ato do Poder Público com o regime constitucional de proteção de dados pessoais.

Ocorre que, no dia 23.6.2020, às vésperas da sessão de julgamento, a AGU peticionou nos autos informando a revogação do Termo de Autorização que concedera o acesso da ABIN à base de dados da Carteira Nacional de Habilitação. Requereu, então, fosse declarada a perda de objeto da ADPF.

A partir dessa provocação, os autos retornaram ao meu gabinete, ocasião em que ponderei que, sem embargo da revogação do termo de autorização, o ato do Poder Público impugnado nesta ADPF abrangia todo um quadro de insegurança jurídica gerado por leituras distorcidas do Decreto 10.046/2019. Por esse motivo, reconheci que persistia interesse processual quanto ao pedido de interpretação conforme do regulamento administrativo.

Assim, proferi decisão no dia 24 de junho de 2020, reconhecendo que, não fosse o abandono do intento de transferência massiva e indiscriminada de dados pessoais para a Agência Brasileira de Inteligência, a União enfrentaria grandes dificuldades para sustentar a constitucionalidade da medida perante o Supremo Tribunal Federal. Nessa senda,

apontei que a redação genérica do ato impugnado erigia obstáculos intransponíveis ao exercício do controle judicial, sobretudo por não indicar as finalidades pretendidas pelo órgão solicitante nem a real necessidade de utilização de informações de 76 milhões de brasileiros em atividades de inteligência. Eis o que assentei na ocasião:

> No caso em tela, há uma enorme dificuldade em proceder ao teste de proporcionalidade em todas as suas etapas. Como dito, o único ato material submetido a um mínimo de publicidade consiste no Termo de Autorização 7/2020 e no extrato do mencionado Termo de Autorização, publicados no Diário Oficial da União – DOU 46, Seção 3, de 9 de março de 2020.
>
> Embora a União afirme que este Termo de Autorização "foi emitido de modo completamente transparente, em veículo da imprensa oficial, segundo o procedimento aplicado às solicitações de mesma natureza", não é possível colher do extrato publicado no Diário Oficial da União qualquer informação relevante sobre a natureza dos dados compartilhados tampouco acerca dos parâmetros objeto do compartilhamento.
>
> Ressalte-se que, por disposição expressa do art. 5º do Decreto 10.046/2019, "fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos".
>
> Assim, dificilmente os órgãos envolvidos no compartilhamento tornariam público no futuro os termos em que o compartilhamento ocorreria.
>
> [...]
>
> Assim, do ponto de vista da adequação, seria bastante difícil examinar o ato em questão, já que a única face pública da medida impugnada adota redação genérica para indicar os objetivos do compartilhamento de dados e nem sequer explicita a finalidade pretendida com as atividades de inteligência.
>
> Já sob o prisma da necessidade, diante da ausência de explanação da finalidade do compartilhamento, torna-se impossível aferir se o compartilhamento na dimensão apresentada se revela o meio menos intrusivo possível para alcançar o objetivo apresentado. Aqui talvez seja o elemento

> em que recai o maior ônus da Administração Pública: explicar por que afinal seria necessário o processamento de dados da CNH de 76 milhões de brasileiros para atividades de inteligência.
>
> Por fim, ainda que fosse possível avançar no juízo da proporcionalidade em sentido estrito, dificilmente seria possível compatibilizar uma violação massiva à proteção de dados pessoais, traduzida no compartilhamento irrestrito de dados da CNH de mais de 76 milhões de brasileiros, com alguma finalidade legítima de tratamento de dados para atividades de vigilância.
>
> Por todos esses motivos, entendo que, no caso concreto, há significativa e densa verossimilhança nas alegações do autor, no sentido de que o ato do Poder Público trazido a exame por esta Suprema Corte (i) tem o potencial de violar os preceitos fundamentais da proteção da privacidade, da proteção de dados e da autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X e XII, da CF/88); (ii) não possui base normativa que eventualmente lhe ampare – o que poderia em tese lhe emprestar legitimidade; e (iii) tampouco mostra-se proporcional ante as suas finalidades.

Essas considerações são necessárias para demonstrar que, a despeito do abandono dos propósitos inicialmente almejados pela ABIN, ainda persistem graves riscos para a tutela da privacidade e da autodeterminação informativa.

O tema de fundo da ADPF conduz à inescapável percepção da insegurança gerada pela abertura semântica do Decreto 10.046/2019, que, não raras vezes, tem desaguado em leituras desviantes e extremamente alargadas do seu programa normativo, com manifestos prejuízos para o regime constitucional de proteção de dados pessoais.

Sem maiores digressões, apenas para mencionar o caso específico tratado na ADPF, causa perplexidade que, na defesa apresentada nos autos, a União sustente que o compartilhamento pretendido pela ABIN encontra suporte normativo no inciso I do art. 3º do Decreto 10.046/2019, cujo teor assim dispõe:

> Art. 3º – O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> I – a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais.

Tal linha de pensamento, entretanto, me parece em frontal choque com os lineamentos mais basilares do postulado do Estado Democrático de Direito; confronta, outrossim, com os limites que decorrem do texto constitucional para o tratamento de dados pessoais (bem como da legislação ordinária veiculada pelo Congresso Nacional, no exercício de sua competência para atuar nesse âmbito facultado).

São duas as razões que me conduzem a essa conclusão. A primeira diz respeito à necessidade de promover uma leitura do regulamento administrativo alinhada com o regime constitucional de tutela da privacidade. Trata-se de assunto que será devidamente aprofundado ao longo do presente voto, cabendo, contudo, desde já registrar que o sentido do Decreto 10.046/2019 que melhor traduz os objetivos da ordem constitucional conduz ao abandono de qualquer interpretação que possibilite um amplo e irrestrito compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública Federal.

Assim, sem me antecipar em relação ao aprofundamento do tema, registro que, em homenagem ao direito à autodeterminação informativa, apenas as informações gerais do Estado são alcançadas pelo disposto no art. 3, inciso I, do Decreto 10.046/2019, e não aquelas relacionadas aos atributos da personalidade ou qualidades próprias do cidadão.

Devem ser amplamente compartilhadas, nos termos do dispositivo, somente as informações relativas ao funcionamento do aparato estatal, como gestão de pessoal e do patrimônio público, utilização de recursos orçamentários, formalização de atos e contratos administrativos, apenas

para citar alguns exemplos. Lado outro, em relação às informações pessoais, devem incidir os vetores protetivos da LGPD, estruturados para a salvaguarda da privacidade dos cidadãos, que exigem o preenchimento de requisitos mais rígidos para o fluxo de informações no âmbito dos órgãos públicos federais.

A segunda razão para rejeitar a tese deduzida pela União diz respeito à impossibilidade de invocação dos dispositivos do Decreto 10.046/2019 e da Lei 13.709/2018 para legitimar operações de tratamento de dados no âmbito do Sistema Brasileiro de Inteligência. Afinal, basta um simples lançar de olhos sobre o art. 4º, inciso III, da Lei 13.709/2018 para concluir que o compartilhamento de dados pessoais para fins de defesa nacional "*será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei*".

Ao que tudo indica, considerando a sensibilidade das atividades relacionadas à preservação da soberania nacional, o legislador entendeu que o assunto deveria observar legislação específica, adequada às particularidades desse campo de atuação estatal. Antecipou, contudo, que esse regime especial de tratamento de dados deve ser calibrado à luz dos pilares estruturantes da LGPD, especialmente no que diz respeito à necessidade de apresentação de justificação minudente das finalidades pretendidas pelos órgãos de inteligência.

Esse tema foi exaustivamente debatido na ADI 6.529, de relatoria da EMINENTE MINISTRA CÁRMEN LÚCIA, DJe de 22.10.2021, em que esta Corte assentou que, desde que observados os requisitos legais, é legítimo o compartilhamento de conhecimentos específicos com a Agência Brasileira de Inteligência, na forma do parágrafo único do art. 4º da Lei 9.883/1999.

Na ocasião, o Tribunal conheceu parcialmente da ação para conferir

interpretação conforme ao mencionado dispositivo, estabelecendo que (a) o compartilhamento de dados no âmbito do Sistema Brasileiro de Inteligência somente pode ocorrer quando demonstrado o interesse público da medida; (b) toda e qualquer decisão de fornecimento de dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal; e d) são indispensáveis a instauração de procedimento administrativo formal e a utilização de sistemas eletrônicos de segurança e registro de acesso, para efeito de responsabilização em caso de abuso.

Desse panorama, extraem-se duas importantes conclusões. Primeiro, ao contrário do afirmado pela União, as disposições da LGPD e do respectivo decreto regulamentador não constituem, per se, suporte legal para o compartilhamento de dados pessoais no âmbito do Sistema Brasileiro de Inteligência. Em segundo lugar, embora seja possível o compartilhamento de conhecimentos específicos com a ABIN, isso não afasta necessidade de se examinar, sob a perspectiva constitucional, se as restrições impostas pelo ato administrativo estão devidamente motivadas e se atendem, ou não, às balizas fixadas no julgamento da ADI 6.529, de relatoria da EMINENTE MINISTRA CÁRMEN LÚCIA.

Feitas essas considerações, entendo que, sem embargo da revogação do Termo de Autorização 07/2020, o grave quadro de insegurança jurídica causado pela elasticidade semântica do Decreto 10.046/2019 evidencia a necessidade de realizar o julgamento da ADPF 695 em conjunto com a ADI 6.649.

Cuida-se de rica oportunidade para o Tribunal avaliar, em perspectiva global, se o sentido atribuído pela Administração Pública ao referido decreto regulamentar se compatibiliza, ou não, com a ordem constitucional brasileira.

2.5 Confronto do programa normativo do Decreto 10.046/2019 com a Constituição Federal

A controvérsia abordada na Ação Direta de Inconstitucionalidade 6.649/DF diz respeito, essencialmente, à validade dos dispositivos do Decreto 10.046, de 9 de outubro de 2019, que *dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados*.

O regulamento impugnado desempenha a delicada missão de sistematizar regras e princípios aplicáveis ao compartilhamento de dados entre órgãos públicos federais, em uma tentativa de fundar balizas para aplicação harmônica dos dispositivos da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e da Lei de Acesso à Informação (Lei 12.527/2011). A complexidade do assunto é evidenciada pela existência de conflitos aparentes entre normas que impõem transparência absoluta na condução dos negócios públicos, de um lado, e aquelas que estabelecem limites rigorosos para o fluxo de dados pessoais coletados ou produzidos pelo Estado, de outro.

Se é certo que informações gerais relacionadas à atividade administrativa devem, em regra, se submeter ao princípio da ampla publicidade, não é menos exato que o tratamento de dados pessoais segue lógica diversa, focada na salvaguarda da privacidade dos cidadãos. Essa distinção impõe regime jurídico híbrido para o tratamento das informações coletadas ou produzidas pela Administração Pública, a depender do maior ou menor vínculo que elas guardem com atributos da personalidade ou qualidades próprias do cidadão.

Não há, evidentemente, como ombrear o regime jurídico restritivo que orienta o tratamento de dados pessoais, fundado em vetores protetivos, com as regras e princípios que se aplicam ao manuseio de informações relacionadas ao próprio funcionamento do aparato estatal, como

despesas administrativas, atos de gestão do patrimônio público, licitações, contratos administrativos, pareceres e decisões administrativas, apenas para citar alguns exemplos.

Dadas a complexidade da matéria e as incertezas e aflições que fatalmente incidiriam sobre os agentes responsáveis pela aplicação da lei, impunha-se a construção de balizas interpretativas que fossem capazes de acomodar, em um mesmo programa normativo, o dever geral de publicidade dos negócios públicos e o regime constitucional de proteção de dados pessoais.

Nesse contexto, surge o Decreto 10.046/2019 como uma tentativa de orientar a atuação dos servidores públicos responsáveis pela governança de dados na Administração Pública Federal, sobretudo no que se refere à interoperabilidade e integração dos bancos de dados mantidos pelos diferentes órgãos e entidades que a compõem.

O regulamento impugnado pode ser decomposto em quatro eixos normativos. O primeiro deles, contido nos arts. 1º a 3º, arrola os objetivos que devem orientar o compartilhamento de dados na Administração Pública Federal, com destaque para a simplificação da oferta de serviços públicos, a avaliação e o monitoramento constante da eficiência das políticas públicas e a melhoria da qualidade e integridade dos dados custodiados pelos órgãos federais. Adicionalmente, ao dispor sobre as diretrizes que devem ser observadas nessas operações, o decreto impõe o compartilhamento da informação do Estado da forma mais ampla possível, ao mesmo tempo que assegura a observância da Lei Geral de Proteção de Dados (art. 1º, inciso I).

Outro eixo, delineado nos arts. 4º a 14, estabelece três níveis de compartilhamento de informações, quais sejam: (i) compartilhamento amplo, quando se tratar de dados públicos que não estejam sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser ampla e garantida a qualquer interessado (art. 4º, inciso I); (ii) compartilhamento restrito,

para dados sigilosos que, pela sua natureza, possam ser acessados por todos os órgãos e entidades da Administração Pública Federal (art. 4º, inciso II); e (iii) compartilhamento específico, quando se tratar de dados protegidos por sigilo que, pelo grau de sensibilidade, somente podem ser repassados a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei (art. 4º, inciso III).

O terceiro eixo, contido nos arts. 16 a 20, institui o Cadastro Base do Cidadão, mecanismo de interoperabilidade voltado ao aprimoramento da gestão de políticas públicas e ao aumento da confiabilidade dos cadastros existentes. Cuida-se de repositório unificado que funcionará conforme a política de governança aprovada pelo Comitê Central de Governança de Dados e que será composto, inicialmente, pelas informações biográficas que constam da base temática do CPF.

Por fim, o quarto eixo, delineado nos arts. 21 e seguintes, prevê a estrutura e a forma de funcionamento do Comitê Central de Governança de Dados, a quem compete fixar orientações e diretrizes para a categorização do compartilhamento amplo, restrito e específico; e, ainda, dispor sobre a arquitetura, os requisitos de acesso e a política de segurança do Cadastro Base do Cidadão.

Pois bem. Alega o requerente que, a pretexto de regulamentar diplomas normativos diversos, o regulamento administrativo: a) invadiu competência privativa do Congresso Nacional e exorbitou o poder regulamentar conferido ao Presidente da República; b) dispôs sobre a matéria de forma contrária aos preceitos constitucionais e infraconstitucionais relacionados à proteção de dados e da privacidade; e c) instituiu um cadastro unificado que poderá ser utilizado abusivamente pelos órgãos do poder público federal, além de acarretar riscos de vazamentos e incidentes de segurança.

Embora a Ação Direta tenha como propósito a declaração de inconstitucionalidade da íntegra do Decreto 10.046, de 9 de outubro de 2019, o

raciocínio articulado na petição inicial revela que o desconforto do requerente reside principalmente na disciplina dos níveis de compartilhamento de dados pessoais, na instituição do Cadastro Base do Cidadão e no delineamento do Comitê Central de Governança de Dados. Há receio de que o texto do regulamento possa dar margem a um fluxo desordenado de dados pessoais no âmbito do Poder Executivo, em desacordo com as disposições da LGPD.

Surge, em boa hora, uma alvissareira oportunidade para que o Tribunal, no contexto do compartilhamento de dados entre órgãos e entidades integrantes da Administração Pública, reflita não apenas sobre as salvaguardas institucionais que devem acompanhar o tratamento de dados por órgãos governamentais, como também sobre os limites do poder regulamentar em matéria de privacidade e proteção de dados.

Pois bem. A despeito da complexidade ímpar da matéria, penso que, *a priori*, assiste ao Presidente da República competência para produzir os parâmetros de uniformização necessários à execução da Lei Geral de Proteção de Dados Pessoais pelos órgãos e entidades federais.

A rigor, em se tratando de leis que são objeto de ação administrativa, a expedição de regulamentos constitui providência essencial para o bom funcionamento da estrutura orgânica da Administração Pública Federal. Por meio deles, o Presidente da República não apenas fixa critérios uniformes para a aplicação da legislação pelos órgãos integrantes do aparelho estatal, como também afasta dúvidas e dificuldades que poderiam comprometer a operatividade da lei.

Não por outra razão, doutrinadores de renome preferem substituir a expressão *poder regulamentar* por *dever regulamentar*, que melhor enfatiza a responsabilidade do Chefe do Poder Executivo de instituir normas secundárias necessárias para a fiel execução da lei, impedindo o surgimento de incertezas que possam implicar paralisia administrativa. A esse respeito, a professora Maria Sylvia Zanella Di Pietro alerta que,

"embora o vocábulo poder dê a impressão de que se trata de faculdade da Administração, na realidade trata-se de poder-dever, já que reconhecido ao poder público para que o exerça em benefício da coletividade; os poderes são, pois, irrenunciáveis". (Manual de Direito Administrativo. 14ª ed. São Paulo: Atlas, 2018, p. 115)

No que diz respeito ao tratamento de dados pelo poder público, verifica-se que diversos dispositivos da Lei 13.709/18 pressupõem vigorosa atuação de órgãos administrativos para execução do que neles se dispõe. O legislador, no entanto, dada a generalidade e o caráter abstrato da lei, não foi capaz de dispor sobre todos os aspectos da política legislativa de proteção de dados pessoais, em especial no que concerne à administração das informações biográficas coletadas pelo Estado. Subsiste, então, a necessidade de expedição de normas secundárias para orientar os agentes públicos sobre como proceder diante dessa delicada tarefa.

Deparamo-nos, portanto, com exemplo típico de programa normativo cuja operatividade depende de ulterior regulamentação pelo Chefe do Poder Executivo, por meio da fixação dos parâmetros necessários para aplicação consistente e uniforme da lei. No caso da LGPD, são muitas as normas que impõem ações concretas do Estado em matéria de gestão de dados pessoais e, nessa medida, reclamam a edição de atos complementares para densificação dos princípios gerais por ela estabelecidos.

Destaco, pela pertinência com a demanda, os dispositivos que determinam a manutenção de bases temáticas em plataformas integradas, estruturadas para uso compartilhado; e os que orientam os gestores públicos a desenvolverem mecanismos eletrônicos de interoperabilidade, com a finalidade de aumentar a confiabilidade dos cadastros administrativos, aprimorar a gestão de políticas públicas e permitir a atuação articulada dos órgãos estatais na prestação de serviços públicos.

É o que dispõem os arts. 25 e 26 da Lei Geral de Proteção de Dados Pessoais:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público geral.
>
> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

No mesmo sentido, destaco que a moderna Lei 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital, prevê como um dos seus princípios a "*atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle de serviços públicos, com o compartilhamento de dados pessoais em ambiente seguro quando for indispensável para a prestação do serviço, nos termos da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) [...]*".

Mais adiante, a Lei do Governo Digital assim estabelece:

> Art. 39. Será instituído mecanismo de interoperabilidade com a finalidade de:
>
> I - aprimorar a gestão de políticas públicas;
>
> II - aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública, por meio de mecanismos de manutenção da integridade e da segurança da informação no tratamento das bases de dados, tornando-as devidamente qualificadas e consistentes;
>
> III - viabilizar a criação de meios unificados de identificação do cidadão para a prestação de serviços públicos;
>
> IV - facilitar a interoperabilidade de dados entre os órgãos de governo;
>
> V - realizar o tratamento de informações das bases de dados a partir do número de inscrição do cidadão no CPF, conforme previsto no art. 11 da Lei nº 13.444, de 11 de maio de 2017.

> Parágrafo único. Aplicam-se aos dados pessoais tratados por meio de mecanismos de interoperabilidade as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

Nossa legislação federal, portanto, contempla um plexo de disposições normativas que impõem à Administração Pública a difícil tarefa de implementar bancos de dados de natureza interoperável, desenvolvidos para permitir o compartilhamento eletrônico de informações entre órgãos governamentais, sem prejuízo da irrestrita observância dos princípios gerais e mecanismos de proteção elencados na Lei Geral de Proteção de Dados Pessoais.

Há um outro aspecto fundamental que não pode ser olvidado pela Corte. Mesmo que ausentes os referidos comandos legais, é certo que a Constituição Federal impõe ao Estado o dever de desenvolver a atividade administrativa do modo mais eficiente, mais econômico e mais adequado ao interesse público. Naturalmente, o cumprimento da determinação constitucional pressupõe emprego das mais modernas tecnologias e soluções computacionais, sobretudo em um contexto de amplo desenvolvimento de ferramentas digitais, de modernas aplicações de informática e de computação em nuvem (*cloud computing*).

É impensável que, na sociedade moderna, as repartições públicas operem com instrumentos defasados, renunciando à tecnologia, às ferramentas digitais, e desprezando as melhores práticas gerenciais. Ou seja, não é dado ao Estado virar as costas para o progresso tecnológico, tampouco permanecer amarrado ao passado. Cuida-se de mais cristalina aplicação do princípio da eficiência administrativa, ou daquilo que os italianos chamam de *princípio da boa administração*. (CLARICH, Marcello. Manuale di Diritto Amministrativo. 5ª ed. Bolonha: il Mulino, 2022, pp. 152-153)

Isso não quer dizer que o dever de eficiência sirva de manobra para o descumprimento do princípio da legalidade nem que constitua um che-

que em branco para o administrador público. Revela, apenas, a assunção de um compromisso de eficiência e busca dos melhores resultados pelo Estado brasileiro, o que de modo algum representa uma licença para o desatendimento dos preceitos éticos que informam o regime constitucional, entre eles os mecanismos de proteção de dados pessoais.

São diversos os exemplos de emprego de ferramentas tecnológicas no interesse do cidadão e da eficiente prestação de serviços públicos. Apenas para citar um caso, destaco portaria recente do Ministro do Trabalho e Previdência que, em benefício de idosos ou de pessoas com deficiência, dispensa segurados do INSS ou beneficiários do Benefício de Prestação Continuada (BPC) de comparecerem presencialmente às agências do INSS ou agências bancárias para realização da assim chamada *prova de vida* (Portaria MTP 220, de 2 de fevereiro de 2022).

A partir de agora, a Administração Pública se valerá de mecanismos menos intrusivos, como o compartilhamento de dados, para evitar pagamentos indevidos a pessoas falecidas e combater fraudes no âmbito da seguridade social. Por meio de integração de bases de dados, informações que já se encontram em posse de órgãos públicos federais serão utilizadas para dispensar a *prova de vida*. Basta que o cidadão tenha sacado dinheiro em agências bancárias, solicitado renovação de carteira de identidade ou habilitação, passaporte ou registro de votação, para que seja considerado vivo. Deparamo-nos, aqui, com exemplo real de legítima utilização do compartilhamento de dados em benefício do cidadão.

A propósito, registro que as informações prestadas pela Presidência da República demonstram, em geral, os propósitos que orientaram a edição do Decreto 10.046/2019 e, no particular, a preocupação do Poder Executivo com a preservação da privacidade dos titulares de dados pessoais. Destaco:

> "O Decreto n. 10.046/2019 permite a gestão e o uso de dados já gerados nos sistemas da Administração Pública Federal de forma a garantir qua-

lidade da informação, com o uso da tecnologia para promover eficiência nos processos, bem com garantir a segurança da informação através de critérios previstos pelo próprio Decreto e com base na Lei Geral de Proteção de Dados – LGPD (vide artigo 5º do Decreto n.º 10.046/2019).

[...] Trata-se de um mecanismo essencial para a autenticação digital, que reduz a ocorrência de falsificação ideológica e duplicação de identificação, o que evidentemente evita fraudes e estelionatos. Além disso, traz maior confiabilidade em operações, inclusive transações financeiras, simplifica e automatiza procedimentos de prova de vida, identificação, reduzindo custos e riscos no fornecimento de serviços públicos. Outros benefícios dos dados biométricos são a desduplicação de cadastros do governo, trazendo qualidade e unicidade dos dados. Todas essas medidas devem ser pautadas em tecnologia de segurança da informação, a fim de garantir a eficiência na execução de serviços públicos.

[...]

Tendo em vista a pluralidade de bases de dados já custodiadas pelo Estado, é crucial a interoperabilidade entre elas para fins, dentre outros, de cruzamento dos dados nela existentes. Frequentemente, tais dados se referem à mesma pessoa física ou jurídica, mas revelam informações contraditórias. Com isso, é inviabilizado o acesso a serviços públicos a cidadãos que fariam jus a benefícios. Analogamente, essa inconsistência poderia implicar a concessão de acesso a pessoas que, por sua vez, não estariam legalmente habilitadas. A inconsistência entre bases de dados tem tais efeitos práticos, em detrimento da celeridade e da correta prestação de bens e serviços públicos. Essas inconsistências nas bases de dados foram amplamente analisadas por recentes acórdãos do Tribunal de Contas da União. Destacam-se, nesse sentido, o Acórdão n.º 1.706/2020, que analisou o compartilhamento de dados para validação do pagamento do auxílio emergencial, e o Acórdão n.º 1.123/2020, que analisou divergências entre diversas bases de dados do governo federal.

Essas incongruências nas concessões de serviços públicos geram distorções que afrontam o princípio da isonomia de tratamento, que deve nortear as ações públicas. Em um cenário ainda mais negativo, essas inconsistências podem causar prejuízo ao erário: a concessão de benefício, por exemplo, a quem não está apto a recebê-lo gera, muitas das vezes, a

não concessão desse mesmo benefício a quem o detém de direito – em um contexto de limitações orçamentárias e financeiras de recursos públicos federais".

Não há como negar que o texto da norma impugnada é fiel aos propósitos elencados nas informações prestadas pela Presidência da República. A moldura semântica do decreto presidencial revela compromisso do Estado brasileiro com adoção de ferramentas tecnológicas capazes de aprimorar a prestação de serviços públicos e aumentar a eficiência da atividade administrativa, ao mesmo tempo que prestigia as normas e princípios previstos na Lei Geral de Proteção de Dados Pessoais.

Longe de indicar um preciosismo redacional, as inúmeras remissões que são feitas às regras e princípios instituídos pela LGPD são cruciais para o desfecho da presente controvérsia. São elas que me conduzem à certeza de que as disposições do decreto presidencial não contêm nenhuma permissão expressa para compartilhamento de dados pessoais de maneira ampla e irrefletida, fora do eixo de proteção instituído pela Lei 13.709/2018.

E isso por um simples motivo. Em razão do constante diálogo que o decreto presidencial promove com as normas protetivas de dados pessoais, seu programa normativo, quando interpretado com razoabilidade, sinaliza para um duplo padrão de tratamento das informações custodiadas em poder da Administração Pública.

De um lado, para as informações gerais do Estado, vigora regime mais flexível e maleável, focado no acesso à informação e no controle social da atuação estatal. E, de outro, no que diz respeito aos dados pessoais, prevalece regime mais rigoroso, voltado fundamentalmente para a proteção do indivíduo em face do risco de malversação de seus atributos biográficos.

Quanto às primeiras, o decreto contempla previsões genéricas, fundadas na Lei 12.527/2011 (Lei de Acesso à Informação), no sentido de im-

por (a) ampla divulgação, preferencialmente em canais de dados abertos e de transparência ativa, de informações públicas, a exemplo de despesas administrativas, estrutura de pessoal, estatísticas oficiais e documentos públicos (art. 4º, inciso I); e (b) compartilhamento parcimonioso de informações sigilosas do Estado, restrito a órgãos e entidades que compõem a Administração Pública Federal, nos termos da legislação (art. 4º, incisos II e III).

Por outro lado, sempre que menciona ou tangencia especificamente a temática do tratamento de dados pessoais, o decreto presidencial tem o cuidado de determinar a incondicional observância dos princípios gerais e direitos de proteção elencados na LGPD e dos direitos constitucionais à privacidade e proteção de dados. A propósito, assim dispõem os arts. 3º, incisos I e V, 5º, caput, e 21, inciso I, e 26, §1º:

> Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> I - a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais;
>
> [...]
>
> - nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação; e
>
> - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018;
>
> [...]
>
> Art. 5º Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para efetivação do compartilhamen-

> to de dados entre os órgãos e as entidades de que trata o art. 1º, observadas as diretrizes do art.
>
> 3º e o disposto na Lei nº 13.709, de 2018.
>
> [...]
>
> Art. 21. Fica instituído o Comitê Central de Governança de Dados, a quem compete deliberar sobre:
>
> I - as orientações e as diretrizes para a categorização de compartilhamento amplo, restrito e específico, e a forma e o meio de publicação dessa categorização, observada a legislação pertinente, referente à proteção de dados pessoais.
>
> [...]
>
> Art. 26. As controvérsias no compartilhamento de dados entre órgãos e entidades públicas federais solicitantes de dados e o gestor de dados serão decididas pelo Comitê Central de Governança de Dados.
>
> §1º As resoluções do Comitê Central de Governança de Dados a respeito de controvérsias observarão as normas que protegem os dados objetos de controvérsia.

Qualquer interpretação desviante dessa lógica, no sentido de possibilitar ampla, irrestrita e irresponsável difusão dos dados pessoais custodiados pelo Estado, conflita não apenas com diversas previsões expressas do próprio decreto presidencial, mas principalmente com preceitos sensíveis que compõem a espinha dorsal da Constituição da República e da Lei Geral de Proteção de Dados Pessoais, como os direitos à privacidade e à autodeterminação informativa.

Esse mesmo espírito deve guiar a construção e o funcionamento do Cadastro Base do Cidadão. Tenho para mim que, desde que interpretados de maneira sistemática e em conformidade com as regras da LGPD, os dispositivos do Decreto 10.046/2019 não abrem espaço para a instituição de uma base integradora descomunal, nos moldes temidos pelos requerentes.

Muito pelo contrário. Embora seja permitida e até mesmo necessária a instituição de instrumentos de interoperabilidade aptos a simplificar o fluxo de dados entre órgãos públicos, as inúmeras alusões feitas pelo decreto ao regime protetivo instituído pela LGPD impõem a necessidade de estabelecimento de ferramentas rigorosas de controle de acesso ao Cadastro Base do Cidadão.

Qualquer tentativa de abertura ampla dos elementos nele contidos, mesmo que restrita ao conjunto de órgãos públicos federais, conflitaria frontalmente com as normas que orientam o tratamento de dados pessoais. Nesse sentido, os arts. 6º, 7º e 23 da Lei 13.709/2018 estabelecem procedimento específico para o compartilhamento de dados pessoais pelo Poder Público, prevendo que, para cada entidade interessada no tratamento de informações protegidas, sejam apresentados (i) propósitos legítimos; (ii) compatibilidade do tratamento com as finalidades informadas; e (iii) limitação do compartilhamento ao mínimo necessário para atendimento do interesse público.

2.6 Distorções na composição do Comitê Central de Governança de Dados.

Considerando a relevância das atribuições exercidas pelo Comitê Central de Governança de Dados, é preciso refletir com cautela sobre as normas que estabelecem a composição do colegiado e a forma de indicação de seus membros.

Entre os argumentos articulados na petição da ADI 6.649, encontra-se a alegação de que o Decreto 10.046/2019 limita a participação no Comitê Central de Governança a "*funcionários da administração direta federal (art. 22), sem qualquer previsão de composição multissetorial*". Pondera, ainda, que se trata "*de um desenho institucional inadequado para promover a segurança, a necessidade, a adequação e a boa-fé no compartilhamento e utilização das informações pessoais*".

A esse respeito, entendo que os argumentos lançados pelo requerente são capazes de demonstrar que o Comitê Central de Governança de Dados, na forma como estruturado pelo Decreto 10.046/2019, não apenas oferece proteção deficiente para valores centrais da ordem constitucional, como também constitui fator de desestabilização das garantias previstas na Lei 13.709/2018.

Há, atualmente, um certo consenso acerca da necessidade de criação de autoridades administrativas independentes, destacadas especificamente para fiscalização e controle de atividades potencialmente lesivas ao direito de privacidade. São órgãos que desempenham papel fundamental para a concretização e o êxito das políticas de proteção enunciadas no direito positivo, constituindo fio condutor do regime constitucional de proteção de dados pessoais.

A experiência internacional nos mostra que, desde os primeiros ensaios de proteção desse direito fundamental, os países europeus reconheceram a necessidade de criação de uma ou mais autoridades independentes para monitoramento e supervisão das operações de tratamento de dados pessoais.

Já em de 25 de outubro de 1995, a Diretiva 95/46 do Parlamento Europeu dispunha que as autoridades públicas responsáveis pela fiscalização das atividades de tratamento de dados "*exercerão com total independência as funções que lhes forem atribuídas*". Posteriormente, em 7 de dezembro de 2000, a Carta dos Direitos Fundamentais da União Europeia estabeleceu, ao lado da consagração do direito fundamental à proteção de dados pessoais, a necessidade de que o *cumprimento dessas regras fique sujeito à fiscalização por parte de uma autoridade independente* (art. 8º).

A seu turno, o Regulamento Geral sobre Proteção de Dados (GPDR, na sigla em inglês), aprovado pelo Parlamento Europeu em abril de 2016, dispõe que "*os Estados-membros deverão instituir uma ou mais au-*

toridades públicas independentes com o propósito de fiscalizar a observância deste regulamento". Também prevê que os membros dessas autoridades "*devem agir com total independência no exercício de suas atribuições [...] e não devem estar sujeitos a influências externas, diretas ou indiretas, nem devem solicitar ou receber instruções de outras autoridades*".

No âmbito da OCDE, diversos países optaram pela criação de entidades independentes vocacionadas a apoiar o Estado no gerenciamento de informações pessoais. Nesse modelo, compete a estas entidades a tarefa de construir parâmetros éticos e procedimentos qualificados para o tratamento de dados do cidadão. (OCDE. The Path to Becoming a Data-Driven Public Sector. OCDE Publishing: Paris, 2019, p. 113).

Coube a cada ente nacional, no exercício de sua soberania, esculpir o arquétipo legal das agências responsáveis pelo controle de atividades potencialmente lesivas ao direito de privacidade. A experiência internacional sinaliza, contudo, um ponto de confluência na legislação dos países democráticos: há uma invariável preocupação de instituir as autoridades nacionais a partir de perfil institucional autônomo, que seja capaz de assegurar o exercício da função de controle com total independência.

Estudo conduzido por Graham Greenleaf, a respeito do regime de proteção de dados de 132 países, comprovou que a esmagadora maioria das nações criou agências independentes para fiscalização do tratamento de dados pessoais. Dentro do universo de países analisados, apenas 14 não seguiram esse modelo, relegando a atividade de controle para entidades subordinadas ao governo. Isso, segundo o autor, seria motivo de grande desonra para os integrantes dessa minoria (GREENLEAF, Graham. Global Data Privacy 2019: DPAS, PEAS and their networks: 158 Privacy Laws & Business International Report, 2019, pp, 11-14).

Em Portugal, a Lei 58, de 8 de agosto de 2019, assegurou a execução, na ordem jurídica interna, do Regulamento Geral sobre Proteção de

Dados (GPDR). Paralelamente ao reconhecimento do direito fundamental à proteção de dados pessoais, o legislador português instituiu a Comissão Nacional de Proteção de Dados (CNPD) como "*entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto à Assembleia da República*". Em homenagem à independência da CNPD, a lei lhe atribuiu a seguinte composição multissetorial: (a) três membros eleitos pela Assembleia da República; (b) dois membros indicados pelo Governo; (c) um magistrado indicado pelo Conselho Superior da Magistratura; e d) um membro do *Parquet* designado pelo Conselho Superior do Ministério Público.

No Canadá, o *Privacy Act* de 1985 atribuiu essas atividades a uma autoridade independente denominada *Privacy Commissioner*, indicada pelo Governador-geral (*Governor in Council*), após consulta de todos os líderes partidários com representação no Parlamento. Após a indicação formal, o nome proposto deve ainda ser aprovado em resolução das duas Casas do Congresso Nacional.

Nos Estados Unidos da América, o Estado da Califórnia editou legislação específica sobre privacidade, intitulada *California Consumer Privacy Act* (CCPA). À semelhança do regulamento europeu, esse moderno diploma legislativo previu que as normas e princípios nele reconhecidos seriam fiscalizados por uma agência independente, composta por (a) um membro indicado pelo Governador; (b) um membro indicado pelo Procurador-Geral; (c) e dois membros indicados pelo Parlamento. Em todos os casos, o CCPA exige que os indicados tenham vasta experiência nas áreas de privacidade, tecnologia e direitos do consumidor.

Na Nova Zelândia, o governo reuniu, no âmbito do Poder Executivo, um Grupo de Aconselhamento Ético para o tratamento de dados pessoais (*Data Ethics Advisory Group*). A esse respeito, é fundamental destacar que, não obstante se trate de órgão de caráter interno, o governo estabe-

leceu procedimento seletivo público (*expression of interest process*) para escolha dos membros do colegiado, exigindo ainda que os candidatos comprovassem notório conhecimento nas áreas de privacidade, direitos humanos, ética, tecnologia e políticas públicas (https://www.stats.govt.nz/news/stats-nz-convenes-data-ethics-advisorygroup).

O exame dos modelos adotados pelas nações democráticas, especialmente pela perspectiva do arquétipo legal das autoridades públicas de controle, revela uma correlação necessária entre a previsão de mecanismos capazes de garantir independência a essas entidades e a efetiva defesa do direito de proteção de dados pessoais.

Nesse sentido, a experiência internacional é capaz de demonstrar que a tutela efetiva do direito à privacidade depende da correta calibragem do perfil institucional dos órgãos responsáveis pela regulamentação, controle e monitoramento de atividades de tratamento de dados pessoais. Assim, é fundamental reconhecer a necessidade de estruturar essas entidades a partir de uma composição plural e democrática, aberta, em alguma medida, a constante diálogo com a sociedade civil.

No âmbito interno, esse modelo tem sido reproduzido nas legislações setoriais aprovadas pelo Congresso Nacional. É o que ocorreu, por exemplo, com a instituição da Autoridade Nacional de Proteção de Dados (ANPD), composta fundamentalmente por 5 diretores escolhidos pelo Presidente da República e por ele nomeados, após aprovação do Senado Federal. Adicionalmente, a lei exigiu que os membros tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos pretendidos. Estabeleceu, por fim, mandato de 4 anos para os diretores, que somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo disciplinar (arts. 55-D e 55-E da Lei 13.709/18).

Da mesma forma, a Lei 13.444/17, que dispõe sobre a Identificação Civil Nacional (ICN), instituiu Comitê Gestor do programa, cabendo-lhe,

entre outras atribuições, orientar a implementação da interoperabilidade entre a base de dados biométricos da Justiça Eleitoral e os bancos de dados administrados pelo Poder Executivo. Ante a sensibilidade da matéria, o Congresso Nacional atribuiu semblante multissetorial ao Comitê Gestor da ICN, composto por: (a) três representantes do Poder Executivo; (b) três representantes do Tribunal Superior Eleitoral; (c) um representante da Câmara dos Deputados; (d) um representante do Senado Federal; e (e) um representante do Conselho Nacional de Justiça (art. 5º).

Na contramão da experiência internacional e das legislações setoriais aprovadas pelo Congresso Nacional, o Decreto 10.046/19 atribuiu ao Comitê Central de Governança de Dados uma estrutura hermética, ocupada exclusivamente por representantes da Administração Pública federal, designadamente servidores do Ministério da Economia, da Presidência da República, da Controladoria-Geral da União, da Advocacia-Geral da União e do Instituto Nacional do Seguro Social (art. 22).

Cuida-se, a rigor, de instituição com perfil insular, hostil a qualquer proposta de abertura democrática e de pluralização do debate e, nessa medida, fechada à participação de representantes oriundos de outras instituições republicanas e de entidades da sociedade civil.

A falta de alinhamento do ato editado pelo Chefe do Poder Executivo com as boas práticas observadas nas nações democráticas requer atenção do Tribunal. Longe de um mero preciosismo acadêmico, a particular arquitetura institucional introduzida pelo regulamento produz efeitos transversais na ordem jurídico-constitucional, podendo acarretar um autêntico desmonte dos pilares estruturantes da LGPD e, no limite, comprometer a própria eficácia do direito fundamental à proteção de dados pessoais.

As distorções identificadas na composição do Comitê Central de Governança de Dados oferecem, ainda, grave risco de comprometimento da imagem do país no plano externo, podendo, em certa medida, ameaçar

pretensões deduzidas pelo Estado brasileiro de ingresso em entidades internacionais relevantes, como a Organização para a Cooperação e Desenvolvimento Econômico – OCDE.

Como se sabe, em janeiro de 2022, o governo brasileiro iniciou tratativas formais para ingresso nesse importante organismo de cooperação multilateral. No curso do processo de adesão, o país será avaliado a respeito da adequação de sua legislação, instituições e práticas aos padrões defendidos pela OCDE em diversos setores, como meio ambiente, saúde, responsabilidade fiscal, sistema tributário e proteção da concorrência e do consumidor.

Não há dúvidas, pois, que, ao longo dos próximos meses, o Estado brasileiro será rigorosamente escrutinado acerca de sua política de privacidade de dados, seja no que diz respeito à existência de instituições capazes de responder diligentemente contra ameaças de malversação dos princípios estruturantes da LGPD, seja no que concerne à compatibilidade do sistema doméstico às normas, aos padrões e aos valores compartilhados pelas nações democráticas.

A propósito do assunto, não se pode perder de vista a advertência feita por Fabrício Bertini Pasquot Polido, em artigo publicado no site CONJUR (O ingresso do Brasil na OCDE e padrões em matéria digital, Revista Consultor Jurídico, publicado em 7 de março de 2022, disponível em <www.conjur.com.br>). Destaco:

> Além desses objetivos, a OCDE prioriza iniciativas que estejam diretamente atreladas ao livre fluxo de dados e confiança digital. Não basta a existência de uma Lei Geral de Proteção de Dados – a LGPD – e uma Autoridade Nacional de Proteção de Dados no caso brasileiro, mas antes a consolidação de um desenho institucional dotado de efetividade e autonomia quanto à formulação de políticas e aplicação de decisões, além de princípios de transparência na composição de conselhos políticos. Práticas sólidas de cooperação digital por parte do Estado brasileiro também serão escrutinadas à luz das diretrizes mais recentes da organização, como os princípios OCDE

> sobre Inteligência Artificial e objetivos de promoção do livre fluxo de dados com confiança e Princípios de Alto-Nível relativos ao Acesso Confiável de Governos a Dados Pessoais. Membros da OCDE, como na pretendida acessão do Estado brasileiro à organização, devem assegurar que padrões adequados de privacidade de dados estejam comprovados tecnicamente, com leis e regulamentos que estabelecem regras relativas às garantias de segurança e confiança de usuários de internet e consumidores digitais, além do combate à desinformação e promoção de princípios democráticos e dos direitos humanos associados às operações digitais.

O perfil orgânico estabelecido pelo decreto se torna ainda mais grave quando constatada a extensão e a relevância das funções desempenhadas pelo Comitê Central de Governança de Dados. Nos termos do art. 21 do Decreto 10.046/2019, compete ao órgão: a) expedir regulamentos para disciplinar a forma, o alcance e os limites inerentes ao compartilhamento de dados pelos órgãos integrantes da Administração Pública federal; b) deliberar sobre orientações e diretrizes para categorização do compartilhamento amplo, restrito e específico, especialmente à luz da LGPD; c) dispor sobre orientações e diretrizes para acesso de órgãos públicos ao Cadastro Base do Cidadão; d) escolher as bases temáticas que serão integradas ao Cadastro Base do Cidadão; e e) dispor sobre a inclusão, nessa base integradora, de novos dados provenientes das bases temáticas administradas pelos órgãos federais.

Dada a relevância e a sensibilidade da sua missão institucional, é inequívoco que o Comitê Central de Governança de Dados ocupa posição de centralidade no regime constitucional de proteção da privacidade. Cuida-se de entidade que atua em articulação direta com a Autoridade Nacional de Proteção de Dados, desempenhando atribuições que dialogam intimamente com as regras e princípios instituídos pela LGPD, sobretudo no que diz respeito à preservação da privacidade dos usuários de serviços públicos federais.

Essas premissas conduzem à conclusão de que a arquitetura institucional atualmente conferida ao Comitê Central de Governança de Dados desarticula um mecanismo que é fundamental para o fortalecimento das

salvaguardas previstas na LGPD, no caso, a independência dos órgãos vocacionados ao controle das atividades de tratamento de dados pessoais.

Não bastasse isso, a forma de indicação dos membros desse órgão vai de encontro ao modelo seguido pelas nações democráticas e pelo próprio legislador brasileiro, interditando a participação democrática e a pluralização do debate no âmbito da entidade que estabelece os limites, a extensão e as condições de acesso ao Cadastro Base do Cidadão, seguramente a maior base de dados pessoais existente no território nacional.

A respeito da eficácia objetiva do direito à autodeterminação informativa, Ingo Wolfgang Sarlet leciona que *outra importante função atribuída aos direitos fundamentais e desenvolvida com base na existência de um dever geral de efetivação atribuído ao Estado, por sua vez agregado à perspectiva objetiva dos direitos fundamentais, diz com o reconhecimento de deveres de proteção (schutzpflichten) do Estado, no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos (...)*". (SARLET, Ingo Wolfgang. Proteção de Dados Pessoais e deveres de proteção estatais, Revista Consultor Jurídico, publicado em 27 de agosto de 2021, disponível em <www.conjur.com.br>)

Prossegue o autor afirmando que a tutela do direito à autodeterminação informativa "*depende de estruturas organizacionais e de procedimentos adequados*" que sejam capazes de assegurar, com o maior nível possível de eficácia, a tutela dos valores éticos que orbitam a atual ordem constitucional. Por esse motivo, haveria "*íntima vinculação entre direitos fundamentais, organização e procedimento, no sentido de que os direitos fundamentais são, ao mesmo tempo e de certa forma, dependentes da organização e do procedimento (no mínimo, sofrem uma influência por parte destes), mas simultaneamente também atuam sobre o direito procedimental e as estruturas organizacionais*".

No âmbito acadêmico, já tive a oportunidade de afirmar que "*importante consequência da dimensão objetiva dos direitos fundamentais está em ensejar um dever de proteção pelo Estado dos direitos fundamentais contra agressões dos próprios Poderes Públicos, provindas de particulares ou de outros Estados*". Todavia, ressaltei que não existe "*ordinariamente um dever específico de agir por parte do Estado, uma vez que os Poderes Públicos gozam de discricionariedade para escolher uma das diferentes opções de ação que se lhes abrem, levando em conta os meios que estejam disponíveis, as colisões de direitos e interesses envolvidos e a sua escala de prioridades políticas*". (MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, 14ª edição, São Paulo, Saraiva, 2019, p. 169)

Dessa forma, considerando que o Comitê Central de Governança de Dados é composto única e exclusivamente por representantes do Poder Executivo, e que seus membros não gozam de qualquer garantia contra influências indevidas, entendo que a estrutura organizacional prevista no art. 22 do Decreto 10.046/19 afronta o regime de proteção de dados instituído pela atual ordem constitucional.

Convém ressaltar, todavia, que a invalidação, *tout court*, do dispositivo impugnado acarretaria uma situação ainda mais nociva para a tutela da privacidade dos usuários de serviços públicos, desmantelando a entidade responsável pelo estabelecimento de limites ao compartilhamento de dados entre órgãos da Administração Pública federal.

Ante o risco de desestabilização do sistema, considero prudente reconhecer efeitos prospectivos à declaração de inconstitucionalidade, preservando a atual estrutura orgânica do Comitê Central de Governança de Dados pelo prazo de 60 dias, a contar da data de publicação da ata de julgamento. Assim, ao modular os efeitos da decisão, o Tribunal garantirá ao Presidente da República prazo hábil para a superação do modelo

orgânico declarado inconstitucional, de modo a resgatar a trajetória de fortalecimento dos mecanismos de proteção de dados pessoais.

Trata-se, a meu ver, de solução conciliatória, que permite ao Tribunal atuar na defesa de direitos negligenciados pelo Estado, sem, contudo, invadir o domínio dos representantes democraticamente eleitos ou assumir compromisso com a conformação da fisionomia de órgãos integrantes do Poder Executivo.

2.7 Consequências do desrespeito ao regime de proteção de dados pessoais. Surgimento de pretensões materiais e responsabilização do agente público infrator.

A partir da inclusão do direito de proteção de dados pessoais no catálogo de direitos fundamentais, põe-se em perspectiva a questão relativa à responsabilização de agentes públicos pelo descumprimento do dever de tutela previsto no art. 5º, inciso LXXIX, da Constituição Federal.

Trata-se de um debate que assume substancial relevância no âmbito do tratamento de dados por órgãos estatais, na medida em que, dada a colossal extensão dos dados coletados pelo Estado, exsurgem riscos de abusos na utilização dos dados pessoais ou, em caso de omissão ou desídia do gestor público, de graves incidentes de segurança.

Assim sendo, deixando de lado qualquer pretensão de esgotamento da matéria, o que demandaria uma análise abrangente do ordenamento jurídico brasileiro – algo incompatível com o objeto da demanda – passo a discorrer brevemente sobre as consequências jurídicas do descumprimento do direito fundamental à proteção de dados pessoais.

Sobre o ponto, há consenso na doutrina acerca das consequências imediatas que exsurgem quando levada a efeito uma ingerência (injustificada) no âmbito de proteção de um direito fundamental (SCHLINK, Bernard; PIEROTH, Bodo. Direitos Fundamentais. 2ª ed. Saraiva: São Paulo, 2019, p. 124).

Nas palavras de Ingo Wolfgang Sarlet:

> "quando nos referimos aos direitos fundamentais como direitos subjetivos, temos em mente a noção de que ao titular de um direito fundamental é aberta a possibilidade de impor judicialmente seus interesses juridicamente tutelados perante o destinatário". (...) "a noção de uma perspectiva subjetiva dos direitos fundamentais engloba a possibilidade de o titular do direito fazer valer judicialmente os poderes, as liberdades ou mesmo o direito de ação ou às ações negativas ou positivas que lhe foram outorgadas pela norma consagradora do direito fundamental em questão (...)." (SARLET, Ingo Wolfgang. Curso de Direito Constitucional. 10ª edição, São Paulo, Saraiva, 2021, pp. 352-353)

Nesse mesmo sentido, o reconhecimento de um direito subjetivo de envergadura constitucional, de acordo com a formulação de Vieira de Andrade, está atrelado "*à proteção de uma determinada esfera de autorregulamentação ou de um espaço de decisão individual; tal como é associado a um certo poder de exigir ou pretender comportamentos ou de produzir autonomamente efeitos jurídicos*". (VIEIRA DE ANDRADE. Os direitos fundamentais na Constituição portuguesa de 1976. Coimbra: Almedina, 1987, p. 163).

Considerando que o âmbito de proteção do direito à proteção de dados é instituído, em larga medida, pela atribuição legiferante do Legislador, convém consignar, pelos riscos suscitados pela matéria, que a violação ao direito de proteção de dados pessoais gera, em favor do cidadão, pretensão de direito material, que por seu turno faculta o exercício do direito de ação.

Faço, aqui, especial referência ao surgimento da (i) pretensão reparatória civil, exercida de acordo com a lógica e as disposições do direito privado; (ii) da pretensão punitiva disciplinar, um poder-dever de titularidade da Administração, proveniente dos estatutos dos servidores públicos federais, estaduais, distritais e municipais; e (iii) da pretensão punitiva, de caráter eminentemente repressivo, prevista na Lei de Improbidade Administrativa.

Atualmente, diante da clareza do art. 42 da LGPD, há um certo consenso acerca da necessidade de reparação dos danos causados em decorrência do tratamento de dados pessoais. A esse respeito, dispõe a lei que *o controlador ou operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo*.

Trata-se de regra evidentemente aplicável ao âmbito do Poder Público, com as devidas adaptações. São pertinentes, a esse respeito, as considerações feitas pelo Supremo Tribunal Federal no julgamento do tema 940 da repercussão geral, cujo paradigma é o RE 1.027.633, de relatoria do EMINENTE MINISTRO MARCO AURÉLIO, em que se fixou o entendimento de que a ação por danos causados por agente público deve ser ajuizada contra o Estado, a quem compete, posteriormente, exercer o direito de regresso contra o responsável, se identificada conduta culposa ou dolosa.

Assim sendo, o tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais (ingerência) importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa.

Em relação às pretensões repressivas e disciplinares, há que se ter em mente que, insisto, o compartilhamento de dados entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, "*fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos*".

Dessa forma, deve-se ter presente que a transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da incidência de outras tipificações legais, a depender das particularidades do caso concreto.

Assinalo também quanto à possibilidade de responsabilização disciplinar dos servidores públicos pela malversação das informações pessoais, conforme previsto no respectivo estatuto funcional.

Adotados os delineamentos acima expostos, tenho que este Supremo Tribunal Federal fomentará o espraiamento de uma cultura institucional de proteção de dados pessoais no interior dos órgãos administrativos para, com isso, impedir, ou ao menos minimizar, possíveis violações ao direito constitucional à proteção de dados.

3. Conclusão

Ante o exposto, voto no sentido de conhecer a ação direta e a arguição de descumprimento de preceito fundamental e, julgando parcialmente procedentes os pedidos, confiro interpretação conforme ao Decreto 10.046/2019, traduzida nos seguintes termos:

1. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.

2. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, "*fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos*".

3. O acesso de órgãos e entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao atendimento integral das diretrizes acima arroladas, cabendo ao Comitê Central de Governança de Dados, no exercício das competências aludidas nos arts. 21, incisos VI, VII e VIII do Decreto 10.046/2019:

   3.1 prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos. Nesse sentido, a permissão de acesso somente poderá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º, inciso III, e art. 23, caput e inciso I, da Lei 13.709/2018;

   3.2 justificar prévia e minudentemente, à luz dos postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD, tanto a necessidade de inclusão de novos dados pessoais na base integradora (art. 21, inciso VII) como a escolha das bases temáticas que comporão o Cadastro Base do Cidadão (art. 21, inciso VIII).

   3.3 instituir medidas de segurança compatíveis com os princípios

de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso.

4. O compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI 6.529, Rel. Min. Cármen Lúcia, quais sejam: (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.

5. O tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo.

6. A transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da aplicação das sanções disciplinares previstas nos estatutos dos servidores públicos federais, municipais e estaduais.

Voto, ainda, no sentido de declarar, com efeito *pro futuro*, a inconstitucionalidade do art. 22 do Decreto 10.046/19, preservando a atual estrutura do Comitê Central de Governança de Dados pelo prazo de 60 dias, a contar da data de publicação da ata de julgamento, a fim de garantir ao Chefe do Poder Executivo prazo hábil para (i) atribuir ao órgão um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas; e (ii) conferir aos seus integrantes garantias mínimas contra influências indevidas.

É como voto.

LEGISLAÇÃO

EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022

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.

As Mesas da Câmara dos Deputados e do Senado Federal, nos termos do § 3º do art. 60 da Constituição Federal, promulgam a seguinte Emenda ao texto constitucional:

Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:

"Art. 5º .....

.....

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

.....(NR)

Art. 2º O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:

"Art. 21. .....

.....

XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei." (NR)

Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:

"Art. 22. .....

.....

XXX - proteção e tratamento de dados pessoais.

....." (NR)

Art. 4º Esta Emenda Constitucional entra em vigor na data de sua publicação.

Brasília, em 10 de fevereiro de 2022

Mesa da Câmara dos Deputados	Mesa do Senado Federal
Deputado ARTHUR LIRA Presidente	Senador RODRIGO PACHECO Presidente
Deputado MARCELO RAMOS 1º Vice-Presidente	Senador VENEZIANO VITAL DO RÊGO 1º Vice-Presidente
Deputado ANDRÉ DE PAULA 2º Vice-Presidente	Senador ROMÁRIO 2º Vice-Presidente
Deputado LUCIANO BIVAR 1º Secretário	Senador IRAJÁ 1º Secretário
Deputada MARÍLIA ARRAES 2ª Secretária	Senador ELMANO FÉRRER 2º Secretário
Deputada ROSE MODESTO 3ª Secretária	Senador ROGÉRIO CARVALHO 3º Secretário
Deputada ROSANGELA GOMES 4ª Secretária	Senador WEVERTON 4º Secretário

Este texto não substitui o publicado no DOU 11.2.2022

PROPOSTA DE EMENDA À CONSTITUIÇÃO Nº 17, 2019.

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.

As Mesas da Câmara dos Deputados e do Senado Federal, nos termos do art. 60, da Constituição Federal, promulgam a seguinte Emenda à Constituição Federal, de 5 de outubro de 1988:

Art. 1° Inclua-se no art. 5°, da Constituição Federal, o seguinte inciso XII-A:

"Art. 5° .....

.....

XII-A - é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais.

JUSTIFICAÇÃO

A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão.

O avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados.

Por isso, países de todo o planeta já visualizaram a importância e imprescindibilidade de se regular juridicamente o tratamento de dados dos cidadãos. É o caso dos membros da União Europeia, que, hoje, já contam com a segunda e moderna versão regulatória sobre o assunto, chamado de Regulamento Geral de Proteção de Dados. O RGPD entrou em vigor em 25 de maio de 2018, gerando um impacto de nível global, sobretudo em face de milhares de empresas que ofertam serviços ao mercado europeu.

Na América do Sul, países vizinhos como Chile e Argentina, entre outros, já contam com I eis próprias de proteção de dados. De fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado.

Foi o caso de Portugal: sua Constituição, adotada em 1976, assegura o direito e a garantia pessoal de utilização da informática, estabelecendo, também, normas específicas de acesso e tratamento de dados pessoais. Algo similar se vê na Estônia, Polônia e, mais recentemente, no Chile, que, em 5 de junho de 2018, editou a Ley no 27.096, constitucionalizando a proteção de dados pessoais.

Convictos de que o Brasil necessita muita mais do que uma lei ordinária sobre o assunto, apesar da envergadura jurídica da Lei no 13.709, de 14 de agosto de 2018 (LGPD), propomos a presente mudança à Constituição Federal.

Nesta Proposta, também buscamos, além de instituir o direito fundamental à proteção de dados pessoais, também disciplinar questão tormentosa: a competência constitucional para legislar sobre o tema.

Sabemos que existem diversas propostas de leis estaduais e municipais versando sobre o assunto, inclusive em flagrante réplica da LGPD. Não há racionalização nisso: a fragmentação e pulverização de assunto tão caro à sociedade deve ser evitada. O ideal, tanto quanto se dá com outros direitos fundamentais e temas gerais relevantes, é que a União detenha a competência central legislativa. Do contrário, pode -se correr o risco de, inclusive de forma inconstitucional, haver dezenas -talvez milhares - de conceitos legais sobre o que é “dado pessoal” ou sobre quem são os “agentes de tratamento” sujeitos à norma legal.

Impõe-se, portanto, que o país apresente uma legislação uniforme quanto à proteção e tratamento de dados, tendo em vista ser pratica-

mente impossível aos governos e empresas de todo o mundo se adaptarem a normas específicas de cada localidade. Além disso, a pluralidade normativa pode trazer problemas de compatibilidade e adequação dos dados, em especial nos serviços disponibilizados pela rede mundial de computadores, que utilizam os dados pessoais de formas cada vez mais abrangentes e inovadoras.

Trata-se de alteração que é altamente aconselhável para a racionalização do tratamento de dados no país e sua inclusão na realidade internacional da disciplina da matéria. Por essa razão, esperamos poder contar com o apoiamento dos nobres Pares à presente proposta.

Sala das sessões, em de fevereiro de 2019.

Senador **EDUARDO GOMES - MDB-TO**

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Lei Geral de Proteção de Dados Pessoais (LGPD).

REVISTA JURÍDICA
DO BANCO DO NORDESTE

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade,

a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019)

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

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

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

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

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arqui-

vamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

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

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras,

precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O tratamento de dados pessoais cujo acesso é público deve

considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários

para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluí-

do pela Lei nº 13.853, de 2019)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019)

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em

regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III

Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos

de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV

Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados

deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controla-

dor, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a fina-

lidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019)

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I

Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informa-

ções claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II - (VETADO);

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada

em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019)

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019)

Art. 30. A autoridade nacional poderá estabelecer normas comple-

mentares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II

Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

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

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

V - quando a autoridade nacional autorizar a transferência;

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

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

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

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser

revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I

Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados,

a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Seção III

Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser

exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das

relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco

ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I

Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o

mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a

ser aplicada pelo seu descumprimento.

CAPÍTULO IX
DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (Redação dada pela Lei nº 14.460, de 2022)

§ 1º (Revogado pela Lei nº 14.460, de 2022)

§ 2º (Revogado pela Lei nº 14.460, de 2022)

§ 3º (Revogado pela Lei nº 14.460, de 2022)

Art. 55-B. (Revogado pela Lei nº 14.460, de 2022)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - (revogado); (Redação dada pela Lei nº 14.460, de 2022)

V-A - Procuradoria; e (Incluído pela Lei nº 14.460, de 2022)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD

serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela

Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de ges-

tão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento

do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade

econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imó-

veis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: (Incluído pela Lei nº 14.460, de 2022)

I - que lhe forem transferidos pelos órgãos da Presidência da República; e (Incluído pela Lei nº 14.460, de 2022)

II - que venha a adquirir ou a incorporar. (Incluído pela Lei nº 14.460, de 2022)

Art. 56. (VETADO).

Art. 57. (VETADO).

Seção II

Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares

e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre

a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procu-

ração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional, e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim

Aloysio Nunes Ferreira Filho

Eduardo Refinetti Guardia

Esteves Pedro Colnago Junior

Gilberto Magalhães Occhi

Gilberto Kassab

Wagner de Campos Rosário

Gustavo do Vale Rocha

Ilan Goldfajn

Raul Jungmann

Eliseu Padilha

Este texto não substitui o publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

REVISTA JURÍDICA
DO BANCO DO NORDESTE

LEI Nº 12.965, DE 23 DE ABRIL DE 2014

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

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

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet,

seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazena-

mento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (Redação dada pela Lei nº 13.709, de 2018)

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput,** tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I

Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei

nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II

Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser

disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I

Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput.**

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput.**

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissio-

nalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput,** observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais. (Redação dada pela Lei nº 13.709, de 2018)

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

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.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV

Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos

terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no **caput,** bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

Miriam Belchior

Paulo Bernardo Silva

Clélio Campolina Diniz

Este texto não substitui o publicado no DOU de 24.4.2014

NORMAS PARA APRESENTAÇÃO DE ORIGINAIS

A Revista Jurídica do Banco do Nordeste é uma publicação semestral do Banco do Nordeste do Brasil S.A., que tem por finalidade divulgar a produção intelectual de profissionais e acadêmicos de Direito e de áreas afins, criando uma fonte de pesquisa permanente para a comunidade jurídica brasileira, mormente no que se refere às questões envolvendo as Empresas Estatais (Sociedades de Economia Mista e Empresas Públicas).

1. DIRETRIZES EDITORIAIS

1.1 A linha editorial da Revista abrange todas as áreas do Direito, com foco prioritário nas temáticas atinentes às Empresas Estatais (Empresas Públicas e Sociedades de Economia Mista).

1.2 Os trabalhos encaminhados para publicação deverão ser inéditos e sua publicação não deve estar pendente em outro local. Uma vez publicados, estes trabalhos consideram-se licenciados para o Banco do Nordeste do Brasil S/A com exclusividade, pelo prazo de duração dos direitos patrimoniais do autor. Os trabalhos também poderão ser publicados em outros lugares desde que após autorização prévia e expressa do Comitê Editorial da Revista, citada a publicação original como fonte, constando o nome da editora, a cidade, o ano de publicação, título e volume do periódico e respectivas páginas.

1.3 A Revista Jurídica do Banco do Nordeste publica trabalhos inéditos, depois de submetidos à aprovação em duas etapas:

• Exame por no mínimo 2 (dois) pareceristas anônimos, para avaliação de forma e conteúdo; e • Seleção dos trabalhos pelo Comitê Editorial.

1.4 O autor faculta ao Banco do Nordeste publicar seu trabalho na Revista Jurídica do Banco do Nordeste, em mídia tradicional e eletrônica, existente ou que venha a ser descoberta, para efeito de divulgação científica da Revista e de seu conteúdo, conforme a Lei 9.610/98.

1.5 Uma vez aceitos, os trabalhos passarão por revisão quanto à forma, a exemplo de correções ortográficas, gramaticais e adequação ao formato da Revista, sem qualquer alteração em seu conteúdo. As provas tipográficas não serão enviadas aos autores.

1.6 Após avaliados, os pareceres poderão ser encaminhados aos autores, para que tomem ciência da aceitação do artigo ou, em caso de rejeição, possam adaptar seu texto ou justificar a manutenção do formato inicial.

1.7 Não será prestada nenhuma remuneração autoral pela licença de publicação dos trabalhos na Revista Jurídica do Banco do Nordeste ou qualquer tipo de mídia, impressa ou eletrônica (Internet, CDRom, e-book etc.). Em contrapartida, o colaborador receberá 03 (três) exemplares do periódico em Revista Jurídica do Banco do Nordeste cujo número seu trabalho tenha sido publicado, salvo em caso de publicação exclusiva por meio on-line.

1.8 Os trabalhos que não se ativerem às normas aqui apresentadas serão devolvidos a seus autores, que poderão reenviá-los, desde que efetuadas as modificações necessárias.

1.9 O conteúdo dos artigos, as ideias e os conceitos neles emitidos são de responsabilidade exclusiva de seus autores.

1.10 A remessa do texto pelo autor ao Comitê Editorial para fins de publicação implica a cessão dos direitos autorais para a Revista Jurídica do Banco do Nordeste, a permissão de publicação em meio eletrônico e a possibilidade de reprodução do texto para pesquisa pessoal.

1.11 Os trabalhos recebidos e não publicados na edição da Revista imediatamente posterior ao seu envio não serão devolvidos, deixando de persistir, nesta hipótese, a regra do item 2.10, salvo se o autor manifestar interesse na publicação de seu trabalho na edição seguinte da Revista.

1.12 A Revista será composta pelas seguintes seções:

• Doutrina: constituída por artigos científicos ou parecer(es) jurídico(s);

• Jurisprudência: formada por acórdãos, apresentados preferencialmente em seu inteiro teor, referentes à linha editorial da Revista; e

• Atualização Legislativa: estruturada por legislação relacionada à linha editorial da Revista.

2. APRESENTAÇÃO DOS TRABALHOS

2.1 Formato: todas as colaborações devem ser enviadas pela internet para o email revistajuridi-ca@bnb.gov.br. Recomenda-se a utilização do processador de texto Microsoft Word 97 ou superior. Pode-se, no entanto, utilizar qualquer processador de texto, desde que os arquivos sejam gravados no formato RTF (Rich Text Format). • Os textos devem ter no máximo 30 páginas. Os parágrafos devem ser alinhados à esquerda. Não devem ser usados recuos, deslocamentos, nem espaçamentos antes ou depois. Não se deve utilizar o tabulador para determinar os parágrafos: o próprio já determina, automaticamente, a sua abertura. Como fonte, usar o Times New Roman, corpo 12. Os parágrafos devem ter entrelinha 1,5; as margens superior e inferior 2,0 cm e as laterais 3,0 cm. O tamanho do papel deve ser A4. Poderão também ser recebidos trabalhos em língua estrangeira (espanhol ou inglês).

2.2 Título do artigo: o título deve ser breve e suficientemente específico e descritivo, em português e em inglês, contendo as palavras-chave que representam o conteúdo do artigo.

2.3 Folha de rosto: os trabalhos deverão ser precedidos por uma folha na qual se fará constar: o título do trabalho, o nome do autor (ou autores), qualificação (situação acadêmica, títulos, instituições às quais pertença e a principal atividade exercida), endereço completo para correspondência, telefone, e-mail, e declaração de ineditismo (a autorização

de publicação será solicitada em caso de aprovação do artigo).

2.4 Resumo e Sumário: os trabalhos deverão ser precedidos por um breve Resumo (10 linhas no máximo) em português e em inglês, e de um Sumário, em português, do qual deverão constar os itens com até 3 dígitos, redigido, preferencialmente, conforme as normas da NBR 6028, da Associação Brasileira de Normas Técnicas (ABNT).

2.5 Palavras-chave: deverão ser destacadas as palavras-chave (palavras ou expressões que expressem as ideias centrais do texto) limitadas ao número de 05 (cinco), em português e em inglês, as quais possam facilitar posterior pesquisa ao trabalho.

2.6 Destaques no texto: todo destaque que se queira dar ao texto impresso deve ser feito com o uso de itálico. Jamais deve ser usado o negrito ou a sublinha.

2.7 Citações: devem seguir o padrão nota de rodapé, recomendado pela ABNT. Citações de textos de outros autores deverão ser feitas entre aspas, sem o uso de itálico, quando no corpo do texto; ou em fonte menor (Times New Roman 10) quando destacadas.

2.8 Notas: nota referente ao corpo do artigo deve ser indicada com um número alto, imediatamente depois da frase a que diz respeito. Deverá vir no rodapé do texto, sem ultrapassar cinco linhas por cada página.

2.9 Materiais gráficos: fotografias nítidas em formato JPG e gráficos no programa “Corel Draw” poderão ser aceitos, desde que estritamente indispensáveis à clareza do texto. Deverão ser assinalados, no texto, pelo seu número de ordem, os locais onde devem ser intercalados. Se as ilustrações enviadas já tiverem sido publicadas, mencionar a fonte e apresentar a permissão para reprodução.

2.10 Tabelas e Quadros: as tabelas e os quadros deverão ser acompanhados de cabeçalho que permita compreender o significado dos dados

reunidos, sem necessidade de referência ao texto, obedecendo às normas de apresentação tabular, da Fundação IBGE em vigor. Devem também ter numeração sequencial própria para cada tipo e suas localizações devem ser assinaladas no texto, com a indicação do número de ordem respectivo.

2.11 Referências: seguem, preferencialmente, a norma em vigor, NBR 6023, da Associação Brasileira de Normas Técnicas (ABNT). As referências bibliográficas deverão conter: sobrenome do autor em letras maiúsculas; vírgula; nome do autor em letras minúsculas; ponto; título da obra em itálico; ponto; número da edição (a partir da segunda); ponto; local; dois pontos; editora (não usar a palavra editora); vírgula; ano da publicação; ponto.

2.12 Referência de documento pesquisado na Internet: sempre que possível, deve ser informado o endereço eletrônico específico, visando facilitar a localização imediata do documento. Evite-se, portanto, o endereço eletrônico geral (da instituição que publicou o documento, por exemplo; ou revista, no caso de artigo de periódico). Quando houver o endereço específico do documento ou artigo, é preferível este ao do site. Os autores poderão obter outras informações pelo telefone (085) 3299.3085, fax (085) 3299.3786, correio eletrônico revistajuridica@bnb.gov.br e http://www.bnb.gov.br/revistajuridica.

AGRADECIMENTO ESPECIAL

Esta Edição Especial da Revista Jurídica do Banco do Nordeste é um projeto coletivo e fruto do esforço de diversas pessoas dedicadas à nobre missão de disseminar o conhecimento. Neste sentir, registramos nosso agradecimento a todos e a todas que, de alguma forma, contribuíram com este propósito.

Mas, em particular, gostaríamos de fazer um agradecimento especial ao Enrico Martins, CEO e Founder da empresa 9Net, por sua sensibilidade, confiança e compreensão da importância do projeto, que tornaram possível a materialização desta Edição Especial da Revista Jurídica do Banco do Nordeste.

O Enrico Martins é um conhecido empresário com mais de 20 anos de experiência em TI, cybersegurança, privacidade, gestão de risco e compliance. Formado em ciência da computação e marketing, especialista em cybersegurança pelo MIT, especialista em projetos de infraestrutura e segurança da informação e TI *as a service*, com vasta experiência em projetos internacionais na América Latina. Seu foco é tornar a área de TI, segurança e GRC, mais funcionais, para que possam entregar valor e competitividade ao negócio.

Esta Edição Especial foi possível em razão
do apoio da empresa 9Net.

Tiragem: 500

Nesta Edição

REVISTA JURÍDICA
DO BANCO DO NORDESTE

Banco do Nordeste