OBSERVATÓRIO DA LGPD
UNIVERSIDADE DE BRASÍLIA

ANÁLISE SETORIAL
IMPACTOS DA LGPD NO BRASIL

ORGANIZADORES

LAURA SCHERTEL MENDES

GIOVANNA MILANESE

PAULO RICARDO DA SILVA SANTANA

SHANA SCHLOTTFELDT

TAYNÁ FROTA DE ARAÚJO

EDUARDA COSTA ALMEIDA

ELIS BANDEIRA A. BRAYNER

ANUÁRIO DO OBSERVATÓRIO DA LGPD DA UNIVERSIDADE DE BRASÍLIA

VOLUME 2

Universidade de Brasília
Faculdade de Direito

Anuário do Observatório da LGPD da Universidade de Brasília

Análise setorial dos impactos da LGPD no Brasil

Volume 2
Brasília-DF
2023

Para esclarecimentos sobre esta obra, entrar em contato com observatorio.lgpd.unb@gmail.com

Volume 2

Organização
Coordenação Geral: prof.ª Laura Schertel Mendes;
Coordenação Adjunta: Giovanna Milanese;
Coordenação de Pesquisa: Paulo Ricardo S. Santana e Shana Schlottfeldt;
Assessores da Coordenação de Pesquisa: Igor M. Caldas Machado, Luís Fernando O. S. Costa, Sayuri Hamaoka e Sofia de M. Vergara;
Revisão e Organização: Eduarda Costa, Elis Bandeira A. Brayner e Tayná Frota de Araújo.

Informações

Observatório da LGPD/Unb
Faculdade de Direito
Universidade de Brasília
Campus Universitário Darcy Ribeiro, CEP: 70.910-900, Brasília-DF, Brasil

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central da Universidade de Brasília – BCE/UNB)

A636 Anuário do Observatório da LGPD da Universidade de Brasília [recurso eletrônico] : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes … [et al.]. – Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v.

Inclui bibliografia. Modo de acesso: World Wide Web.

ISBN 978-65-00-92398-8 (v. 1).

ISBN 978-65-00-92399-5 (v. 2).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Universidade de Brasília. 3. Proteção de dados. 4. Direito comparado. I. Mendes, Laura Schertel (org.).

CDU 34

AUTORES

André Felipe Krepke

Camila Cristina da Silva

Elis Bandeira Alencar Brayner

Gustavo Vieira de Sousa

Igor Marques Caldas Machado

Isabella Maria Farias Carvalho

Lívia Rodrigues Alves

Luis Eduardo de Souza Leite Trancoso Daher

Luís Fernando Oliveira de Souza Costa

Paulo Ricardo da Silva Santana

Rafaella Bacellar Marques

Rodrigo Toledo Costa de Almeida

Sofia de Medeiros Vergara

Tayná Frota de Araújo

Thobias Prado Moura

Wanessa Larissa Silva de Araújo

REVISORES

A realização deste anuário contou com a significativa participação de revisores, que atuaram na avaliação e revisão dos artigos submetidos pelos pesquisadores do Observatório, fornecendo orientações e sugestões de melhoria. Oferecemos nosso mais sincero agradecimento pelas valiosas contribuições de cada um.

Cynthia Picolo

Eduarda Chacon

Eduarda Costa

Felipe Medon

Gabriel Fonseca

Giovanna Milanese

Isabela Maria Rosal

Maria Cristine Lindoso

Matheus Pimenta

Mônica Fujimoto

Rodrigo Silva

Thiago Moraes

SUMÁRIO

APRESENTAÇÃO

É com um forte sentimento de missão cumprida que apresentamos o Volume 2 do Anuário do Observatório da LGPD da Universidade de Brasília (Unb). Esta obra concretiza os resultados de um árduo trabalho de pesquisa acadêmica na temática da proteção de dados. Em uma conjuntura de acirrada vigilância sobre os dados pessoais dos indivíduos, debater a privacidade e a proteção de dados é uma demanda que se impõe. Nesse sentido, o presente anuário se estabelece como uma realização relevante sobre o tema.

O Observatório surgiu em 2021 a partir de uma necessidade de aprofundamento da pesquisa de alta qualidade sobre a proteção de dados. Em 2022, mantivemos a mecânica de funcionamento desde a criação do Observatório, promovendo, para a comunidade acadêmica da Unb, discussões de alto nível em encontros com acadêmicos e profissionais especializados nos mais variados temas relacionados à privacidade e proteção de dados.

A partir de 2022, entendemos que, para atingir nossa missão, seria necessário abrir as portas para membros externos. Foi quando o grupo passou a admitir membros de universidades de todo o país e de diversos níveis acadêmicos. Assim, graduandos, graduados, mestrandos, mestres, doutorandos e doutores trabalharam juntos, comprometidos com um único propósito: elaborar pesquisas de excelência e de relevância para o cenário da proteção de dados no Brasil.

O Volume 1 focou em uma abordagem comparativa da LGPD com o GPDR a partir da análise de casos práticos discutidos na esfera administrativa e judicial, tanto do Brasil quanto da Europa. Por seu turno, o Volume 2 deu continuidade à pesquisa, focando nos avanços da regulação da proteção de dados no Brasil, mas por meio de uma abordagem setorial.

A LGPD representa, sem sombra de dúvidas, um marco legal ímpar para o ordenamento jurídico brasileiro, não só por introduzir uma regulamentação inovadora e atual, mas também por promover um debate social acerca da importância dos dados pessoais em uma sociedade profundamente movida por eles.

Contudo, a proteção de dados precisaria vencer alguns obstáculos após sua publicação: prorrogação de vigência de parte da norma, estruturação da Autoridade Nacional de Proteção de Dados (ANPD), expedição de regulamento de fiscalização, etc. Em certa medida, tudo era novo, gerando impacto no mercado e em diversos setores da sociedade, muito em razão da

necessidade de compreender o novo diploma, o papel do novo agente regulador e como se daria o processo de adequação.

Partindo desse cenário, a abordagem setorial do Volume 2 se revela um mecanismo poderoso para compreender a jornada da proteção de dados no Brasil a partir da organização de um panorama sobre as normas, regulamentos, decretos e correlatos produzidos para importantes setores econômicos e sociais: financeiro, saúde, transportes etc.

Este Volume encerra um capítulo essencial na trajetória do Observatório da LGPD da Unb. Neste encerramento, não podemos deixar de agradecer aos autores, pelo comprometimento e empenho para produzir cada artigo desta obra. Agradecemos ainda aos revisores, que aceitaram o desafio de participar do projeto, oferecendo significativas contribuições, por meio de revisões, sugestões de melhoria e aperfeiçoamento dos artigos elaborados. E, por fim, um agradecimento aos organizadores – coordenadores e assessores - que atuaram com persistência e dedicação, mesmo diante das adversidades, para que este anuário pudesse sair do papel.

Aos leitores, desejamos que esta obra os inspire a pensar e a construir uma proteção de dados cada vez mais sólida e capaz de enfrentar os desafios que a sociedade da vigilância impõe.

Brasília, 1º de dezembro de 2023

Laura Schertel Mendes[1]

Giovanna Milanese[2]

Paulo Ricardo da Silva Santana[3]

[1] Coordenadora Geral do Observatório da LGPD da Universidade de Brasília
[2] Coordenadora Geral Adjunta do Observatório da LGPD da Universidade de Brasília
[3] Coordenador de Pesquisa do Observatório da LGPD da Universidade de Brasília.

PROTEÇÃO DE DADOS PESSOAIS E O UNIVERSO DA SAÚDE: INTERSEÇÕES E DESAFIOS

André Felipe Krepke[1]

Resumo: A chegada da proteção de dados a várias áreas continua demandando uma contínua análise conjunta da lei e demais orientações, guias, e recomendações de órgãos especializados. Dentro da área da saúde não se mostrou diferente. Nesse sentido o presente artigo busca compreender, partindo de uma visão jurídica, das interseções entre a Lei Geral de Proteção de Dados e orientações setoriais na saúde. Buscou-se, mediante uma análise qualitativa dos documentos apresentados, compreender como agentes de tratamento devem compreender o conceito de saúde na proteção de dados. Para tanto foram observadas as definições de dados pessoais e dados pessoais sensíveis, seguidas de suas bases legais aplicáveis a saúde. Logo após foram pormenorizadas questões relativas aos agentes de tratamento. Por último observou-se os reflexos da lei sobre o contexto da pesquisa científica.

Palavras-chave: saúde; dados sensíveis; proteção de dados; lei geral de proteção de dados

Abstract: *The arrival of data protection in various areas continues to demand a continuous joint analysis of the law and other guidelines, guides, and recommendations from specialized entities. Within the health area, it was no different. In this sense, this article seeks to understand, from a legal point of view, the intersections between the General Data Protection Law and sectorial guidelines in health. We sought, through a qualitative analysis of the documents presented, to understand how treatment agents should understand the concept of health in data protection. For this reason, the definitions of personal data and sensitive personal data were observed, followed by their legal bases applicable to health. Soon after, questions related to treatment agents were detailed. Finally, the effects of the law on the context of scientific research were observed.*

[1] Mestrando em Direito e Inovação no PPGD da UFJF. Pesquisador do NEAPID. Bolsista no Núcleo de Inovação Tecnológica da UFJF.

Keyworsds*: *health; sensible data; data protection; general data protection law

Introdução

Proteger as informações, permitindo ao mesmo tempo seu fluxo para a continuidade das mais variadas atividades, tem sido um dos desafios da atualidade. Uma das causas está na maior informatização da vida, com a melhoria tanto quantitativa do processamento, permitindo quantidades cada vez maiores de banco de dados, bem como qualitativa, mediante a adoção de métodos e técnicas com resultados mais valiosos[2].

A necessidade de reformular, frente a essas mudanças, rotinas de trabalho, mentalidade de colaboradores, cláusulas contratuais e a atualização constante de computadores já é rotina em alguns locais, fruto da lenta, porém contínua e crescente influência da Lei Geral de Proteção de Dados em todos os setores, não sendo diferente na área da saúde.

Desde o diagnóstico de determinada doença, da prescrição medicamentosa, até a conversa entre médico (a) e paciente há a presença dos dados de saúde, abarcando assim uma grande quantidade de situações, as quais precisam ser alcançadas pela temática da proteção de dados.

Para tanto, nesse texto analisaremos como a Lei Geral de Proteção de Dados (LGPD) tem sido interpretada no campo da saúde, voltando nosso olhar, principalmente, para o diálogo entre os estudos jurídicos e os materiais produzidos pelos entes responsáveis do campo da saúde, no contexto brasileiro. O estudo buscará priorizar conclusões aplicáveis tanto ao setor público quanto ao privado, distinguindo as especificidades quando necessário.

O presente artigo tomou como ponto de partida normas, guias regulamentares e cartilhas publicadas desde 2019 até o início de 2023. Desta forma há uma análise documental e bibliográfica sobre o tema, conjuntamente com uma perspectiva qualitativa dos documentos e artigos selecionados.

[2] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 150-151.

1. Tratamento de dados pessoais na atividade de saúde

Tratar dados pessoais hoje necessariamente passa pelo estudo da LGPD, vigente desde 2020 no Brasil. Fruto de intensos debates e anos de tramitação, essa legislação preza pelo fluxo informacional dentro de determinados parâmetros, colocando em seus fundamentos tanto a autodeterminação informativa e o livre desenvolvimento da personalidade (art. 2º, incisos II e VII), como desenvolvimento econômico e inovação (art.2°, VI).

Carregando consigo toda uma principiologia e novos conceitos, ela chega ao nosso sistema nos apresentando uma forma mais protetiva e justa para tratar dados pessoais. Justamente por seu caráter abrangente, vários setores da sociedade devem compreendê-la e internalizá-la.

No campo da saúde, inicialmente, devemos nos deter a um primeiro conceito da lei: dados pessoais e dados pessoais sensíveis. O primeiro é definido no art. 5º, inciso I, como toda "informação relacionada a pessoa natural identificada ou identificável", abarcando, assim, tanto informações que identificam imediata quanto mediatamente um indivíduo, como o nome, estado civil, CPF, número de telefone e endereço residencial. O segundo, por sua vez, não é necessariamente conceituado, mas exemplificado pela LGPD no art. 5º, inciso II, como informações de origem racial, étnica, opinião política, filiação a sindicato, convicção religiosa, saúde ou vida sexual, genético ou biométrico.

A chave de interpretação dessa categoria reside no princípio da não-discriminação[3], presente no art. 6º, IX, vedando tratamentos para fins discriminatórios ilícitos e abusivos, decorrente do risco às liberdades e direito fundamentais em tratamentos inadequados. Contudo, essa conceituação nos leva a ir além do rol taxativo da norma, reconhecendo outras situações assimétricas, decorrentes de estigmas históricos e situações estruturais presentes na sociedade, as quais são responsáveis por privilegiar, indevidamente, determinadas qualidades e condições em detrimento de outras[4].

Outro ponto para o tratamento de dados sensíveis está no papel do contexto. Um dado não sensível pode ser utilizado para práticas discriminatórias, bem como um dado sensível pode

[3] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p.451.
[4] TEFFÉ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco, 2022.

ser utilizado para um propósito legítimo[5]. O prenome ou sobrenome pode inferir a nacionalidade ou etnia ou mesmo uma tatuagem pode indicar uma convicção religiosa ou política. Dessa forma, "nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou pelas outras informações às quais tem sido associada"[6].

Pelo risco inerente a essa categoria a LGPD possui algumas alterações quanto à forma de tratamento desses dados. Cada uma dessas mudanças, quando comparadas aos dados "gerais", são importantes para o campo da saúde.

Uma das principais orientações são as bases legais. Elas são a justificativa para o tratamento de dados, tornando-o lícito perante o ordenamento. Desta forma qualquer atividade que maneje dados deve encontrar sua finalidade em uma delas. O art. 7º apresenta dez incisos, abarcando possibilidades tanto a agentes de tratamento público quanto privados. Já o art. 11 da lei traz aquelas aplicáveis aos dados sensíveis, em dois incisos, sendo o II subdividido em 7 alíneas. Essa separação é importante na medida em que: i) algumas se repetem, ii) algumas se repetem, porém são adaptadas, iii) outras não se repetem e permanecem adstritas à sua categoria. Nesse sentido é de suma importância identificar qual tipo de dados estamos tratando e ao mesmo tempo não reproduzir de maneira acrítica os procedimentos entre eles.

Dentro do contexto de hospitais, consultórios, prontuários, formulários, bem como em estudos por órgãos de pesquisa, há uma gama de dados e situações que se enquadram em cada um dos artigos e incisos. Assim, é mister não agrupar todos os casos como sensíveis apenas por estarem em um estabelecimento que tenha por finalidade a saúde de pacientes. Logo, para exercer a tutela da saúde não necessariamente trataremos somente dados sensíveis, mas também os considerados "gerais".

Outras disposições, importantes para a saúde, estão nos artigos 7º, VII e 11, II, f, bem como o art. 13, tratando, respectivamente, da tutela da saúde e disposições sobre os estudos de saúde pública. Ambos são relevantes à medida que existem constantes compartilhamentos de

[5] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon, 2019. *Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade*. 2019. 119 f. Dissertação (Mestrado) – Curso de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora. p. 49. Disponível em: https://bit.ly/3kHzLxS. Acesso em: 21 fev. 2023.

[6] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância: a privacidade hoje*. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Renovar, Rio de Janeiro, 2008. p. 77.

dados entre operadoras e prestadores de serviços de saúde e são utilizados dados para contribuir em pesquisas.

2. Bases legais aplicáveis ao tratamento de dados pessoais para a saúde

Na aplicação das bases legais, o "Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços de Saúde" do Conselho Nacional de Saúde destaca[7] que antes mesmo da efetiva coleta dos dados sensíveis em uma consulta temos a chegada do paciente, no chamado protocolo de atendimento, onde se fornecem dados cadastrais. Aqui temos situações em que é possível tanto a coleta de dados sensíveis quanto não sensíveis, demandando atenção quanto a cada um deles para efetivo cumprimento das disposições da LGPD.

Uma das bases a se ter atenção em todas as etapas é o consentimento, justamente por estar presente nas duas categorias (arts. 7º e 11), mas apresentar distinção quanto à sua forma de obtenção.

O termo consentimento é definido pela lei no art. 5º como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Trata-se de uma das formas legítimas de tratamento de dados, ligada intrinsicamente a um dos fundamentos da LGPD, qual seja, a autodeterminação informativa. Nesse sentido, para fornecer o dado ao agente de tratamento, não devem restar dúvidas ao titular sobre como os dados são tratados e, diante dos esclarecimentos, ele(a) decide prosseguir com a relação jurídica.

O consentimento ainda deve ser obtido por escrito ou por forma capaz de demonstrar a obtenção deste, conforme art. 8º da LGPD, bem como deve ser específico ao tratamento, impedindo manifestações genéricas (art.8º, §4º). Se estivermos diante de dados pessoais sensíveis, e aqui não só aqueles diretamente ligados a questões de saúde, o consentimento ganha mais uma qualificadora: é necessário destacar ao titular o dado sensível em questão entre todos os demais e se ele(a) concorda com o tratamento destes para os fins determinados, conforme art. 11, I.

[7] CONSELHO NACIONAL DE SAÚDE. *Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde.* 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf, p.48 Acesso em: 14 fev. 2023.

Outro ponto relativo ao consentimento está no privilégio que dão a essa base legal em detrimento das demais. Justamente pelo maior protagonismo dado aos titulares pela lei e pela possibilidade de sua revogação unilateral, ela é alçada a patamares muito elevados. Contudo, o que se tem percebido é o nivelamento em importância entre as bases legais do art. 7º, pois cada uma delas é apta a legitimar o tratamento de dados, colocado por alguns como o "fim da cultura do consentimento"[8].

Algumas das orientações de entidades ligadas a saúde, contudo, entendem por centralizar o consentimento no debate, especialmente quanto aos dados sensíveis. É o caso da Cartilha da Agência Nacional de Saúde Suplementar (ANS), versão 2020, e a Cartilha do Conselho Federal de Medicina (CFM), versão 2022, os quais apresentam uma perspectiva introdutória e educativa da proteção de dados aos profissionais da saúde.

A cartilha da ANS destaca em determinado ponto: "a palavra é: consentimento", colocando-o em destaque, quando comparado com as demais bases[9]. Já a Cartilha do CFM intitula determinado capítulo como "o necessário 'consentimento' como regra geral para o tratamento de dados pessoais"[10].

Outra importante contribuição que defende esse posicionamento é a Nota Técnica Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES[11] da ANS. Nela se consubstanciam importantes orientações da Agência no tema e, em determinados pontos do documento, ela dispõe que "a regra geral é a vedação do tratamento de dados pessoais sem o expresso consentimento do titular ou de seu responsável legal, no caso do incapaz"[12]. A nota técnica aprofunda sobre as possibilidades de dispensa de consentimento, chamando-as de exceções, as quais são elencadas[13] pela Agência.

---

[8] OLIVEIRA, Caio César de. TAVARES FILHO, Paulo César. A LGPD e o início do fim da cultura do consentimento. *Jota*. 28 jun. 2021. Disponível em: https://bit.ly/3usiz43. Acesso em: 22 fev. 2023.

[9] AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. *LGPD: informações básicas para entender a Lei Geral de Proteção de Dados Pessoais*. Rio de Janeiro, 2021. Disponível em: cartilha_lgpd_r2.pdf (www.gov.br). Acesso em: 13 fev. 2023.

[10] CONSELHO FEDERAL DE MEDICINA. *LGPD: a Lei Geral de Proteção de Dados Pessoais e a atuação do profissional da medicina*. Brasília, 2022. p.18 Disponível em: https://www.flip3d.com.br/pub/cfm/index9/?numero=38&edicao=5305. Acesso em: 7 fev. 2023.

[11] AGÊNCIA NACIONAL DE SAÚDE. *NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES*. Processo SEI nº 33910.029786/2019-51. 2019. Disponível em: http://cnsaude.org.br/wp-content/uploads/2020/10/Nota_Tecnica_LGPD_ANS_CNSAUDE.pdf. Acesso em: 08 fev. 2023.

[12] AGÊNCIA NACIONAL DE SAÚDE. Ibid. p. 6

[13] São destacadas várias hipóteses, como o envio, pelas operadoras de planos privados à ANS, dos dados de cadastros de beneficiários do Sistema de Informações de Beneficiários; o compartilhamento do DATASUS com a ANS das bases de dados do Sistema de Informações Hospitalares (SIH) e do Sistema de Informações

O próprio Código de Boas Práticas do CNS apresenta entendimento nesse sentido. Dentro do tema de compartilhamento de dados entre estabelecimentos de saúde e operadoras ele enfatiza:

> É importante notar, ainda, que a Lei Geral de Proteção de Dados trouxe uma regra especial quanto ao tratamento de dados pessoais sensíveis no seu art. 11, privilegiando o uso do consentimento em detrimento das demais bases legais da lei. Isto porque o legislador, ciente da importância e da criticidade deste tipo de informações, privilegiou a transparência e a informação ao titular dos dados em relação ao uso dos seus dados.
>
> Portanto, ao realizar o tratamento de dados pessoais sensíveis, os agentes de tratamento devem privilegiar a obtenção do consentimento (quando não for a hipótese de dever regulatório acima exposto), oportunizando o paciente a ciência quanto ao uso dos seus dados. O uso de outras bases legais, conforme observado o inciso II do art. 11 é via de exceção e os agentes de tratamento deverão comprovar a indispensabilidade do tratamento, que deverá tomar por base os princípios da lei e o interesse do paciente.[14]

Essa linha interpretativa observa a disposição das bases legais dos dados sensíveis. O consentimento ocupa sozinho o inciso I do art.11, enquanto as demais se subdividem em alíneas do inciso II, o qual ainda as vincula a indispensabilidade dessas informações. Essa disposição topográfica geraria uma aparente preferência legislativa.

Contudo, ao longo dos anos as leis de proteção de dados no mundo caminharam para um "refratário protagonismo do consentimento"[15], movimento que não retira o titular do centro, mas relembra demais interesses legítimos quando do fluxo de informações; ao mesmo tempo a técnica legislativa do art. 11 não apresenta uma hierarquia, mas uma posição de igualdade entre as hipóteses[16]. Assim, em que pese as orientações técnicas, entende-se o consentimento como uma base importante, porém não prioritária[17].

Ambulatoriais (SAI) para processamento do ressarcimento ao SUS, e do Cartão Nacional de Saúde (CNS), para enriquecimento e melhoria da qualidade dos cadastros de beneficiários; e o compartilhamento de registros de saúde com os médicos assistentes e outros prestadores de serviços de saúde para melhorar o cuidado e o resultado em saúde para o paciente; Ibid, p.7-8.

[14] CONSELHO NACIONAL DE SAÚDE, op. cit. p.92.

[15] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais – As funções e os limites do consentimento*. 3ª ed. Rio de Janeiro: Forense. 2021, p.133.

[16] MULHOLLAND, Caitlin. Dados pessoais sensíveis e o consentimento na Lei Geral de Proteção de Dados Pessoais. *Revista do Advogado*, n.144, nov. 2019, p. 47-53, p.52.

[17] Também nesse sentido TEFFÉ, op.cit. p.151-159.

As demais circunstâncias de tratamentos demandam novamente identificar se estamos diante de dados não pessoais a serem utilizados para a prestação de serviços de saúde, ou se estamos lidando com dados sensíveis de saúde, ao mesmo tempo discriminando quem são os agentes de tratamento.

Se estivermos diante de preenchimentos de formulários, fichas cadastrais, entende-se por se utilizar primordialmente as bases legais do art. 7º e, quando houver dados sensíveis, o art. 11. O Código de Boas Práticas da ANS ratifica o contexto[18] e o princípio da finalidade como importantes balizas. Desse modo, as informações colhidas na recepção de um hospital são diferentes daquelas compartilhadas durante a consulta com o/a profissional da saúde. Na primeira podemos enxergar tanto as bases legais do consentimento (art. 7º, I), cumprimento de obrigação legal (II) quanto a execução do contrato (V). Já na conversa entre médico e paciente, somado ao feitio do prontuário médico[19], deve observar a efetiva tutela da saúde (art.11, II, f), o consentimento em destacado quando for aplicável (art.11, I) bem como outras hipóteses adequadas ao caso.

Profissionais da saúde devem ser orientados de que não há revogação das disposições dos Códigos de Ética Médica ou outras normas aplicadas às categorias profissionais devido a vigência da LGPD. Assim, a aplicação das bases legais não implica em desconsiderar, por exemplo, o sigilo dos prontuários, muito pelo contrário. Uma das disposições, o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II e art. 11, II, a), aplica-se à guarda dos prontuários médicos físicos e digitais pelo prazo de 20 anos contados do último registro estabelecido em lei[20].

A convergência dessas normas não implica em renúncia de algumas delas, pois cada uma permanece com suas atribuições e contribuem para a formação de um ambiente mais seguro para os dados pessoais. Diante disso profissionais e estabelecimentos da saúde devem conjugar as normativas já conhecidas com a disposição da LGPD.

[18] O termo "contexto" é citado em praticamente todos os temas referentes às bases legais no Código de Boas Práticas.
[19] Conforme art.1º da Resolução nº 1.638/02 define-se prontuário médico "como o documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo".
[20] Conforme art.6º da Lei 13.787/2018: "Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados".

Isso pode vir, desta forma, a atrair mais de um tipo de responsabilidade aos agentes, respondendo tanto a processos disciplinares nos conselhos de classe; administrativos junto à Autoridade Nacional de Proteção de Dados; e também judiciais, frente a possibilidade de responsabilização civil pelo tratamento ilícito de dados, causando danos a titulares, conforme art. 42 da LGPD[21].

Outra importante situação a ser elencada é a "tutela da saúde", previsto no art. 7º, VIII e no art. 11, II, alínea "f". Trata-se da única base legal com o termo explícito "saúde". Nela ainda há uma condicionante subjetiva para sua utilização: somente "profissionais de saúde, serviços de saúde ou autoridade sanitária". Certos pontos devem ser destacados aqui.

Em primeiro lugar está a indefinição do conceito de "tutela da saúde" pela lei. O que poderia ou não ser considerado nesses termos? Para tanto o Código de Boas Práticas do CNS orienta[22] seguir o Regulamento Geral de Proteção de Dados europeu (GDPR) nos arts. 9(2)(h) e art. 9(3), separando os casos em atividades de medicina preventiva, chamadas de atividades fim pelo Código do CNS, e pelos casos em que há profissionais sujeitos à obrigação de sigilo. Na dicção da lei:

> Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3; (...)
>
> 3. Os dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.

[21] 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.
[22] CONSELHO NACIONAL DE SAÚDE. op.cit. p.17-18.

A perspectiva do sigilo e guarda/manuseio de documentos não é nova no campo da saúde. O Código de Ética Médica dispõe, nos artigos 73 a 79, sucessivas proibições quanto a revelação de sigilo profissional, resguardando pacientes de indevidas exposições. Algumas possuem a revelação condicionada, como as informações de exames médicos de trabalhadores que só podem ser apresentadas quando houver risco à saúde dos empregados ou da comunidade (art. 76). Por outro lado, há situações de sigilo absoluto, quanto à "referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos, em meios de comunicação em geral, mesmo com autorização do paciente" (art. 75).

Outra contribuição quanto a compreensão dessa base está na Nota Técnica 3/2019 da ANS, anteriormente citada. Nela a Agência destaca dois termos: "serviços de saúde" e "autoridade sanitária". Ambos não estavam nas primeiras versões quando do projeto de lei, mas foram inseridas pela Lei nº 13.853/2019.

No entendimento da ANS a adição dos serviços de saúde contemplou "gestores públicos e privados de saúde, como as operadoras de planos privados de assistência à saúde, não apenas no atendimento assistencial, mas também na gestão do cuidado"[23], enquanto a inclusão de "autoridade sanitária" indica que "não se limita à tutela da saúde individual, alcançando também a saúde pública"[24].

3. Definição dos agentes de tratamento no campo da saúde

Uma das situações mais complexas a serem consideradas quando do tratamento de dados de sensíveis relativos à saúde, ou qualquer dado para a prestação de serviços de saúde, é definir quem serão os controladores e operadores na relação jurídica. Se deve essa constatação frente a grande cadeia de agentes ao longo do processo, característica muito presente em outros setores da sociedade.

A definição legislativa do operador é, conforme art. 5º, VI, a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", enquanto o operador é, no inciso VI, a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

[23] AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. NOTA TÉCNICA. op.cit, p.8.
[24] Ibid.

No campo da saúde, como inicialmente destacado no artigo, há prestadores de serviços de saúde, profissionais sujeitos ao sigilo profissional, laboratório e farmácias, adicionando aqui as agências e conselhos, como a Agência Nacional de Saúde Suplementar, a Agência Nacional de Vigilância Sanitária e o Conselho Federal de Medicina.

Cada um deles possui objetivos e atribuições distintas sobre os dados dos titulares frente a cada situação, permitindo concluir que agrupar todas as situações em regra única pode gerar incerteza no momento da aplicação da norma. Algumas balizas, contudo, podem ser analisadas para evitar problemas na definição das posições.

A primeira é quando há um mesmo dado ou base de dados cuja as finalidades são definidas por um ou mais controladores. Essa possibilidade é chamada de controladoria conjunta e está definida no "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado", publicado pela Autoridade Nacional de Proteção de Dados (ANPD). Segundo o Guia, é a

> determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD.[25]

Pode-se ter mais nitidez de como ela funciona nos casos de compartilhamento de dados apresentados pelo Código de Boas Práticas do CNS[26]: quando dois profissionais da saúde, sujeitos ao sigilo profissional, trocam informações sobre determinado paciente, com finalidades de tutela da saúde deste, mas com áreas de conhecimento distintas, ou quando uma pesquisa clínica realiza coleta de dados e há uma plataforma utilizada para análise dos resultados, a qual possui suas finalidades quanto aos mesmos dados.

A segunda baliza está em não tornar a posição de determinado agente como estanque, pois enquanto um estabelecimento de saúde pode figurar como controlador quanto ao paciente,

[25] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. V. 2.0. Brasília. Abr. 2022. p.14. Disponível em: https://bit.ly/3z2N5pk. Acesso em: 23 fev. 2023.

[26] Ambos os casos são adaptações dos exemplos trazidos nas páginas 78-79 e 122. CONSELHO NACIONAL DE SAÚDE, op.cit. p. 78-79, 122.

pode se tornar operador ou co-controlador frente a Agência Nacional de Saúde, quando esta solicitar dados de saúde, utilizando a base de cumprimento de obrigação legal ou regulatória[27].

A terceira é não confundir prepostos e agentes do controlador como agentes de tratamento. Assim, na repartição de funções em um hospital, pessoas naturais que exercem as atividades conforme as orientações daquela e expressam seus objetivos não são controladores ou operadores[28], analisando sempre o contexto para se chegar a conclusões diversas.

Por último deve ser levada em conta a questão fática, segundo a ANPD, quando da definição dos papeis. Esse ponto é relevante na medida em que por mais que sejam estabelecidos em contrato controladores e operadores, caso algum operador comece a definir finalidades essenciais de um tratamento, poderá ser considerado controlador. Nas palavras da ANPD

> A identificação do controlador deve partir do conceito legal e dos parâmetros auxiliares indicados neste Guia, sempre considerando o contexto fático e as circunstâncias relevantes do caso. O papel de controlador pode decorrer expressamente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Não obstante, a efetiva atividade desempenhada por uma organização pode se distanciar do que estabelecem as disposições jurídicas formais, razão pela qual é de suma importância avaliar se o suposto controlador é, de fato, o responsável pelas principais decisões relativas ao tratamento.[29]

4. Pesquisas na área da saúde

O último tópico referente ao tratamento de dados nessa área é sobre as pesquisas. Mais uma vez necessário diferenciar quando tratamos dados sensíveis ou "gerais" para essa finalidade.

É destacado o papel central dos órgãos de pesquisa enquanto agentes de tratamento aptos a utilizarem essas bases. Sua definição está no art.5º, XVIII como

> 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

[27] CONSELHO NACIONAL DE SAÚDE, op.cit.. p.89.
[28] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, op. cit. p.9.
[29] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo*. p.8.

> objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

A ANPD, em estudo preliminar sobre o tema, aponta a necessidade de o órgão possuir, na sua missão institucional, a pesquisa básica ou aplicada para fins históricos, científicos, tecnológicos ou estatísticos[30].

Ainda sobre a definição de órgão de pesquisa, a autoridade entende pela impossibilidade de uso dessas bases por pessoas jurídicas de direito privado com fins lucrativos devido a definição legal, orientando-as a utilizar outras hipóteses como o consentimento e o legítimo interesse[31].

A regulamentação da pesquisa, contudo, não deve observar apenas a LGPD, mas sim todo um contexto regulatório e histórico[32] por trás desse sistema.

Para empreender estudos em seres humanos é necessário passar pelo sistema CEP/Conep, quando o Conselho de Ética em Pesquisa local é consultado e, ao observar as normas e orientações dadas pelo Conselho Nacional de Ética em Pesquisa, decide se determinado protocolo de pesquisa pode ser iniciado.

Como regulamentações importantes para a matéria cite-se a Resolução CNS nº 466/12 e a Resolução CNS nº 510/16, a primeira trazendo as principais definições e normas gerais, enquanto a segunda se especifica aos estudos em ciências humanas e sociais.

Um dos aspectos primordiais para a iniciar a pesquisa é o recolhimento do Termo de Consentimento Livre e Esclarecido, ou TCLE. Nele devem estar contidas várias, se não todas as informações sobre a pesquisa que será realizada, tornando todos os pontos nítidos. Nele, "além de explicar os detalhes da pesquisa (justificativa, objetivos, procedimentos, desconfortos, riscos, benefícios, grupos pesquisados, etc), também deve informar e assegurar os direitos dos participantes"[33]. O consentimento aqui não necessariamente será o mesmo da base legal, uma vez que estamos diante de normas distintas. Dessa forma, conforme a ANPD, "é plenamente

[30] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Estudo Técnico A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa.* Brasília, abril 2022. p.15.
[31] Ibid. p.15.
[32] Sobre a construção da bioética, a qual exerce influência sobre as pesquisas em humanos, confira-se: MARINI, Bruno. O eugenismo, o holocausto e o Código de Nuremberg como antecedentes do surgimento da bioética e do biodireito. *Magis*. 18 fev. 2023. Disponível em: https://magis.agej.com.br/o-eugenismo-o-holocausto-e-o-codigo-de-nuremberg-como-antecedentes-do-surgimento-da-bioetica-e-do-biodireito/. Acesso em: 21 fev. 2023.
[33] BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Comissão Nacional de Ética em Pesquisa. *Cartilha dos Direitos dos Participantes de Pesquisa - Versão 1.0*. Brasília: CONEP/CNS/MS, 2020.

possível que o consentimento seja dispensável do ponto de vista da legislação de proteção de dados pessoais e necessário do ponto de vista ético."[34]

Outro aspecto, quanto a pesquisa na saúde, deve ser observado: a adoção de processos de anonimização ou pseudoanonimização. Apesar da anonimização e pseudoanonimização dizerem respeito não só aos dados sensíveis, entendeu o legislador por colocá-las dentro da Seção II da lei. Essas são medidas de segurança, onde o dado perde total (art. 5º, XI e art. 12), ou parcialmente (art. 13, §4º) sua ligação com o titular, impedindo sua identificação. Esse estímulo[35], conforme art. 7º, IV e art. 11, II, c, demonstra o balanceamento da lei, tanto na valorização do conhecimento com os melhores resultados nas pesquisas, com a proteção das garantias fundamentais dos participantes.[36]

Considerações Finais

A proteção de dados tornou-se matéria a ser estudada nos vários campos da sociedade, uma vez que todas as atividades voltadas a pessoa humana precisam, em algum momento, tratar dados pessoais para sua continuidade. Uma dessas áreas é o setor de saúde.

A chegada da LGPD nesse campo demanda não só uma análise do ponto de vista dogmático, mas de uma interseção e diálogo entre direito, saúde e segurança da informação, a fim de garantir a contínua prestação de serviços a pacientes, conferindo maior qualidade de vida, bem como a segurança nas pesquisas para alcançar o melhor resultado, preservando o sigilo de seus participantes.

Dessa forma foram apresentadas as principais intersecções da Lei Geral de Proteção de Dados com os preceitos da saúde a partir da análise não só de textos jurídicos, mas das próprias recomendações publicadas por Conselhos e Agências diretamente ligados à área da saúde.

Discutiu-se como e quais dados pessoais são possivelmente tratados dentro desse meio. Posteriormente foram elencadas as bases legais aplicáveis aos principais casos. Em seguida foram debatidos alguns reflexos das definições de agentes de tratamento dentro do campo da

[34] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Estudo Técnico. op.cit. p.14.
[35] A ANPD não entende o termo "sempre que possível", presente nos arts.7º, IV e art.11, II, "c", como uma obrigação ou pré-requisito para a pesquisa, mas que sim como uma forma de demonstrar a necessidade de meios aptos a proteger, conforme o contexto, os participantes da pesquisa. Ibid. p. 16-17.
[36] DONEDA, D.; LIMA BARRETO, M.; ARAÚJO ALMEIDA, B. de. Uso e proteção de dados pessoais na pesquisa científica. Direito Público, [S. l.], v. 16, n. 90, 2019. p.189 Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3895. Acesso em: 24 fev. 2023.

saúde e, por último, foram destacadas repercussões sobre os estudos realizados por órgãos de pesquisa.

É certo que o debate irá continuar para além dessas normas, conforme novas tecnologias e situações demandem ora outros caminhos para resolução de desafios na saúde, ora recorrendo aos princípios e valores sedimentados tanto na proteção de dados quando nas regulamentações setoriais já existentes.

Referências bibliográficas

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. LGPD: informações básicas para entender a Lei Geral de Proteção de Dados Pessoais. Rio de Janeiro, 2021. Disponível em: cartilha_lgpd_r2.pdf (www.gov.br). Acesso em: 13 fev. 2023.

AGÊNCIA NACIONAL DE SAÚDE. *NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES*. Processo SEI nº 33910.029786/2019-51. 2019. Disponível em: http://cnsaude.org.br/wp-content/uploads/2020/10/Nota_Tecnica_LGPD_ANS_CNSAUDE.pdf. Acesso em: 08 fev. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. V. 2.0. Brasília. Abr. 2022. p.14. Disponível em: https://bit.ly/3z2N5pk. Acesso em: 23 fev. 2023.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais – As funções e os limites do consentimento*. 3ª ed. Rio de Janeiro: Forense. 2021.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Comissão Nacional de Ética em Pesquisa. *Cartilha dos Direitos dos Participantes de Pesquisa - Versão 1.0*. Brasília: CONEP/CNS/MS, 2020.

CONSELHO FEDERAL DE MEDICINA. LGPD: a Lei Geral de Proteção de Dados Pessoais e a atuação do profissional da medicina. Brasília, 2022. Disponível em: https://www.flip3d.com.br/pub/cfm/index9/?numero=38&edicao=5305. Acesso em: 7 fev. 2023.

CONSELHO NACIONAL DE SAÚDE. Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde. 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 14 fev. 2023

DONEDA, D.; LIMA BARRETO, M.; ARAÚJO ALMEIDA, B. de. Uso e proteção de dados pessoais na pesquisa científica. Direito Público, [S. l.], v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3895. Acesso em: 24 fev. 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados e suas repercussões*

no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon, 2019. *Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade*. 2019. 119 f. Dissertação (Mestrado) – Curso de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora. p. 49. Disponível em: https://bit.ly/3kHzLxS. Acesso em: 21 fev. 2023.

MARINI, Bruno. O eugenismo, o holocausto e o Código de Nuremberg como antecedentes do surgimento da bioética e do biodireito. *Magis – Portal Jurídico*. 18 fev. 2023. Disponível em: https://magis.agej.com.br/o-eugenismo-o-holocausto-e-o-codigo-de-nuremberg-como-antecedentes-do-surgimento-da-bioetica-e-do-biodireito/. Acesso em: 21 fev. 2023.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e o consentimento na Lei Geral de Proteção de Dados Pessoais. *Revista do Advogado*, n.144, nov. 2019, p. 47-53.

OLIVEIRA, Caio César de. TAVARES FILHO, Paulo César. A LGPD e o início do fim da cultura do consentimento. *Jota*. 28 jun. 2021. Disponível em: https://bit.ly/3usiz43. Acesso em: 22 fev. 2023.

RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância: a privacidade hoje*. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Renovar, Rio de Janeiro, 2008.

TEFFÉ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco, 2022.

APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO SISTEMA FINANCEIRO NACIONAL

Camila Cristina da Silva[1]

Resumo: A privacidade percorreu uma longa trilha metamórfica no último século, influenciada e moldada pelo avanço tecnológico, associando-se a outras relevantes questões modernas, como a proteção de dados financeiros e bancários. Nessa senda, o objetivo do presente artigo é investigar a regulamentação do Sistema Financeiro Nacional, por meio da análise dos normativos do Banco Central (BACEN) e do Conselho Monetário Nacional (CMN), especialmente a Resolução n° 4.658/2018, à luz da Lei Geral de Proteção de Dados (LGPD). Abordou-se, especialmente, a recente inovação financeira do *open banking*, regulamentada pela Resolução BCB n° 32 de 29/10/2020. Utilizou-se do levantamento bibliográfico, especificamente com o uso de obras e autores consolidados academicamente na área jurídica de proteção de dados pessoais no Brasil e, para o tema *open banking*, foram extraídas referências publicadas em revistas diretamente do repositório de artigos científicos da CAPES. A análise revela a evidente preocupação dos atores financeiros governamentais brasileiros em se adequarem à Lei n° 13.709/2018, impondo uma série de regulamentações para garantir que as instituições privadas também sigam as diretrizes da LGPD, inclusive diante dos novos modelos de negócio oriundos do reflexo do avanço tecnológico sobre o sistema financeiro brasileiro.

Palavras-chave: Privacidade. Proteção de Dados Pessoais. Sistema Financeiro Nacional. Sistema Financeiro Aberto. Open Banking.

Abstract: *Privacy has gone through a long metamorphic path in the last century, influenced and shaped by technological advances, associating itself with other relevant modern issues, such as the protection of financial and banking data. In this regard, the aim of this article is to*

[1] Bacharelanda em Direito na Universidade de Brasília (UnB). Pesquisadora e assistente no Observatório da LGPD, coordenado pela professora-doutora Laura Schertel.

investigate the regulation of the National Financial System, through the analysis of the regulations of the Central Bank (BACEN) and the National Monetary Council (CMN), specially the Resolution No. 4.658/2018, in the light of the General Data Protection Law (LGPD). The recent financial innovation of open banking, regulated by BCB Resolution No. 32 of 10/29/2020, was addressed in particular. Bibliographical survey was used, specifically with the use of academically consolidated works and authors in the legal area of personal data protection in Brazil and, for the theme open banking, references published in journals extracted directly from the CAPES repository of scientific articles. The analysis reveals the evident concern of brazilian government financial actors to adapt to Law No. 13,709/2018, imposing a series of regulations to ensure that private institutions also follow the LGPD guidelines, including in the face of new business models arising from the reflection of the technological advances on the Brazilian financial system.

Keywords: *Privacy. Data Protection. National Financial System. Open Financial System. Open Banking.*

Introdução

A noção de privacidade pressupõe uma vida privada a ser protegida[2], por conseguinte, remonta a diversas civilizações e épocas da História humana. Contudo, nem sempre se tratou de uma questão jurídica a ser tutelada. É inerente à modernidade a inquietação com os limites da privacidade[3]. Primordialmente, era indissociável do conhecido *right to be let alone*, comumente difundido como "direito de ser deixado só", lançado ao mundo pelo consagrado artigo norte-americano do fim do século XIX - *The right to privacy* - de Brandeis e Warren[4]. Havia uma estreita relação entre o direito à privacidade e o isolamento da sociedade. Inegável, nessa senda, que o nascimento da privacidade se deu em um contexto particularmente individualista. Outrossim, ela não permanece estática em seu berço, pois amadurece, dinâmica, rumo a caminhos inimagináveis.

A complexificação tecnológica promoveu procedimentos sofisticados que, progressivamente, utilizaram e utilizam-se de informações relativas à pessoa para que uma

[2] VÉLIZ, Carissa. Privacidade é Poder: porque e como você deveria retomar o controle de seus dados. São Paulo: Editora Contracorrente, p. 10, 2021.
[3] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, p. 37, 2006.
[4] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. IV, n. 5, p. 195, 1890.

cadeia de processos mercadológicos opere a pleno funcionamento. O processamento de dados comportamentais passou a ser a matéria-prima de grandes empresas de tecnologia e interesse de Estados - a solidificação do capitalismo de vigilância[5]. Nesse contexto, a privacidade como uma mera concepção de refúgio marginalizado não se bastava. No cenário jurídico internacional, em meados da metade do século XX, a privacidade eleva o seu patamar ao status de direito humano[6], positivada em diversos instrumentos de direito internacional.

Em um determinado ponto, a privacidade englobava um conteúdo tão vasto que se tornou insuficiente denominá-la somente com um conceito único e restrito. A partir de uma definição, deu-se maior atenção e desenvolvimento teórico a quatro essencialmente distintas, mas intimamente interligadas: a privacidade, em sentido estrito, a autodeterminação informativa, o livre desenvolvimento da personalidade e a proteção de dados pessoais[7].

A proteção de dados pessoais assumiu um papel protagonista como tema principal em inúmeras decisões judiciais e propostas de leis por meados dos anos 70, com a massificação do uso de banco de dados robustos, em grande escala. Tem-se de exemplo uma variedade de legislações como a Lei Federal de Proteção de Dados da Alemanha (1977) e normativos estadunidenses, sendo o *Privacy Act* (1974) o mais representativo e primordial. Nas décadas seguintes, embora de lados opostos do mundo, cada uma das regiões buscou regulamentá-la a seu modo e modelo jurídico.[8]

Em uma análise temporal, é plausível concluir, comparativamente, que o ordenamento jurídico brasileiro somente recentemente preocupou-se em normatizar diretamente o tema, embora o tangenciasse em outras legislações, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, o Marco Civil da Internet e a Lei de Acesso à Informação. Tardiamente ou não, o Brasil não somente reconheceu a proteção de dados pessoais como uma essencial questão a ser tutelada conforme a Lei n° 13.709 de 2018 (“LGPD”), como também, por meio de julgamento histórico do Supremo Tribunal Federal (“STF”) e da Emenda Constitucional

[5] ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância. Rio de Janeiro: Intrínseca, p. 20, 2021.
[6] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em: https://www.unicef.org. Acesso em:
[7] MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. 1ª Edição, São Paulo: Editora Saraiva, p. 30-35, 2014.
[8] MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. 1ª Edição, São Paulo: Editora Saraiva, p. 30-35, 2014.

115/22, que concedeu o status de direito fundamental autônomo, diante de sua fundamentalidade para manter a estabilidade democrática.[9]

Em um raciocínio similar, o desenvolvimento tecnológico também reverberou sobre a sofisticação dos sistemas econômicos. Assim como novas discussões e novas interações sociais surgiram da relação privacidade-tecnologia, ocorre, analogamente, com o sistema financeiro. Nesse contexto, o dinheiro, na contemporaneidade, apresenta-se como uma das mais poderosas invenções humanas[10], transcendendo a realidade material. Trata-se de um produto da imaginação coletiva que se transcreve como um consenso intersubjetivo no mundo real[11], permitindo não somente ser digital, mas ter a sua mais complexa formatação nas configurações virtuais. Tal aspecto intrínseco, em um ambiente com os fatores externos necessários, levou à origem de novos agentes de mercado - as *fintechs* -, que, consigo, incorporam inovadores modelos de negócios, capazes de desafiar as tradicionais instituições financeiras[12].

Nesse contexto, dados pessoais bancários - contemplados no escopo de proteção da LGPD - estão, cada vez mais, em evidência como um produto mercadológico, necessários para que os novos atores do sistema financeiro sejam capazes de cumprir as suas propostas comerciais. Essa mudança gera pressão nos agentes reguladores financeiros, que devem ser capazes de estabelecer um padrão normativo adequado[13] à legislação de proteção de dados pessoais. Por conseguinte, urge investigar, se, de fato, os responsáveis estão caminhando lado a lado com o progresso tecnológico, aplicando regulação efetiva para as instituições financeiras, independentemente de serem tradicionais ou não.

Destarte, o propósito deste artigo é examinar a regulação do Sistema Financeiro Nacional (SFN) por meio da análise dos regulamentos do Banco Central (BACEN) e do Conselho Monetário Nacional (CMN) em conformidade com a Lei Geral de Proteção de Dados (LGPD). Especificamente, será abordada a inovação recente do *open banking*, a qual é regulamentada, primordialmente, pela Resolução BCB n° 32 de 29/10/2020. Por meio do levantamento bibliográfico, foram selecionadas obras e autores consagrados na área jurídica de

[9] MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. 1ª Edição, São Paulo: Editora Saraiva, p. 30-35, 2014.
[10] HARARI, Yuval. Sapiens: uma breve história da humanidade. Porto Alegre, RS: L&PM, p. 132, 2017.
[11] HARARI, Yuval. Sapiens: uma breve história da humanidade. Porto Alegre, RS: L&PM, p. 132, 2017.
[12] GOETTENAUER, Carlos. Implementação do Sistema Financeiro Aberto brasileiro e regulação por incentivos: estudo sobre a estratégia regulatória de Open Banking no Brasil. Revista de Direito Setorial e Regulatório, v. 7 n° 2, p. 118-135, outubro de 2021.
[13] BIS. Policy responses to fintech: a cross-country overview. Bank forInternational Settlements - Financial Stability Institute. Basileia. 2020. (FSI Insights on policy implementation No 23).

proteção de dados pessoais no Brasil. Para o tema do *open banking*, artigos publicados em revistas científicas foram extraídos diretamente do portal de periódicos da CAPES. A análise demonstra que os atores financeiros governamentais brasileiros estão claramente preocupados em se conformar com a Lei n° 13.709/2018, impondo uma série de regulamentações para garantir que as instituições privadas também sigam as diretrizes da LGPD, especialmente em relação aos novos modelos de negócio que surgiram devido ao avanço tecnológico no sistema financeiro brasileiro.

1. O Sistema Financeiro Nacional (SFN)

O Sistema Financeiro Nacional, em uma compreensão sintética, é uma rede de intermediação de recursos econômicos entre agentes superavitários para deficitários. Trata-se, portanto, de um complexo de instituições que permitem a transferência de ativos financeiros entre quaisquer pessoas e os tomadores de recursos finais na economia, possibilitando a liquidez de títulos e de valores mobiliários.[14] Desse modo, o mercado financeiro pode ser segregado entre quatro esferas mercadológicas distintas, mas intrinsecamente correlacionadas: mercado de capitais, mercado de crédito, mercado monetário e mercado de câmbio.[15]

O ponto embrionário do Sistema Financeiro Nacional (SFN) atual é a reforma bancária da década de 60, com a promulgação da Lei n° 4.595, de 31 de dezembro de 1964[16]. A estrutura do SFN hodierna é composta pelo que foi determinado no art. 1° desta legislação:

> Art. 1º O Sistema Financeiro Nacional, estruturado e regulado pela presente Lei, será constituído:
> I - do Conselho Monetário Nacional;
> II - do Banco Central do Brasil;
> III - do Banco do Brasil S. A.;
> IV - do Banco Nacional do Desenvolvimento Econômico;
> V - das demais instituições financeiras públicas e privadas.[17]

[14] CAVALCANTE, Francisco. Mercado de Capitais. 5ª ed. Rio de Janeiro: Campus, 2002.
[15] Disponível em: Funcionamento do Sistema Financeiro Nacional — Portal do Investidor (www.gov.br)
[16] SILVA, Sheldon William et al. O sistema financeiro nacional brasileiro: contexto, estrutura e evolução. Revista da Universidade Vale do Rio Verde, v. 14, n. 1, p. 1015-1029, 2016.
[17] BRASIL. Lei n° 4.595, de 31 de dezembro de 1964. Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4595.htm#:~:text=LEI%20N%C2%BA%204.595%2C%20DE%2031%20DE%20DEZEMBRO%20DE%201964&text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20e,Nacional%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 18 de fev. 2023..

Revogou-se, portanto, a antiga SUMOC com o intuito de dar o protagonismo regulador para as duas novas instituições monetárias que passariam a controlar, com maior autonomia, todo e qualquer agente financeiro de mercado atuante no Brasil: o Banco Central (BACEN) e o Conselho Monetário Nacional (CMN). O CMN figura no topo da pirâmide financeira brasileira, com o nível mais elevado na hierarquia de poderes e as suas competências envolvem todos os grandes mercados, desde a fixação de diretrizes cambiais, monetárias e creditícias até a regulamentação de taxas de juros e de operação de instituições financeiras públicas e privadas. O conceito destas diretrizes, conforme o art. 17 da citada lei, pode ser pormenorizado como:

> as pessoas jurídicas públicas ou privadas, que tenham como atividade principal ou acessória a coleta, intermediação ou aplicação de recursos financeiros próprios ou de terceiros, em moeda nacional ou estrangeira, e a custódia de valor de propriedade de terceiros.[18]

Nota-se, por conseguinte, que estas pessoas jurídicas são fundamentais para o pleno funcionamento e desenvolvimento da economia de qualquer nação, haja vista a necessidade da sua existência a fim de tornar a intermediação financeira eficiente. Podem, ou não, por conseguinte, agir com o objetivo de obtenção de lucro, embora o mais comum que operem visando, primordialmente, à lucratividade. O fato é: a conexão entre quem detém o dinheiro e quem precisa dele só é possível com a eficácia necessária mediante intermediação de um terceiro, que atua, geralmente, com a cobrança de juros para tal[19].

Nesse contexto, o papel do BACEN é substancial. Trata-se da entidade estatal que atua como executor e fiscalizador daquilo previsto e decidido pelo Conselho Monetário. As atribuições principais dessa autarquia federal variam desde o controle de operações monetárias e de crédito, fiscalização do sistema financeiro, permissão de funcionamento das instituições, até a popularmente conhecida emissão de dinheiro físico (papel-moeda e metal), dentre outras tantas responsabilidades previstas na lei da Reforma Bancária que seguem vigentes[20]. Em cronologia, a Constituição Federal de 1988 foi outro grande marco no desenvolvimento

[18] BRASIL. Lei n° 4.595, de 31 de dezembro de 1964. Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4595.htm#:~:text=LEI%20N%C2%BA%204.595%2C%20DE%2031%20DE%20DEZEMBRO%20DE%201964&text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20e,Nacional%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 18 de fev. 2023..

[19] SILVA, Sheldon William et al. O sistema financeiro nacional brasileiro: contexto, estrutura e evolução. Revista da Universidade Vale do Rio Verde, v. 14, n. 1, p. 1015-1029, 2016.

[20] SILVA, Sheldon William et al. O sistema financeiro nacional brasileiro: contexto, estrutura e evolução. Revista da Universidade Vale do Rio Verde, v. 14, n. 1, p. 1015-1029, 2016.

regulatório do SFN ao realizar uma abertura de mercado capaz de gerar concorrência legal e avanços na área, diante da busca dos atores financeiros por um espaço no mercado. Dessarte, pós-constituinte, novas categorias de instituições financeiras puderam inserir-se na roda econômica.[21]

Analogamente, o SFN pode, portanto, ser subdivido em dois campos essencialmente distintos, mas complementares. O primeiro, denominado como subsistema de supervisão, é composto não somente pelo CMN e BACEN, mas também por outros entes públicos como a Comissão de Valores Mobiliários (CVM), Superintendência de Seguros Privados (SUSEP) e outros conselhos e secretarias. A partir disso, compreende-se ser justamente a esfera responsável pelo estabelecimento das regras e pela fiscalização e aplicação destas, associada diretamente com a regulação governamental. O segundo é o subsistema operativo, conhecido como a esfera de intermediação, é formado, em síntese, pelas demais instituições financeiras que não estejam comportadas no campo de supervisão, isto é, o que conhecemos como bancos, empresas de crédito e as *fintechs*.[22]

Ante o quanto exposto, cabe, a seguir, explorar uma delimitação específica do subsistema de supervisão: a proteção de dados pessoais no Sistema Financeiro Nacional.

1.1. Regulação de Proteção de Dados Pessoais no SFN

A regulação dos agentes financeiros acerca da proteção de dados bancários é indissociável do surgimento das *fintechs* - startups com modelos de negócio similares aos de bancos tradicionais, mas com o diferencial de possuírem a estrutura mais simplificada, com o uso de tecnologia de ponta para prestação de serviços financeiros com eficiência e velocidade única no mercado, por meio de operações via ciberespaço (internet).[23] Abaixo, a conceituação oficial apresentada pelo Banco Central:

> *Fintechs* são empresas que introduzem inovações nos mercados financeiros por meio do uso intenso de tecnologia, com potencial para criar novos modelos de negócios. Atuam por meio de plataformas *online* e oferecem serviços digitais inovadores

[21] SILVA, Sheldon William et al. O sistema financeiro nacional brasileiro: contexto, estrutura e evolução. Revista da Universidade Vale do Rio Verde, v. 14, n. 1, p. 1015-1029, 2016.
[22] ASSAF NETO, Alexandre. Mercado financeiro. 11. ed. São Paulo: Atlas, 2012
[23] LIMA, Rafael Pereira; SILVEIRA, Daniel Barile da. Fintech e o Direito do Consumidor. Revista de Direito, Governança e NOVAS Tecnologias. Salvador, v. 4, n° 1, p.109-128, jan-jun, 2018.

> relacionados ao setor. No Brasil, há várias categorias de *fintechs*: de crédito, de pagamento, gestão financeira, empréstimo, investimento, financiamento, seguro, negociação de dívidas, câmbio e multisserviços.[24]

Nessa lógica, as *fintechs*, inevitavelmente, ocupam um relevante espaço na esfera operacional do Sistema Financeiro Nacional, estando, portanto, sujeitas aos regramentos instituídos tanto pelo BACEN quanto pelo CMN, notadamente quanto à proteção de dados bancários, haja vista ser um dos ativos mais primordiais do sistema de atividades financeiras dos modelos das *fintechs*[25]. Urge, então, a compreensão delimitada da concepção adotada pelo ordenamento jurídico brasileiro de dado pessoal, qual seja "qualquer informação relacionada a uma pessoa física identificada ou identificável"[26].

A referida concepção, ao mesmo tempo, diz muito e pouco, considerando que o conceito adotado pela legislação brasileira assume uma versão bastante abrangente.[27] O nome completo de uma pessoa, por exemplo, pode, consigo, carregar uma bagagem de informações sobre aquele indivíduo, como processos judiciais, contas bancárias, débitos com o governo, dívidas, rendimentos, entre tantos outros. No entanto, um dado isolado, a como o número da agência bancária, sobrenome ou valor do salário, embora capazes de identificar uma pessoa, somente dirão algo a partir de uma combinação com outros dados.

Os novos e tradicionais modelos de negócio financeiros, estão, portanto, regulados tanto pelos ditames publicados pelo BACEN e pelo CMN, mas também, por sua natureza mercadológica, envolvendo, inegavelmente, o tratamento de dados pessoais em grande parte dos processos produtivos, estão sob a aba de aplicação da LGPD. Assim, diante da pressão regulatória imposta, em 26 de abril de 2018, o Banco Central, intermediando decisão do Conselho Monetário Nacional, tornou pública a Resolução n° 4.658, a qual dispõe sobre:

> a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem

[24] Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/fintechs
[25] Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/fintechs
[26] BRASIL. Congresso Nacional. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 18 fev. 2023
[27] FRAZÃO, Ana, et. al. Capítulo 10: Compliance de Dados Pessoais. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Revista dos Tribunais, São Paulo, 2019.

> observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.[28]

A resolução, embora em nenhum de seus dispositivos cite diretamente o termo “dados pessoais”, referindo-se somente pela nomenclatura genérica de “dados”, encontra respaldo em uma série de princípios e direitos dos titulares previstos na Lei Geral de Proteção de Dados Pessoais, promulgada posteriormente, em agosto do mesmo ano. A exemplo, tem-se as seguintes previsões do normativo que estão em conformidade com o princípio da segurança e o da prevenção da LGPD - indispensabilidade de utilizar medidas técnicas, administrativas e físicas capazes de proteger os dados pessoais de acessos não autorizados e incidentes como perda, vazamento e compartilhamento indevido, aptas a prevenção de danos durante o tratamento (art. 6°, incisos VII e VIII)[29]:

> Art. 3º A política de segurança cibernética deve contemplar, no mínimo:
> II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;
> III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; (...)
> V - as diretrizes para
> b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição; (...)
> § 2º Os procedimentos e os controles de que trata o inciso II do caput devem abranger, no mínimo, a autenticação, e criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.[30]

---

[28] BRASIL. Banco Central do Brasil. Resolução n° 4.658, de 26 de abril de 2018. Disponível em :https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 18 de fev. 2023.

[29] BRASIL. Congresso Nacional. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 18 fev. 2023

[30] BRASIL. Banco Central do Brasil. Resolução n° 4.658, de 26 de abril de 2018. Disponível em :https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 18 de fev. 2023.

Outro princípio fundamental da LGPD que também pode ser visualizado em diversos dispositivos legais da Resolução é o da responsabilização e prestação de contas, também conhecido como *accountability*, o qual prevê a necessidade de se assumir a responsabilidade pelo que é feito com os dados e demonstrar o cumprimento das normas relativas ao seu respectivo tratamento (art. 6°, inciso X):

> Art. 3º A política de segurança cibernética deve contemplar, no mínimo:
> IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição; (...)
> § 4º O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV do caput, devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

Entende-se, por conseguinte, que a Resolução n° 4. 658/2018 dispõe sobre um escopo de aplicação (política de segurança cibernética) para além do que é regulamentado pela LGPD (tratamento de dados pessoais de pessoas físicas). No entanto, é essencial compreender a Lei n° 13.709/2019, como um polo de influência regulatório, interfere, para além do citado, com dois conceitos primordiais, considerando a relação entre instituições financeiras e os terceiros que prestam serviços de armazenamento em nuvem: o de controlador (quem toma as decisões referente ao tratamento) - e de operador (quem o faz em nome do controlador)[31] de dados pessoais.[32]

Assim, apesar da anterioridade da vigência da Resolução diante da LGPD, é inegável que a construção de um consenso jurídico acerca de determinados conceitos e orientações fundamentais acerca do tratamento de dados pessoais há muito estava sendo consolidado, o que permitiu que o BACEN e o CMN exercessem a sua função regulatória tangenciando temas essenciais previstos na legislação de proteção de dados pessoais.

---

[31] BRASIL. Congresso Nacional. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 18 fev. 2023

[32] GOETTENAUER, Carlos. O sistema financeiro brasileiro, política de segurança cibernética e proteção de dados pessoais: uma abordagem sob a ótica da regulação policêntrica. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, n° 2, p. 172-186, outubro de 2020.

2. O Sistema Financeiro Aberto (*Open Banking*)

Com a crise econômica mundial de 2008 como um ponto-chave para desencadear desconfiança e descredibilidade no modelo tradicional bancário, o Sistema Financeiro sofreu um abalo estrutural, permitindo a abertura de brechas para a entrada de novos modelos de negócio, descrito anteriormente com o surgimento do fenômeno das *fintechs*[33]. Nesse panorama moderno de inovação tecnológica associada a novas formas de prestar serviços financeiros, emerge a proposta do *Open Banking*. Trata-se de um conceito relativamente nebuloso em se conceder o significado mais completo e adequado, haja vista a ausência de consenso de uma definição imposta por um agente regulador, mas, o qual, inegavelmente, é um retorno regulatório das recentes transformações sofridas, não só no Sistema Financeiro Nacional brasileiro, mas em todo o mundo[34].

O *Open Banking* está direta e intimamente interligado com viabilidade de transferir o processamento de dados dos servidores da instituição financeira para um serviço de computação em nuvem fornecido por empresas de tecnologia. Além disso, pode ser entendido e livremente traduzido como Sistema Financeiro Aberto (SFA), em que ocorre o:

> compartilhamento de dados por meio de APIs (Application Program Interfaces), ou seja, a criação de uma infraestrutura tecnológica fornecida pelas próprias instituições bancárias, que permite aos terceiros intervenientes acessarem os dados dos clientes com sua devida autorização, em conformidade com os padrões de segurança estabelecidos.[35]

No Brasil, a regulação do *Open Banking* é responsabilidade do Banco Central, o qual, por meio da Resolução BCB n° 32 de 29 de outubro de 2020, estabeleceu os requisitos técnicos e procedimentos operacionais para a implementação do SFA no país, dispondo no Capítulo IV, "Do Escopo de Dados e Serviços", acerca, especificamente, do compartilhamento de dados entre as instituições participantes.

---

[33] GOETTENAUER, Carlos. O sistema financeiro brasileiro, política de segurança cibernética e proteção de dados pessoais: uma abordagem sob a ótica da regulação policêntrica. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, n° 2, p. 172-186, outubro de 202

[34] GOETTENAUER, Carlos. Implementação do Sistema Financeiro aberto brasileiro e regulação por incentivos: estudo sobre a estratégia regulatória de Open Banking no Brasil. Revista de Direito Setorial e Regulatório, v. 7 n° 2, p. 118-135, outubro 2021;

[35] GOETTENAUER, Carlos. Implementação do Sistema Financeiro aberto brasileiro e regulação por incentivos: estudo sobre a estratégia regulatória de Open Banking no Brasil. Revista de Direito Setorial e Regulatório, v. 7 n° 2, p. 118-135, outubro 2021;

A principal correlação regulatória a ser realizada entre o Sistema Financeiro Aberto implementado com a LGPD é o conceito de consentimento, um dos requisitos mínimos para o funcionamento e operacionalização do *Open Banking*. Na legislação brasileira de proteção de dados pessoais, trata-se de uma base legal, isto é, uma hipótese para autorizar ou permitir, fundamentadamente, a realização de um tratamento, o qual é previsto nos seguintes dispositivos legais:

> 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.

Desse modo, entende-se que, embora não exista uma regulamentação específica elaborada pelo BACEN ou pelo CMN acerca do tratamento de dados pessoais no funcionamento do Open Banking, é inegável que toda e qualquer operação realizada no contexto dessa nova modalidade de interação entre instituições financeiras está sob o escopo de aplicação da Lei Geral de Proteção de Dados Pessoais, haja vista o caráter inerente de uso de dados para que o Sistema Financeiro Aberto opere com os fins mercadológicos propostos em sua concepção inicial.

Considerações Finais

Os conceitos de privacidade e sistema financeiro, ao primeiro olhar, podem ser entendidos sem uma relação que os posicione em um mesmo panorama de análise. No entanto, com um olhar analítico, percebe-se que ambos são conceitos indissociáveis, com a relação reforçada mediante a inserção da proteção de dados pessoais como intermediadora de um diálogo concreto e direto, principalmente ao se considerar o contexto do Sistema Financeiro Nacional. Uma das funções primordiais dos órgãos públicos reguladores é garantir a segurança da população - a engrenagem de todo e qualquer esfera econômica - e as entidades brasileiras

como BACEN e CMN somente cumpririam tamanha responsabilidade ao estar em conformidade com os regramentos pertinentes, como a Lei Geral de Proteção de Dados Pessoais.

Isto posto, torna-se evidente que a LGPD encontra respaldo para ser aplicada perante as instituições financeiras públicas e privadas, além de ser notável a preocupação dos agentes reguladores do Estado brasileiro em adequarem os seus normativos conforme a construção jurídica consolidada da privacidade e da proteção de dados pessoais, aplicando conceitos-chave e princípios da referida legislação em sua atuação regulatória.

Referências Bibliográficas

ASSAF NETO, Alexandre. *Mercado financeiro*. 11. ed. São Paulo: Atlas, 2012

BIS. Policy responses to fintech: a cross-country overview. Bank for International Settlements - Financial Stability Institute. Basileia. *FSI Insights on policy implementation No 23*, 2020

BRASIL. Banco Central do Brasil. *Resolução n° 4.658, de 26 de abril de 2018.* Disponível em:https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 18 de fev. 2023.

BRASIL. Congresso Nacional. *Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 18 fev. 2023

CAVALCANTE, Francisco. *Mercado de Capitais*. 5ª ed. Rio de Janeiro: Campus, 2002.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

FRAZÃO, Ana, et. al. *Capítulo 10: Compliance de Dados Pessoais.* Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Revista dos Tribunais, São Paulo, 2019.

GOETTENAUER, Carlos. Implementação do Sistema Financeiro Aberto brasileiro e regulação por incentivos: estudo sobre a estratégia regulatória de Open Banking no Brasil. *Revista de Direito Setorial e Regulatório*, v. 7 n° 2, p. 118-135, outubro de 2021.

GOETTENAUER, Carlos. O sistema financeiro brasileiro, política de segurança cibernética e proteção de dados pessoais: uma abordagem sob a ótica da regulação policêntrica. *Revista de Direito, Estado e Telecomunicações*, Brasília, v. 12, n° 2, p. 172-186, outubro de 2020.

HARARI, Yuval. *Sapiens: uma breve história da humanidade.* Porto Alegre, RS: L&PM, 2017.

LIMA, Rafael Pereira; SILVEIRA, Daniel Barile da. Fintech e o Direito do Consumidor. *Revista de Direito, Governança e NOVAS Tecnologias*, Salvador, v. 4, n° 1, p.109-128, jan-jun, 2018.

MENDES, Laura Schertel. *Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo*

direito fundamental. 1ª Edição, São Paulo: Editora Saraiva, p. 30-35, 2014.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos, 1948.* Disponível em: https://www.unicef.org. Acesso em: 18 de fev. 2023.

SILVA, Sheldon William et al. O sistema financeiro nacional brasileiro: contexto, estrutura e evolução. *Revista da Universidade Vale do Rio Verde*, v. 14, n. 1, p. 1015-1029, 2016.

VÉLIZ, Carissa. *Privacidade é Poder: porque e como você deveria retomar o controle de seus dados.* São Paulo: Editora Contracorrente, 2021.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. IV, n. 5, 1890.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância*. Rio de Janeiro: Intrínseca, p. 20, 2021.

O TRATAMENTO DE DADOS PESSOAIS NO CONTEXTO DA NOVA LEI DO CADASTRO POSITIVO

Elis Bandeira Alencar Brayner[1]

Resumo: Em 8 de abril de 2019, foi sancionada a Lei Complementar 166/2019, que alterou substancialmente a Lei do Cadastro Positivo e provocou dúvidas sobre a proteção de dados pessoais na construção de perfis creditícios. A partir desse contexto, este trabalho buscou realizar uma revisão bibliográfica e analisar compilado legislativo acerca da utilização de dados pessoais na formação do *score* de crédito dos consumidores e os direitos e deveres incluídos neste âmbito com a Lei Geral de Proteção de Dados. Adiante, analisou-se o funcionamento do Cadastro Positivo no Brasil, as alterações trazidas pela Lei Complementar nº 166/2019 e os dispositivos legais que regulamentam o tratamento de dados pessoais. Observou-se que tanto a Lei Complementar 166/2019 quanto a Lei Geral de Proteção de Dados trouxeram diversos dispositivos delimitando as informações utilizadas no Cadastro Positivo, garantindo que o titular dos dados esteja envolvido neste tratamento e efetivando a proteção de seus dados pessoais.

Palavras-chave: avaliação de crédito; cadastro positivo; proteção de dados; privacidade

Abstract: *On April 8, 2019, the Supplementary Law 166/19 was sanctioned, amending substantially the Law of the "Cadastro Positivo" (Positive Register) and sparked concerns over the personal data protection when developing credit profiles. Within this context, a literature review and legislative compilation was carried out regarding the use of personal data in the development of consumers' credit score and the rights and obligations included in the scope of*

[1] Elis Bandeira Alencar Brayner é pós-graduanda em Direito Digital e Proteção de Dados do Instituto Brasiliense de Direito Público (IDP). Bacharela em Direito pela Universidade de Brasília (UnB). Pesquisadora do Privacy Lab - Centro de Direito, Internet e Sociedade (CEDIS) do IDP. Coordenadora de Comunicação do Observatório da LGPD/UnB. Estagiária da Pós-Graduação da Defensoria Pública da União no 5º Ofício Cível. Advogada.

the credit profile through the Brazilian General Data Protection Law. Thereafter, there was an analysis of the operation of the "Cadastro Positivo" in Brazil, the changes brought by the Complementary Law No. 166/2019 and the legal mechanisms that regulate personal data treatment. It was noted that both the Complementary Law 166/2019 and the Brazilian General Data Protection Law brought several devices to limit the information used in the "Cadastro Positivo" (Positive Register), ensuring that the data subject is involved in this treatment and enforcing the protection of their personal data.

***Keywords*:** *credit scoring; credit record; data protection; privacy*

Introdução

Por meio da análise de dados pessoais, as agências de crédito mensuram os riscos envolvidos na concessão de crédito ou no cumprimento de obrigações financeiras e atribuem uma nota entre 0 a 1.000 pontos ao consumidor – quanto maior a nota, presumivelmente maior é sua confiabilidade. Destarte, estabelece-se uma relação de confiança mútua em que o consumidor fornece seus dados para receber benefícios creditícios, como a concessão de empréstimos com taxas de juros menores (CARVALHO, 2003, p. 356).

No entanto, o tratamento de dados pessoais vem se tornando o foco de diversas discussões, haja vista vivermos hoje em uma sociedade em que vigora o "capitalismo de vigilância", conceito cunhado por Shoshana Zuboff, que define a sociedade que se organiza pela extração de dados pessoais sobre dados comportamentais. Estes dados são analisados por equipamentos eletrônicos de forma a criar predições sobre os indivíduos, que serão vendidas a terceiros para que estes saibam o perfil de seus consumidores e possam criar estratégias para lucrar ainda mais (ZUBOFF, 2019, p.113).

De acordo com Zuboff, quanto maior a quantidade de dados, maior é a exatidão das predições feitas pela inteligência artificial. O histórico de crédito funciona da mesma maneira, o que é conhecido no mercado financeiro como o princípio de "*more is better*" ou, em tradução livre, "mais é melhor", incentivando a extração e tratamento do maior número de dados possível (BESSA, 2019, p. 51).

Por outro lado, no meio jurídico, percebe-se uma preocupação crescente com relação ao tratamento de dados pessoais e a privacidade dos indivíduos, o que se reflete no panorama legislativo brasileiro com a reforma à Lei do Cadastro do Cadastro Positivo pela Lei

Complementar nº 166/2019 e a promulgação da Lei Geral de Proteção de Dados Pessoais. Faz-se necessário, por conseguinte, analisar se a construção do histórico de crédito dos cidadãos brasileiros preserva sua privacidade e os beneficia concretamente.

1. O sistema da análise de crédito

Os indivíduos são submetidos a avaliações desde sua infância; citam-se, a título de exemplificação, as provas feitas na escola para aferir seus conhecimentos acerca do conteúdo passado em sala de aula. A noção é bem simples: são realizadas perguntas e, quanto maior a nota do aluno, melhor é considerado seu desempenho nos estudos. Esse conceito é também aplicado na vida adulta, por meio da avaliação de crédito.

As agências de pontuação de crédito originaram-se no final do século XIX, nos Estados Unidos da América (EUA), com o objetivo de avaliar a capacidade de um indivíduo pagar empréstimos e financiamentos por meio da avaliação de suas características e comportamentos, determinando a confiabilidade na quitação de suas dívidas (SIMÃO, 2022, p. 14). Dessa forma, o risco de uma operação é mensurado por meio de uma nota atribuída ao indivíduo; quanto maior a nota, menor é o risco e, por conseguinte, podem ser oferecidas condições melhores de crédito, como menores taxas de juros.

Isto é, a avaliação de crédito representa a confiabilidade de um indivíduo, entendimento mais complexo que a aferição do desempenho em idade escolar. Um dos pontos centrais na infraestrutura de pontuação consiste nas informações utilizadas como base para definir se o cidadão seria confiável, responsável e, portanto, "merecedor" do acesso ao crédito e, com o avanço da tecnologia por meio de processamento automatizado de dados e a criação de algoritmos capazes de analisar vultosas quantidades de informação, essa questão se tornou ainda mais sensível (SIMÃO, 2022, p. 45). Nesse sentido, há uma certa carga de julgamento moral nessa situação que pode resultar na estigmatização do indivíduo (KRIPPNER, 2017, p. 37):

> Novas ferramentas digitais tornam possível uma nova economia de julgamento moral. Registros passivos são transformados em métricas ativas, que implicam cálculo, eficiência e a obrigação de estar no controle e prestar contas a si mesmo. As métricas tornam-se injunções morais. [...]. Gaste, mas de forma controlada. Dirija, mas não muito rápido. Coma, mas mantenha-se saudável. A racionalidade protetiva do Fitbit

> ou do score oferece vigilância benevolente, instruindo implicitamente as pessoas a se automonitorarem e, se necessário, chegarem mais longe ou transformarem suas vidas. (FOURCADE, 2016, p. 2)

A despeito dos problemas envolvidos na pontuação de crédito, essa atividade se expandiu, tornou-se legalmente reconhecida em diversos países e é, inclusive, estimulada pelo Banco Mundial. Ainda em 2003, o Banco Mundial realizou um projeto denominado "Doing Business", descontinuado apenas em 2021, no qual defendia reformas institucionais de forma a estabelecer "condições legais para que birôs de crédito exerçam suas atividades" e incentivando a adoção de políticas de *score* de crédito, para um desenvolvimento do sistema financeiro (SIMÃO, 2022, p. 16).

1.1. Panorama legislativo brasileiro

Ao final dos anos 1990, com a promulgação do Código de Defesa do Consumidor, que trata dos cadastros de inadimplentes em sua Seção VI, Capítulo V, a discussão sobre a necessidade de um marco legal que regulasse a avaliação de crédito tornou-se mais premente e, desde então, mais de 40 (quarenta) projetos de lei sobre o tema foram apresentados ao Congresso Nacional (FALCÃO, 2016, p. 23). A primeira tentativa de regulamentação do tratamento de informações de crédito feita pelo Governo Federal se deu pelo Projeto de Lei nº 5.870/2005 e suas principais razões foram:

> (...) indicadas formalmente em Mensagem Interministerial, firmada conjuntamente pelos Ministros da Justiça e da Fazenda e dirigida, em 17 de agosto de 2005, ao Presidente da República. O propósito principal seria "dotar o País de um arcabouço legal que incentive a troca de informações pertinentes ao crédito e transações comerciais, reduzindo o problema da assimetria de empréstimos e a aplicação nas relações comerciais, favorecendo principalmente os indivíduos e as empresas que apresentem um bom histórico de crédito". (BESSA, 2011, p. 40)

Não obstante, foi apenas após anos de debates no congresso, em 9 de junho de 2011, que entrou em vigor a chamada Lei do Cadastro Positivo (LCP), Lei nº 12.414/2011, visando à melhora na avaliação de riscos e consequente oferta de condições mais vantajosas àqueles que

necessitam de crédito. Nesse contexto, faz-se necessário destacar que o termo "Cadastro Positivo" designa:

> (...) uma política destinada à formação do histórico de crédito de pessoas naturais e jurídicas, por meio da criação de bancos de dados com informações de pagamento de dívidas e de cumprimento de obrigações pecuniárias dessas pessoas. (FALCÃO, 2016, p. 24).

Essa nomenclatura surgiu em contraste com um termo introduzido pelo Código de Defesa do Consumidor do "cadastro negativo", ou seja, o histórico de crédito construído pela análise de dados negativos, quais sejam, as dívidas vencidas e não adimplidas. A terminologia do "Cadastro Positivo" resulta da percepção do mercado financeiro de que, para traçar previsões sobre os consumidores, seriam necessárias mais informações, não somente aquelas relativas às dívidas dos indivíduos, isto é, as informações relativas ao adimplemento, como por exemplo compromissos quitados dentro do prazo, histórico de pagamentos realizados e a capacidade de assumir novas obrigações financeiras (BESSA, 2011, p. 28).

A Lei nº 12.414/2011, em teoria, conciliaria o interesse econômico das instituições financeiras e das concedentes de crédito na elaboração do cadastro positivo e a proteção à privacidade e aos dados pessoais dos consumidores durante esse procedimento. Anteriormente, não havia sido definida a extensão da prerrogativa dos birôs de crédito de coletar e tratar dados pessoais e por quanto tempo esses dados poderiam ser armazenados, deixando os consumidores sem a tutela efetiva de seu direito à privacidade. Todavia, a LCP não encerrou esse embate, principalmente em razão da baixa adesão dos indivíduos ao Cadastro Positivo.

A LCP exigia o consentimento dos usuários para que seus dados fossem tratados, o que, de fato, resultava na proteção da privacidade dos consumidores. Não obstante, a baixa adesão dos indivíduos ao Cadastro Positivo fez com que esse instituto não possuísse a força necessária para que aqueles que concedem crédito pudessem avaliar o perfil creditício dos indivíduos, comprometendo o interesse financeiro da lei (SIMÃO, 2022, p. 17).

O Poder Judiciário não se manteve inerte ante a questão da proteção de dados na avaliação de crédito. Em 2014, o Superior Tribunal de Justiça (STJ) distinguiu os termos "cadastro positivo" e "pontuação de crédito", durante o julgamento do Recurso Especial 1.419.697/RS, que foi objeto da primeira audiência pública da história desta egrégia Corte (REVISTA CONSULTOR JURÍDICO, 2014, n.p.). Essa distinção foi essencial para que a

alteração do modelo *"opt in"* para o modelo "*opt out",* trazida pela Lei Complementar 166/2019, pudesse ser feita sem comprometer a proteção de dados pessoais, como se verá adiante.

No julgamento, o Ministro Paulo de Tarso Sanseverino asseverou que a pontuação de crédito não consiste em uma base de dados em sentido estrito, mas em uma metodologia de avaliação de risco baseada em informações publicamente disponíveis, assim, o consentimento prévio do cidadão para inclusão no sistema de pontuação não seria necessário (FALCÃO, 2016, p. 47). Ao final da discussão, a Súmula 550 foi editada estabelecendo, *in verbis*:

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

Cumpre destacar que o entendimento firmado pelo STJ também balizou o respeito à privacidade e transparência na pontuação de crédito, demonstrando a preocupação com a utilização dos dados pessoais mesmo antes da promulgação da Lei Geral de Proteção de Dados (LGPD). Destarte, ao utilizar o sistema de pontuação de crédito, a pessoa jurídica assume certos direitos e deveres, dentre eles a obrigação de informar os dados utilizados na formação do *score* de crédito, caso o consumidor faça essa requisição (ZANATTA, 2019, p. 14).

1.2. Nova Lei do Cadastro Positivo

Em 8 de abril de 2019, foi sancionada a Lei Complementar 166/2019, comumente chamada de Nova Lei do Cadastro Positivo (NLCP), que alterou substancialmente a Lei 12.414/2011 (Lei do Cadastro Positivo, LCP); mais da metade do diploma normativo foi modificado, sendo, ainda, acrescidos cinco novos artigos (BESSA, 2019, p. 51). Dentre essas mudanças, a mais significativa é a alteração do art. 4º da Lei 12.414/2011, que tornou automática a inscrição dos consumidores nos cadastros positivos (RAMOS, 2019, p. 16).

Em realidade, a nova redação altera o momento de manifestação do titular dos dados, o consentimento deixa de ser exigido na abertura do cadastro - modelo *opt in* -, permitindo que o gestor responsável pela administração do banco de dados abra o cadastro positivo, comunicando posteriormente ao consumidor que, após ser avisado, pode solicitar o cancelamento do cadastro

- modelo *opt out* - (CORTAZIO, 2019, p. 13). No ponto, sublinha-se que, (i) enquanto a inclusão ao cadastro era voluntária, menos de 10% dos potenciais tomadores de crédito do Brasil optaram pela adesão, o que gerou um enfraquecimento do cadastro positivo e impediu que os consumidores se beneficiassem com a redução da taxa de juros e da concessão de crédito (BESSA, 2019, p. 52), e que (ii) apenas os agentes autorizados pelo Banco Central, chamados de Gestores de Bancos de Dados (GBDs) podem operacionalizar as bases de dados do cadastro positivo (SEBBEN, 2021, p. 22).

A alteração legislativa também garantiu que a comunicação feita ao consumidor após a abertura do cadastro, que deve ocorrer em até 30 dias, seja realizada gratuitamente e "de maneira clara e objetiva os canais disponíveis para o cancelamento do cadastro no banco de dados" (art. 4º, § 4º, III), salvo na hipótese de que o "cadastrado já tenha cadastro aberto em outro banco de dados." (art. 4º, § 5º) , em que o aviso não é obrigatório (SEBBEN, 2021, p. 60). Ademais, os Gestores de Bancos de Dados devem disponibilizar "em seu sítio eletrônico, de forma clara, acessível e de fácil compreensão, a sua política de coleta e utilização de dados pessoais para fins de elaboração de análise de risco de crédito" (Art. 7-A, §1º, LC 166/2019).

Todavia, há ainda um debate acerca do tratamento de dados pessoais realizados na construção do histórico de crédito e o respeito à privacidade e à dignidade da pessoa humana. Afinal, sob a perspectiva econômica, quanto mais informações os Gestores de Bancos de Dados possuem, melhor é a análise de riscos na concessão de crédito, princípio conhecido na doutrina econômica como *"more is better"* (BESSA, 2019, p. 51). A seguir analisa-se a harmonização entre a Lei Geral de Proteção de Dados e a Lei do Cadastro Positivo a fim de manter preservados os direitos fundamentais dos consumidores.

2. O tratamento de dados pessoais no contexto da Nova Lei do Cadastro Positivo

Apesar de ter sido promulgada em 14 de agosto de 2018, a Lei Geral de Proteção de Dados (Lei 13.709/2018) entrou em vigência apenas em 20 de agosto de 2020, tendo sido proposta como forma de efetivar a tutela "da pessoa em vista de variadas formas de controle e contra a discriminação, com o fim de garantir a integridade de aspectos fundamentais de sua própria liberdade pessoal". Para entender a importância deste diploma legal, rememora-se que o domínio sobre a informação é, há séculos, elemento essencial para o exercício do poder nas sociedades (DONEDA, 2020, p. 26). Nos termos da própria LGPD, sancionou-se o:

> Art. 1º (...) 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.

Além de definir diversos termos importantes, a Lei 13.709/2018 estabeleceu, em seu art. 7º, as bases legais para o tratamento de dados pessoais, a partir disso, a coleta de informações somente pode ocorrer caso haja uma hipótese legal que a autorize. O referido artigo, em seu inciso X, dispõe que uma das hipóteses de tratamento de dados pessoais é "X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente", assim, a utilização de dados pessoais para a construção de um histórico de crédito, mesmo sem o consentimento do titular, como disposto pela Nova Lei do Cadastro Positivo, encontra guarida também na LGPD.

Nota-se que não há restrições específicas na LGPD quanto ao tratamento das informações que seriam utilizadas para a construção do histórico de crédito. Por outro lado, na Nova Lei do Cadastro Positivo, há dois incisos que preveem os dados que não podem ser analisados na construção do histórico de crédito (SIMÃO, 2022, p. 114), quais sejam:

> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
>
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

No entanto, não há menção específicas nos dois diplomas legais acerca da utilização de dados alternativos, que podem ser definidos, de acordo com o *Consumer Financial Protection Bureau* (CFPB 2017, p. 5), como "todos aqueles que se diferem dos tradicionais, encontrados em bancos de dados relacionados à prestação de serviços financeiros", como por exemplo aqueles relacionados a redes sociais, geolocalização, entre outros. A partir desse ponto, surgem dificuldades quanto aos limites da criação de perfis de consumo e o controle das decisões automatizadas de maneira a preservar a proteção dos dados dos indivíduos.

2.1. Perfilização no âmbito creditício

A perfilização, tradução utilizada para o termo da língua inglesa *profiling*, pode ser conceituada como "uma técnica em que um conjunto de características de uma determinada classe de pessoa é inferido a partir de experiências passadas e, em seguida, dados armazenados são pesquisados para indivíduos com um ajuste quase perfeito a esse conjunto de características" (CLARKE, 1993, p. 403). A perfilização, no âmbito do Cadastro Positivo, é utilizada como uma forma de prever comportamentos financeiros de (in)adimplência dos indivíduos.

Os juristas Danielle Citron e Frank Pasquale cunharam o termo "caixas pretas dos algoritmos" ao tratar da construção de perfis creditícios, denunciando que os birôs de crédito americanos utilizavam dados que não eram conhecidos pelos consumidores para classificá-los com algoritmos que reforçam práticas discriminatórias (CITRON e PASQUALE, 2015, p. 11 e 12). De acordo com os autores, "As pontuações de crédito são tão livres de preconceitos como os dados e o software por trás delas." (Tradução livre), indaga-se, então: quais são os dados utilizados para formação do Cadastro Positivo brasileiro?

Inicialmente, cumpre destacar que o Código de Defesa do Consumidor, em sua seção VI, estabelece algumas regras com relação aos bancos de dados e cadastros de consumidores. Nos termos do art. 43 do referido diploma legal, (i) o consumidor deve ter acesso às informações e suas respectivas fontes utilizadas em seus cadastros; (ii) os cadastros devem ser "claros, verdadeiros e em linguagem de fácil compreensão"; (iii) a abertura de um cadastro deve "ser comunicada por escrito ao consumidor"; (iv) o consumidor pode exigir correção imediata dos seus dados, tendo o arquivista que comunicar as alterações no prazo de "cinco dias úteis"; (v) as informações negativas acerca dos consumidores só podem ser armazenadas por até cinco anos; e (vi) os “bancos de dados e cadastros relativos a consumidores e os serviços de proteção ao crédito” são considerados “entidades de caráter público” (ZANATTA, 2019, p. 6).

Destarte, desde a década de 1990, o CDC assegura os direitos de acesso, informação e responsabilidade no que tange aos bancos de dados dos consumidores (ZANATTA, 2019, p. 15). Seguindo essa linha, a Lei Complementar nº 166/2019 incluiu, por meio do art. 7-A, as restrições às informações que não podem ser utilizadas nos bancos de dados, são elas:

> Art. 7º-A Nos elementos e critérios considerados para composição da nota ou pontuação de crédito de pessoa cadastrada em banco de dados de que trata esta Lei,

> não podem ser utilizadas informações: (Incluído pela Lei Complementar nº 166, de 2019)
> I - que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas; (Incluído pela Lei Complementar nº 166, de 2019)
> II - de pessoas que não tenham com o cadastrado relação de parentesco de primeiro grau ou de dependência econômica; e (Incluído pela Lei Complementar nº 166, de 2019)
> III - relacionadas ao exercício regular de direito pelo cadastrado, previsto no inciso II do caput do art. 5º desta Lei. (Incluído pela Lei Complementar nº 166, de 2019)

Entretanto, a Lei do Cadastro Positivo somente veda a utilização de "informações excessivas" que não se relacionem diretamente com a avaliação de crédito, o problema reside aqui: uma informação pode ser útil estatisticamente para a avaliação de crédito, ainda que não seja uma informação de pagamento (SIMÃO, 2022, p. 114). Nesse sentido, uma informação compartilhada em rede social ou por meio de geolocalização poderia ser empregada na construção do histórico de crédito, seriam estes os dados alternativos que ainda não foram regulamentados e precisam ser pensados em futuras decisões e alterações legislativas.

2.2. A possibilidade de revisão de decisões automatizadas

As decisões automatizadas são aquelas tomadas por algoritmos. De forma simplificada, a máquina, ao tomar uma decisão, vale-se de dados de entrada - que podem ser imagens, textos, sons, entre outros, traduzidos em linguagem digital - para fazer uma predição com fundamento no conhecimento obtido pelo algoritmo durante a fase de treinamento (AGRAWAL, GANS, GOLDFARB, 2018, p. 74). Ainda que este conceito não esteja presente na LGPD ou na Lei do Cadastro Positivo, os diplomas legais garantem ao titular dos dados pessoais o direito à revisão de decisões automatizadas, veja-se, respectivamente:

> 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)
> Art. 5º São direitos do cadastrado:

> VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; (Redação dada pela Lei nº 12.414, de 2011)

O direito de revisão a decisões automatizadas foi uma inovação da Lei do Cadastro Positivo, ainda em sua redação inicial, de 2011, determinando que pessoas naturais possam analisar as decisões algorítmicas e inclusive identificar possíveis discriminações, como por exemplo verificar se a utilização do CEP do consumidor está sendo empregada para identificar o risco de uma operação, atribuindo a residência em localização periférica como um risco maior à concessão de crédito (ZANATTA, 2019, p. 18 e 19). Há, no entanto, uma certa opacidade nessas decisões algorítmicas (CITRON e PASQUALE, 2014, p. 15).

Explica-se. Os Gestores de Bancos de Dados apresentam resistência à divulgação precisa de como funcionam suas fórmulas algorítmicas em razão do sigilo comercial e segredo industrial que a protegem, afinal, esses birôs concorrem com base nas metodologias para formar o histórico de crédito. Além disso, estas empresas afirmam que, caso os consumidores soubessem exatamente as informações utilizadas pelos GBDs, poderiam trapacear o sistema para aumentarem seu *score* de crédito. Aliás, mesmo que os consumidores possuíssem transparência total acerca dos algoritmos, essas informações seriam ininteligíveis para o cidadão comum (SIMÃO, 2022, p. 47).

Nesse sentido, pode haver entraves quando um cidadão for argumentar pela revisão da decisão automatizada, em um primeiro momento, no sentido de compreender os mecanismos do Cadastro Positivo para produzir provas e, em um segundo plano, quando se trata de tratamento discriminatório, o cidadão teria que saber quais dados foram utilizados e em qual medida contribuem para a sua pontuação, informações protegidas pela propriedade intelectual. A solução para esse dilema seria a realização de auditorias externas por órgãos reguladores, prevista como possibilidade pelo artigo 7-A, §2º, da Lei do Cadastro Positivo e pela LGPD em seu art. 20 §2º (PASQUALE, 2015, p. 150), no entanto, até o presente momento, não foi expedida a regulamentação para tanto.

Considerações Finais

A alteração trazida pela Lei Complementar nº 166/2019 na inscrição dos consumidores no Cadastro Positivo, substituindo o modelo *opt in* pelo modelo *opt out*, em princípio causou debate sobre a proteção de dados dos cidadãos brasileiros. Essa discussão pode ser ilustrada por

comentários feitos no Plenário da Câmara dos Deputados; ainda em 20 de fevereiro de 2019, antes da entrada em vigor da Lei Complementar, disse o Deputado Federal Aliel Machado (PSB-PR):

> Vamos escolher se defendemos o direito do povo frente ao interesse econômico, porque quem está pressionando pela aprovação do projeto são os bancos que, inclusive, bancaram eleições (SIQUEIRA, 2019).

Não obstante, uma análise mais detida dos dispositivos contidos na Nova Lei do Cadastro Positivo, em conjunto com os direitos e deveres relativos ao tratamento de dados pessoais trazidos com a promulgação da Lei Geral de Proteção de Dados, revela que os consumidores seguem envolvidos na construção do seu histórico de crédito, com sua autonomia preservada. Há, nesse sentido, obrigações explícitas aos birôs de crédito no que tange ao aviso que deve ser dado aos consumidores após sua inclusão no Cadastro Positivo, garantindo que este tratamento não ocorra sem o conhecimento dos titulares dos dados.

Insta rememorar que, antes da LC nº 166/2019, apenas 10% dos cidadãos brasileiros estavam inscritos no Cadastro Positivo, o que impedia que os benefícios creditícios desse instituto pudessem ser de fato constatados pela população. A mudança foi realizada com o propósito de aumentar a adesão dos consumidores, mas não concedeu poder ilimitado aos Gestores de Bancos de Dados.

Nos termos da Lei Geral de Proteção de Dados, a transparência é um princípio que deve reger o tratamento de dados pessoais, garantindo "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" (art. 6º, VI). No ponto, mesmo que possa haver aspectos a serem mais profundamente examinados, como o dos dados alternativos, a Lei do Cadastro Positivo delimitou as informações utilizadas na formação do banco de dados, exigindo que sejam "objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado" (art. 3º), fornecendo ainda os conceitos de cada um desses pontos:

> § 2º Para os fins do disposto no § 1º , consideram-se informações:
> I - objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor;

> II - claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica;
> III - verdadeiras: aquelas exatas, completas e sujeitas à comprovação nos termos desta Lei; e
> IV - de fácil compreensão: aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados.

Ante o exposto, nota-se uma harmonização entre a proteção de crédito e a proteção de dados dos indivíduos, principalmente considerando que a boa utilização do Cadastro Positivo permite que os consumidores possam ter acesso a crédito com taxas e juros reduzidos em vista de seu histórico de adimplência. Por fim, é importante sublinhar que a Lei do Cadastro Positivo, por meio do § 2º do art. 7º-A, preceitua que

> a transparência da política de coleta e utilização de dados pessoais de que trata o § 1º deste artigo deve ser objeto de verificação, na forma de regulamentação a ser expedida pelo Poder Executivo.

Destarte, o dispositivo legal não apenas delimitou as informações que podem ser utilizadas e os agentes responsáveis pelo tratamento, como também possibilitou a regulamentação do controle e fiscalização da transparência da política de tratamento de dados. Espera-se que esta regulamentação seja expedida o quanto antes, garantindo que o disposto no ordenamento jurídico pátrio, no que concerne à proteção da privacidade dos cidadãos, seja executado na prática.

Referências bibliográficas

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. Máquinas Preditivas: a simples economia da inteligência artificial. Rio de Janeiro: Editora Alta Books, 2018. Tradução de Wendy Campos.

BESSA, Leonardo Roscoe. A nova Lei do Cadastro Positivo. DIREITO DO CONSUMIDOR, p. 51-68, 2019.

BESSA, Leonardo Roscoe. Cadastro positivo: comentários à Lei 12.414, de 9 de junho de 2011. São Paulo: Editora Revista dos Tribunais, 2011.

CARVALHO, Ana Paula Gambogi. Revista de Direito do Consumidor – RDC, v. 46, 2003.

CITRON, Danielle Keats; PASQUALE, Frank. The scored society: due process for

automated predictions. *Washington Law Review*, v. 89, 2014

CLARKE, Roger. Profiling: A hidden challenge to the regulation of data surveillance. *Journal of Law & Information Science*, v. 4, 1993.

CONSUMER FINANCIAL PROTECTION BUREAU. *Request for information regarding use of alternative data and modeling techniques in the credit process*, 2017. Disponível em: <http://files.consumerfinance.gov/f/documents/20170214_cfpb_Alt-DataRFI.pdf>. Acesso em: 30 de abr. de 2023.

CORTAZIO, R. Soares. Bancos de dados no Brasil: uma análise do sistema credit scoring à luz da LEI N. 13.709/2018 (LGPD). *Revista Eletrônica da PGE-RJ*, [S. l.], v. 2, n. 3, 2019. DOI: 10.46818/pge.v2i3.99. Disponível em: <https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/99>. Acesso em: 27 jun. 2023.

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

FALCÃO, Rafael dos Santos. Bancos de dados de proteção ao crédito e a lei do cadastro positivo. 2016.

FOURCADE, Marion; HEALY, Kieran. Seeing like a market. *Socio-Economic Review*, p. 9-29, 2016.

KRIPPNER, Greta R. Democracy of Credit: Ownership and the Politics of Credit Access in Late Twentieth-Century America. *American Journal of Sociology*, v. 123, n. 1, p. 1–47, 2017.

MAIOLINO, Isabela; TIMM, Luciano Benetti (Orgs). *Direito do consumidor:* novas tendências e perspectiva comparada. Brasília: Editora Singular, 2019.

PRIMEIRA audiência pública do STJ terá transmissão pelo YouTube. Revista Consultor Jurídico. Disponível em: <http://www.conjur.com.br/2014-ago-24/primeira-audiencia-publica-stj-transmissao-youtube>. Acesso em: 26 de abr. de 2023.

RAMOS, Igor Násser Alves et al. Reflexos da Lei do Cadastro Positivo e da Lei Geral de Proteção de Dados-aspectos "conflituosos" entre privacidade e fomento ao crédito: um estudo a partir do diálogo das fontes. *Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro*, Rio de Janeiro, 2019.

SEBBEN, Naiara Anna. Mercado de crédito, LGPD e cadastro positivo: Reflexões acerca da Lei n° 13.709/2018 e da Lei Complementar n° 166/2019. Londrina, PR: Thoth, 2021.

SIMÃO, Bárbara Prado. *Entre privacidade e eficiência econômica: a trajetória da pontuação de crédito no Brasil.* 2022. Tese de Doutorado.

SIQUEIRA, Carol. Cadastro positivo obrigatório gera debate sobre privacidade e bancos. Agência Câmara de Notícias. Brasília, 19 de jan. de 2019. Disponível em:<https://www.camara.leg.br/noticias/552246-cadastro-positivo-obrigatorio-gera-debate-sobre-privacidade-e-bancos/>. Acesso em: 3 de mai. de 2023.

ZANATTA, Rafael AF. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Publicado em: fevereiro de 2019.

ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile books, 2019.

APLICAÇÃO DA LGPD NO SETOR DE TRANSPORTES

Tayná Frota de Araújo[1]

Resumo: Este artigo objetiva discutir o desenvolvimento de medidas voltadas à proteção de dados pessoais no setor de transportes brasileiro. A partir da metodologia qualitativa, com análise sobre obras doutrinárias e pesquisa legislativa, o estudo parte da proteção constitucional do direito ao transporte e dos dados pessoais para avaliar as condições de legitimidade previstas na Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, para avaliar a harmonização de diferentes fontes do direito em prol da proteção dos titulares, analisou-se as principais normas do setor, além do acórdão do E-RR-933-49.2012.5.10.0001 do Tribunal Superior do Trabalho (TST).

Palavras-chave: Transporte; LGPD; Proteção de Dados Pessoais; Guia de Boas Práticas.

Abstract: *This article aims to discuss the development of measures aimed at protecting personal data in the Brazilian transportation sector. Using a qualitative methodology, with an analysis of doctrinal papers and legislative research, the study starts from the constitutional protection of the right to transportation and personal data to evaluate the conditions of legitimacy provided for in the Brazilian Data Protection Law (LGPD). In addition, in order to assess the harmonization of different sources of law for the protection of data subjects, the main regulations in the sector were analyzed, as well as the Superior Labor Court (TST) decision on E-RR-933-49.2012.5.10.0001.*

Keyworsds: *Transportation; LGPD; Personal Data Protection; Code of Conduct.*

[1] Pós-graduanda em Direito Digital e Proteção de Dados do Instituto Brasiliense de Direito Público (IDP). Bacharel em Direito pela Universidade de Brasília (UnB). Pesquisadora do Centro de Direito, Internet e Sociedade (CEDIS) do IDP e coordenadora Privacy Lab-CEDIS/IDP. Coordenadora de Estudos do Observatório da LGPD/UnB. Pesquisadora do Centro de Estudos Constitucionais Comparados (CECC)/UnB. Gerente da Women Inside Trade (WIT) Starters e da Women In Antitrust (WIA). Advogada.

Introdução

O setor de transportes permite "a circulação das pessoas e das mercadorias utilizadas por elas e, por consequência, a realização das atividades sociais e econômicas desejadas"[2]. Ele não se restringe apenas aos aspectos técnicos, também envolve uma "questão social e política" diante da ordenação desenvolvida para gerir o fluxo de pessoas e produtos nos meios urbano e rural[3]. Trata-se, portanto, de um setor crítico à sociedade[4] e à economia, já que é o "principal responsável pelos fluxos de bens" e representa "uma grande parcela dos custos logísticos dentro da maioria das empresas"[5].

Portanto, a adequação à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018 ou LGPD), é um processo relevante para garantir maior segurança do uso de dados pessoais e permitir o desenvolvimento de novos modelos de negócios, inclusive a nível internacional. Neste setor, verifica-se, por exemplo, a necessidade de atenção aos dados pessoais de passageiros, dos próprios profissionais que atuam no setor e parceiros envolvidos, tendo em vista o direito à proteção de dados pessoais (art. 5º, LXXIX, da Constituição Federal), resguardado constitucionalmente após aprovação da Emenda Constitucional n. 115/2022, e ao próprio transporte (art. 6º, da Constituição Federal), enquanto direito social garantido após a promulgação da Emenda Constitucional 90/2015.

Sob tal panorama, este artigo propõe-se a avaliar o setor econômico do transporte e os principais aspectos quanto à sua adequação à LGPD por meio da análise de obras doutrinárias e pesquisa legislativa, dividindo-se em quatro partes centrais. Primeiro, serão analisadas as características do setor de transportes no Brasil, com destaque ao marco normativo firmado na Constituição Federal. Em seguida, serão discutidas as condições de legitimidade para o tratamento de dados pessoais no setor de transportes, com revisão da literatura especializada e da LGPD, para análise das hipóteses para tratamento de dados pessoais de trabalhadores e passageiros.

Posteriormente, em pesquisa não exaustiva, serão apresentadas disposições legais a nível federal do setor que alcançam a proteção de dados pessoais, como a Lei n. 13.103/2015,

---

[2] VASCONCELLOS, Eduardo Alcântara de. *Transporte e meio ambiente*: conceitos e informações para análise de impactos. São Paulo: Ed. Annablume, 2006. p. 11.
[3] ALBANO, João Fortini. *Vias de Transporte*. Porto Alegre: Bookman, 2016. p. 3.
[4]BOWCUT. *Transportation Industry*. Disponível em: <https://cybersecurityguide.org/industries/transportation/>. Acesso em 21 mar. 2023.
[5] ALBANO, João Fortini. Vias de Transporte. Porto Alegre: Bookman, 2016. p. 2.

que dispõe sobre o exercício da profissão de motorista e disciplina a jornada de trabalho do motorista profissional.

O "Guia de Boas Práticas de Proteção de Dados no Setor de Transporte" elaborado pelo Sistema CNT (Confederação Nacional do Transporte) também será objeto de algumas considerações por ser um dos primeiros guias setoriais que propõe medidas específicas aos agentes de tratamento de dados deste setor.

Por fim, os fundamentos adotados no acórdão dos Embargos de Declaração no Recurso de Revista nº 933-49.2012.5.10.0001 no âmbito do Tribunal Superior do Trabalho (TST) serão brevemente analisados para considerações sobre como os dispositivos da LGPD foram utilizados em caso prático que afeta diretamente o setor econômico em análise, relativo à legalidade ou não da construção de um banco de dados de motoristas no sistema rodoviário.

1. Principais características do Setor de Transportes e proteção constitucional: direito ao transporte e à proteção de dados pessoais

Tradicionalmente, o setor de transportes envolve quatro modalidades: (i) terrestre (carros, caminhões, ônibus e trens); (ii) aquático: navios e barcos; (iii) aéreo: aviões e helicópteros; e (iv) tubular: gasodutos e oleodutos[6]. A Lei n. 10.233/01 foi responsável por reestruturar os transportes aquaviário e terrestre e, dentre as demais providências, criou o Conselho Nacional de Integração de Políticas de Transporte, a Agência Nacional de Transportes Terrestres (ANTT), a Agência Nacional de Transportes Aquaviários (ANTAQ) e o Departamento Nacional de Infraestrutura de Transportes (DNIT).

Por sua vez, a Agência Nacional de Aviação Civil (ANAC) foi instituída em 2005, através da Lei n. 11.182/2005, em substituição ao então Departamento de Aviação Civil (DAC), e atualmente é regulamentada pelo Decreto n. 5.731, de 20 de março de 2006. A Agência, assim como as demais, é uma autarquia vinculada ao Ministério da Infraestrutura, especificamente responsável por regular e fiscalizar as atividades de aviação civil e da infraestrutura aeronáutica e aeroportuária.

De pronto, deve-se considerar que em razão das particularidades de cada modal de transporte, as regulamentações são descentralizadas, isto é, cada modal tende a possuir

[6] ALBANO, João Fortini. Vias de Transporte. Porto Alegre: Bookman, 2016. p. 5.

normativas próprias e específicas. Além disso, existem previsões de normas de segurança para os passageiros, trabalhadores, bens de consumo e até mesmo com relação ao meio ambiente, como no caso do ambiente marinho. Dessa forma, não se objetiva, neste texto, listar exaustivamente todas as normas particulares relacionadas ao tratamento de dados pessoais em cada modal de transporte brasileiro, mas sim debater as normas centrais e abrangentes que possam se aplicar a todos os meios.

Partindo da Constituição, importa considerar que, no Brasil, o transporte é um dos direitos sociais previstos no art. 6º, sendo um dos exemplos de "direitos a prestação material dos direitos sociais", vinculando Estado e particulares ao "propósito de atenuar desigualdades fáticas de oportunidades"[7]. Ademais, o direito ao transporte também possui previsão específica no art. 7º da Constituição, que dispõe sobre os direitos dos trabalhadores urbanos e rurais, como uma das formas que "visem à melhoria de sua condição social".

A Constituição, ao adotar o princípio da predominância do interesse para a repartição de competências entre os entes políticos[8], destinou, à União, a competência privativa para legislar sobre as diretrizes da política nacional de transportes, e trânsito e transporte, como uma das formas de se garantir o desenvolvimento urbano. Assim, os Estados e o Distrito Federal podem, no âmbito da competência legislativa concorrente, legislar sobre direito urbanístico; enquanto, aos Municípios, cabe legislar sobre os transportes coletivos, porque são serviços públicos de interesse local, que possuem o caráter essencial e compõem a política de desenvolvimento urbano.

O art. 178 da Constituição Federal merece destaque porque indica a necessidade de observância às normas internacionais presentes em "acordos firmados pela União, atendido o princípio da reciprocidade". Seria possível considerar, assim, que as normas internacionais não estão restritas ao *modus operandi* dos transportes, mas podem ser capazes de envolver boas práticas ao setor como um todo, inclusive, em proteção de dados. Esta perspectiva pode ser relevante pois, em algumas temáticas como transferência internacional de dados, poderão ser

[7] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 16ª ed. São Paulo: Saraiva Educação, 2021. p. 72-73.

[8] SILVA, José Afonso. Curso de Direito Constitucional Positivo. 43ª ed. São Paulo: Malheiros Editores, 2014, p. 482. Veja-se, a título de exemplo, a fundamentação sobre o tema nos autos da ADI 4.615/CE. Trecho da ementa: "(...) 1. O princípio norteador da repartição de competências entre os entes componentes do federalismo brasileiro é o princípio da predominância do interesse (...). Quando surgem dúvidas sobre a distribuição de competências para legislar sobre determinado assunto, caberá ao intérprete priorizar o fortalecimento das autonomias locais e o respeito às suas diversidades como características que assegurem o Estado Federal, garantindo o imprescindível equilíbrio federativo. (...)". (STF, Ministro relator Roberto Barroso, julgado em Sessão Virtual entre 13 a 19 de setembro de 2019).

reconhecidos padrões estrangeiros desde que respeitem os "princípios, dos direitos do titular e do regime de proteção de dados" estipulados pela LGPD (art. 33, II).

Por sua vez, a garantia à proteção de dados pessoais também é reconhecida como direito fundamental pela Constituição (art. 5º, LXXIX). Este reconhecimento, como indicado por Danilo Doneda, se deve ao fato de que o tratamento de dados pessoais é uma atividade de risco "à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada"[9]. Portanto, deve-se considerar o direito à proteção de dados pessoais enquanto um direito "autônomo e fundamental"[10].

A aplicação - material e territorial - da LGPD exige a adequação de todos os agentes, pessoas físicas e jurídicas, que realizem o tratamento de dados pessoais, nos termos dos arts. 3º e 4º da LGPD. Ademais, vale destacar que outras normas do ordenamento brasileiro asseguram a proteção dos direitos dos titulares, como o próprio Código Civil e o Direito do Consumidor[11], diante da harmonização da disciplina de proteção de dados no sistema jurídico brasileiro.[12]

Ambos os direitos, ao transporte e à proteção de dados pessoais, foram incluídos expressamente na Constituição em um intervalo inferior a dez anos, e são marcos importantes para a promoção da dignidade humana e proteção do cidadão das ações de entes públicos e privados. A partir destas premissas, passa-se ao tópico seguinte para breve avaliação das condições que permitem o tratamento de dados pessoais de modo legítimo, conforme definido pela LGPD, relativas particularmente aos princípios e bases legais para o tratamento.

---

[9] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, v. 12, n. 2, jul/dez. 2011. p. 103.

[10] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, v. 12, n. 2, jul/dez. 2011. p. 103.

[11] A respeito, confira-se: DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 3-20. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019.

[12] MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo à Erik Jaime. In: MARQUES, Cláudia Lima (Coord.). Diálogo das fontes: do conflito à coordenação de normas do direito brasileiro. São Paulo: *Revista dos Tribunais*, 2012. Pesquisas empíricas sobre a aplicação da LGPD em decisões judiciais brasileiras já observam esta tendência. Para mais informações, acesse a segunda edição do Painel LGPD nos Tribunais, desenvolvido pelo CEDIS/IDP, com colaboração do Jusbrasil e apoio do PNUD: <https://painel.jusbrasil.com.br/>.

2. Condições de legitimidade para o tratamento de dados no Setor de Transportes

A LGPD possui uma dupla função de "garantir a privacidade e outros direitos fundamentais [e] fomentar o desenvolvimento econômico"[13]. A tutela dos direitos dos titulares dos dados pessoais[14] (a pessoa humana) é a razão que se sobressai, reconhecendo-se, historicamente, que não existem dados irrelevantes[15] e todo dado pessoal merece ser tutelado[16–17]. Além disso, é importante ter como premissa a avaliação contextual em que o tratamento ocorre[18], para que seja preservado o fluxo de informações atualmente sem perder a geração de valor e proteção aos direitos dos titulares, com base na transparência e segurança da informação.

Conforme o modelo geral de aplicação da LGPD[19], para que o tratamento seja considerado legítimo, deve-se considerar se as bases legais estão diretamente relacionadas à finalidade do tratamento e se este ocorre em respeito aos onze princípios previstos pela LGPD em seu art. 6º, os quais definem diretrizes para a conformidade do tratamento de dados.

Os princípios, enquanto parâmetros, devem guiar todas as etapas do tratamento de dados pessoais. A tríade formada pelos princípios da finalidade, adequação e necessidade, possui relevância por exigir que todo tratamento de dados pessoais seja específico, razoável e proporcional à finalidade delimitada da operação.

Os dados pessoais sensíveis, por terem um alto potencial de risco discriminatório, exigem maiores salvaguardas para sua proteção e apenas podem ser tratados conforme as bases legais específicas previstas no art. 11 da LGPD. Aqui, o princípio da não-discriminação é um

---

[13] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: as funções e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021, p. 108.

[14] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor* - Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 32

[15] No âmbito internacional, trata-se da decisão do Tribunal Constitucional alemão sobre a Lei do Censo de 1983, enquanto no Brasil a decisão do Supremo Tribunal Federal no caso IBGE de 2020, ADI 6387, preconiza este entendimento. Para discussões sobre as duas principais decisões emblemáticas neste sentido, consulte: SCHERTEL, 2014; BIONI, 2021; TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com* - Revista Eletrônica de Direito Civil, v. 9, p. 1-38, 2020.

[16] MENDES, Laura Schertel; DONEDA, Danilo. 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, 2018.

[17] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista De Direitos E Garantias Fundamentais,* 19(3), 2018, p. 159–180. Disponível em: <https://doi.org/10.18759/rdgf.v19i3.1603>. Acesso em: 5.jul.2023.

[18] NISSENBAUM, Helen. *Privacy in context*: Technology, policy, and the integrity of social life. Stanford University Press, 2020.

[19] MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *Caderno Especial LGPD*. São Paulo: Ed. RT, novembro. 2019, p. 35-56.

dos “mais relevantes” por orientar o uso “potencialmente lesivo” de dados sensíveis, diante de “sua capacidade discriminatória, seja por entes privados - i.e. fornecedoras de produtos e serviços - seja por entes públicos”[20].

Não há hierarquia ou preferência entre as bases legais previstas pela LGPD,[21] e a sua aplicação deve ser considerada casuisticamente, obedecendo às limitações impostas e o regime diferenciado conferido aos dados pessoais sensíveis. Independente da seleção de qual base legal é aplicável, esta escolha deve ser justificada conforme cada caso concreto e precisa ser registrada na etapa de mapeamento dos processos que envolvem o tratamento de dados - como se observa de forma explícita no art. 37 da LGPD imposta ao controlador e operador.

Nesse sentido, algumas atividades de tratamento podem trazer mais desafios práticos por envolverem maior fluxo de dados pessoais sensíveis, como por exemplo: a gestão de funcionários e contratados e a gestão de dados pessoais de passageiros. Como essas atividades tendem a ser comuns independente do modal, elas serão objeto de análises a seguir.

2.1. Boas práticas para o tratamento de dados pessoais de funcionários

Por envolver uma relação empregatícia, o tratamento de dados pessoais de funcionários normalmente é dividido em quatro fases centrais: (i) fase pré-contratual, para realização de processos seletivos; (ii) processo de contratação, para confecção do contrato de trabalho; (iii) execução do contrato de trabalho, com o exercício da atividade objetivada pelo contrato; (iv) fase pós-contratual, com o encerramento da relação trabalhista.

Nestas etapas, diversos dados pessoais são tratados para permitir a identificação do titular, inclusive, para a própria operacionalização do contrato firmado. Neste sentido, o nome completo, endereço (físico e de e-mail), telefone, RG, CPF, dentre outros, podem ser tratados. Dados pessoais sensíveis também podem ser tratados, como os dados de saúde (exames admissionais e complementares, carteira de vacinação, laudos para comprovação de deficiência física) e dados relacionados à religião, como nos casos em que se verifica a disponibilidade

[20] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista De Direitos E Garantias Fundamentais*, 19(3), 2018, p. 159–180. Disponível em: <https://doi.org/10.18759/rdgf.v19i3.1603>. Acesso em: 5.jul.2023.
[21] Entendimento consolidado pelo Enunciado 4889 da IX Jornada de Direito Civil (2022).

para trabalhar em certos dias da semana, que exigem maiores salvaguardas por partes dos empregadores para evitar possíveis abusos e usos ilegais dessas informações.

Portanto, a base legal da execução de contrato (art. 7º, V, da LGPD) pode ser aplicável às fases (i) a (iii), quando necessário para avaliação do currículo e elaboração dos documentos que estabeleçam o vínculo entre empregador e empregado. Quando do processo de contratação (ii) e de execução do contrato (iii), além referida base legal, é possível o uso do exercício regular de direitos (art. 11, II, d, da LGPD), pois o titular é parte efetiva do contrato.

O exercício regular de direitos e o cumprimento à obrigação legal podem ser apropriados na fase (iv), em que há mais possibilidade de processos judiciais ocorrerem (art. 11, CLT) e as instituições empregadoras devem seguir períodos específicos de armazenamento das informações, como para fins de comprovação do tempo de serviço e demandas envolvendo aposentadoria.

Nas relações trabalhistas, por causa da relação de subordinação existente, deve-se evitar o uso da base legal do consentimento, pois há maiores chances de estar em risco a efetividade de suas características: a manifestação livre, informada e inequívoca do titular (art. 5º, XII, da LGPD) e, quando para dados pessoais sensíveis, o consentimento de forma específica e destacada (art. 11, I, da LGPD). Identifica-se que nestas situações, a liberdade para o fornecimento do consentimento do titular pode ser prejudicada em razão da hierarquia existente[22].

Com relação às obrigações legais dos empregadores desse setor econômico e o tratamento de dados pessoais sensíveis, o Guia de Boas Práticas do Setor de Transporte[23], produzido pelo Sistema CNT, traz importantes exemplos para avaliação, como os relativos a "dados biométricos, imagem e reconhecimento facial" (protocolo específico 3.2) e "protocolo de exames toxicológicos e testes de bafômetro" (protocolo específico 3.3).

Sobre o tema, em junho de 2023, a Lei n. 14.599/2023[24] realizou modificações no Código de Trânsito Brasileiro e impôs consequências aos condutores (das categorias C, D e E)

---

[22] ARTICLE 29 WORKING PARTY - WP29. *Guidelines on consent under Regulation 2016/679*. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf >. Acesso em: 18 set. 2023.

[23] CNT. *Guia de Boas Práticas de Proteção de Dados no Setor de Transporte*. Disponível em: <http://xn--guia%20de%20boas%20prticas%20de%20proteo%20de%20dados%20no%20setor%20de%20transporte-g0g4qwn5453vbfa/>. Acesso em: 16 jan. 2023.

[24] BRASIL. *Lei n. 14.599*, de 19 de junho de 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14599.htm>. Acesso em: 19 set. 2023.

que testarem positivo aos exames toxicológicos, como a "suspensão do direito de dirigir pelo período de 3 (três) meses, condicionado o levantamento da suspensão à inclusão no Renach de resultado negativo em novo exame" (art. 148-A), ou se recusarem a realizá-los.

Devida à sensibilidade das informações referentes aos resultados de exames toxicológicos e testes de bafômetro, é importante assegurar a confidencialidade e segurança no tratamento dos dados e que seu uso se limite às finalidades específicas para os quais foram coletados e tratados, em especial sob o prisma do princípio da não discriminação. O Guia do Sistema CNT também recomenda que as "empresas e organizações devem documentar e divulgar amplamente para os motoristas profissionais empregados (ou celetistas)"[25] tais informações, que abranja inclusive, dentre outros pontos, o seu tempo de armazenamento.

Portanto, é aconselhável a avaliação cautelosa da finalidade pretendida e se de fato é necessário o tratamento de dados pessoais sensíveis em cada situação, pois, quando possível, estes não devem ser utilizados por apresentarem mais riscos aos titulares. Mesmo quando imprescindíveis, outras medidas que visem à anonimização e à pseudonimização destas informações, bem como o reforço nas medidas de segurança, devem ser incentivadas.

2.2. Boas práticas para o tratamento de dados pessoais de passageiros

Os dados pessoais de passageiros podem ser coletados para a sua identificação e contato (que podem ser dados cadastrais), e envolver desde o nome completo, endereço (residencial e eletrônico) e telefone (pessoal e para contato de emergência), como dados para fins de realização de pagamento, que abrangem informações financeiras sobre o cartão de débito e crédito e o IBAN (*International Bank Account Number* - padrão de identidade internacional de contas bancárias); e dados relativos à reserva e passagens de transporte, que permitam a identificação do consumidor e a prestação do serviço contratado.

Assim, para esses casos, identifica-se como apropriada as bases legais para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art. 7º, V, da LGPD) e o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II, e art. 11, a, da LGPD).

[25] CNT. *Guia de Boas Práticas de Proteção de Dados no Setor de Transporte*. p. 94 Disponível em: <http://xn--guia%20de%20boas%20prticas%20de%20proteo%20de%20dados%20no%20setor%20de%20transporte-g0g4qwn5453vbfa/>. Acesso em: 16 jan. 2023.

A respeito, existem situações em que crianças e adolescentes viajam sem o acompanhamento de seus responsáveis legais, e a Resolução ANTT n. 5.846/2019[26], que regulamenta a Lei n. 13.812/2019[27], define que, em viagens nacionais, é necessária expressa autorização judicial para viagem de criança ou adolescente menor de 16 anos para "fora da Comarca de onde reside, desacompanhada dos pais ou responsável".

No modal aeroviário, desde 2021, a autorização para menores de 16 anos em voos domésticos pode ser emitida em formato digital, por meio da Autorização Eletrônica de Viagem (AEV), regulamentado pelo Conselho Nacional de Justiça[28]. Assim, em ambos os casos é necessária a apresentação de documentos de identificação e os exigidos por lei para que as prestadoras de serviços de transporte certifiquem a regularidade da viagem. Nestas situações, por envolverem menores de idade, todo o processo deve atender o seu melhor interesse (art. 14, da LGPD) e a autorização de seus responsáveis legais.

É possível que informações sensíveis, quando estritamente necessárias, também sejam compartilhadas, como aquelas relativas à saúde e à necessidade de cuidados especializados, indicação de deficiências físicas e restrições alimentares. Nestes casos, pode ser apropriada a base legal para cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II, e art. 11, a, da LGPD). Se necessário, o tratamento para a tutela da saúde (art. 7º, VIII, e art. 11, f da LGPD), há restrição expressa para que o tratamento só aconteça "por profissionais de saúde, serviços de saúde ou autoridade sanitária".

Para a coleta de dados biométricos, recomenda-se o desenvolvimento do Relatório de Impacto de Proteção de Dados Pessoais (RIPD) para que sejam avaliados de forma apropriada as finalidades do tratamento, contexto e aspectos de risco (como suas fontes e âmbito de aplicação). É recomendável que este documento seja elaborado antes do início do tratamento dos dados pessoais para a finalidade desejada ou "assim que se identificar um tratamento que

---

[26] BRASIL. ANTT. *Resolução n. 5846/2019*. Disponível em: <https://anttlegis.antt.gov.br/action/ActionDatalegis.php?acao=detalharAto&tipo=RES&numeroAto=00005846&seqAto=000&valorAno=2019&orgao=DG/ANTT/MI&codTipo=&desItem=&desItemFim=&cod_menu=5408&cod_modulo=161&pesquisa=true>. Acesso em: 17 set. 2023.

[27] BRASIL. *Lei n. 13.812*, de 16 de março de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13812.htm#:~:text=LEI%20N%C2%BA%2013.812%2C%20DE%2016%20DE%20MAR%C3%87O%20DE%202019&text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,da%20Crian%C3%A7a%20e%20do%20Adolescente). Acesso em: 17 set. 2023.

[28] ANAC. *Autorização para viagens de menores desacompanhados dos pais em voos domésticos poderá ser feita em formato digital*. Versão atualizada em 30 de jul. 2021. Disponível em: https://www.gov.br/anac/pt-br/noticias/2021/autorizacao-para-viagens-de-menores-desacompanhados-dos-pais-em-voos-domesticos-podera-ser-feita-em-formato-digital. Acesso em: 18 de set. 2023.

possa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados"[29].

No uso de aplicativos e sites, como para fins de *check-in*, venda de passagens e acompanhamento das informações de viagem, as instituições responsáveis devem se atentar ao mínimo necessário para cada finalidade específica, aplicável ao uso de recursos como cookies e coleta de imagens para fins de comprovação da identidade da pessoa.

Para ações de marketing, é possível o uso das bases legais do consentimento e do legítimo interesse, esta em especial para quando já houver uma relação comercial entre os passageiros e as empresas. Opções como o envio de *newsletter* e oferta de promoções aos consumidores devem garantir as opções de entrada (*opt-in*) e saída (*opt-out*) de forma clara, acessível e facilitada.

Além disso, informações para exercício de direitos, como os meios de contato com o Encarregado, devem ser acessíveis e recomenda-se, particularmente para empresas estrangeiras, a disponibilização dos conteúdos em língua portuguesa para facilitar o acesso e compreensão das informações por parte do público brasileiro.

Portanto, estabelecidas as premissas iniciais que permitem a avaliação da legitimidade de tratamento de dados pessoais conforme a LGPD a partir de alguns exemplos de atividades do setor de transportes, o próximo item pretende tratar de algumas das obrigações relativas ao tema dispostas em legislações específicas. Em razão de seu caráter principiológico e geral, a LGPD não regula de forma pormenorizada cada um dos setores econômicos, evitando-se assim que a Lei "não caia rapidamente na obsolescência nem suscite 'pontos cegos' quanto à sua aplicabilidade"[30], o que exige atenção às particularidades do tema aos meios de transporte.

3. Legislação Setorial e boas práticas no Setor de Transportes

Considerando que as atividades de transporte são reguladas no Brasil por agências autárquicas específicas, o presente tópico destina-se a avaliar alguns dos principais exemplos da legislação setorial no setor a nível federal. A análise não pretende ser exaustiva, mas sim

[29] ANPD. *Relatório de Impacto à Proteção de Dados Pessoais* (RIPD). Versão atualizada em 6 abr. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3>. Acesso em 19 set. 2023.

[30] MENDES, Laura Schertel; DONEDA, Danilo. 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, 2018, p. 24.

exemplificativa, de modo a destacar, através destas normas, as obrigações particulares quanto à proteção de dados pessoais e que, portanto, podem iniciar o debate quanto às melhores práticas para a adequação do setor à LGPD e para a proteção dos direitos dos titulares.

No âmbito federal, a Lei n. 11.442/2007, que dispõe sobre o transporte rodoviário de cargas por conta de terceiros e mediante remuneração, sofreu modificação em 2015 por meio da Lei n. 13.103/2015. Houve a inclusão do art. 13-A, proibindo a "utilização de informações de bancos de dados de proteção ao crédito como mecanismo de vedação de contrato com o TAC e a ETC devidamente regulares para o exercício da atividade do Transporte Rodoviário de Cargas". Este dispositivo é relevante pois estipula e limita legalmente a finalidade do tratamento de dados pessoais, podendo ser exemplo de uma obrigação legal (arts. 7º, II e art. 11, II, a, da LGPD) aplicável aos agentes de tratamento.

A Lei n. 13.103/2015, referente ao exercício da profissão de motorista, também trouxe modificações no Decreto-Lei n. 5.452/1943 (Consolidação das Leis do Trabalho - CLT), responsabilizando o empregado, e o ajudante empregado nas operações em que acompanha o motorista (art. 235-C, §16), pela "guarda, preservação e exatidão das informações contidas" em (i) "anotações em diário de bordo, papeleta ou ficha de trabalho externo" ou (ii) "no registrador instantâneo inalterável de velocidade e tempo", ou (iii) "nos rastreadores ou sistemas e meios eletrônicos, instalados nos veículos, normatizados pelo Contran, até que o veículo seja entregue à empresa". Estas informações, quando vinculadas a uma pessoa física identificada ou identificável, se referem a dados pessoais, o que atrai a aplicação da LGPD.

O Código de Trânsito Brasileiro (Lei n. 9.506/1997) define dentre as atribuições dos órgãos e entidades executivos rodoviários da União, dos Estados, do Distrito Federal e dos Municípios, no âmbito de sua circunscrição (art. 21), a coleta de dados e elaboração de estudos sobre os sinistros de trânsito e suas causas (art. 21, IV), conforme redação dada pela Lei n. 14.599/2023.

Ademais, nesta Lei, também há a obrigação de fornecimento dos dados cadastrais dos veículos registrados e dos condutores habilitados para fins de imposição e notificação de penalidades e de arrecadação de multas nas áreas de suas competências (art. 21, inciso XIV), aos órgãos e entidades executivos de trânsito e executivos rodoviários municipais. Assim, vale ressaltar o necessário zelo com as medidas de segurança da informação e proteção de dados

para permitir o fluxo informacional seguro e a execução de políticas públicas[31] por parte da Administração, amparado legalmente e conforme a competência estabelecida a cada um dos entes públicos.

A Lei n. 14.071/2020, a qual alterou a composição do Conselho Nacional de Trânsito e ampliou o prazo de validade das habilitações, registrou a modificação no art. 129-B para garantir expressamente a observância à LGPD, e ao Código Civil, ressaltando o necessário diálogo das fontes que devem ser operadas no ordenamento brasileiro. A alteração se refere aos casos de "registro de contratos de garantias de alienação fiduciária em operações financeiras, consórcio, arrendamento mercantil, reserva de domínio ou penhor" realizados em "órgãos ou entidades executivos de trânsito dos Estados e do Distrito Federal".

O Decreto n. 8.033/2013, sobre as disposições legais que regulam a exploração de portos organizados e de instalações portuárias, apresenta, em seu art. 40, a criação de um banco de dados próprio para "organizar a identificação e a oferta de mão de obra qualificada para o setor portuário, intitulado SINE-PORTO". Este dispositivo também contém o conteúdo mínimo sobre cada indivíduo: "identificação do trabalhador", "qualificação profissional obtida para o exercício das funções" e "registro ou cadastramento em órgão de gestão de mão de obra, quando couber".

Entretanto, o art. 40 do Decreto n. 8.033/2013 não apresenta explicitamente quais dados seriam necessários para a "identificação" do trabalhador ou quais informações seriam relativas ao campo da "qualificação profissional", por exemplo. Este dispositivo, inclusive, foi editado pelo Decreto n. 8.071/2013, modificando a versão original para excluir do *caput* a então menção direta à finalidade do banco de dados para "trabalhadores portuários avulsos e demais trabalhadores portuários". Logo, os princípios da finalidade, adequação e transparência devem orientar todas as etapas de tratamento de dados pessoais, evitando-se o uso de dados excessivos que representam mais riscos aos titulares.

Além disso, outras normas estabelecem obrigações aos agentes de tratamento de dados do setor de transportes. Um dos exemplos é o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas - eSocial, instituído pelo Decreto n. 8.373/2014. Neste Decreto, estipula-se que o eSocial contenha informações fiscais, previdenciárias e trabalhistas

[31] Não desconsiderando a vasta discussão jurídica sobre o conceito de "políticas públicas por parte da Administração", adota-se neste texto o seu o sentido amplo "para definir uma ação administrativa coordenada em busca de determinado objetivo relevante" (FRAZÃO, Ana. CARVALHO, Angelo Prata de. MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2022, p. 127).

(art. 2º, I), e devem ser prestadas por entes como o "empregador, inclusive o doméstico, a empresa e os que forem a eles equiparados em lei" (art. 2º, §1º, I), o segurado especial (art. 2º, §1º, II) e "as pessoas jurídicas de direito público da União, dos Estados, do Distrito Federal e dos Municípios" (art. 2º, §1º, III).

Ao considerar a atuação de outros agentes e possíveis fontes que orientem as melhores condutas para proteção de dados, o Sistema CNT tem destaque pois foi a primeira entidade do setor a publicar um Guia de Boas Práticas do Setor de Transporte[32] em 2021. O Guia, que contou com a coordenação científica do Professor Danilo Doneda, é uma importante iniciativa promovida pelos próprios participantes do setor econômico em termos de promoção à cultura de proteção de dados pessoais.

O documento, organizado em três partes principais, dispõe inicialmente de um resumo sobre a aplicação da LGPD no setor e delimita a sua aplicação aos "prestadores de serviços de transporte de passageiros e de cargas, bem como de serviços de logística e infraestrutura para transporte"[33]. Em seguida, o documento contém oito "Protocolos Gerais" e três "Protocolos Específicos", que apresentam um bom panorama de quais ações são e podem ser aprimoradas conforme o cotidiano das principais operações que envolvem dados pessoais para os transportadores. Dessa forma, o Guia pretende colaborar com a aplicação da LGPD aos prestadores de serviços de transporte de passageiros e de cargas, além de serviços de logística e infraestrutura para transporte, enquanto participantes do Sistema CNT.

A respeito dos protocolos específicos, relativos aos tratamentos para uso de cartões de transporte; imagem, biometria e reconhecimento facial; e exames toxicológicos; vale destacar a identificação apresentada quanto aos titulares dos dados pessoais, finalidade do tratamento, possíveis bases legais autorizativas e o período de armazenamento previsto. Estes são parâmetros iniciais necessários que orientam os agentes de tratamento de dados pessoais nos processos de mapeamento, identificação de riscos e solução de salvaguardas adicionais.

Dessa forma, o Guia de Boas Práticas é um dos principais exemplos deste setor econômico para a construção conjunta de orientações específicas aos desafios da área e pode

[32] CNT. *Guia de Boas Práticas de Proteção de Dados no Setor de Transporte*. Disponível em: <http://xn--guia%20de%20boas%20prticas%20de%20proteo%20de%20dados%20no%20setor%20de%20transporte-g0g4qwn5453vbfa/>. Acesso em: 16 jan. 2023.
[33] CNT. *Guia de Boas Práticas de Proteção de Dados no Setor de Transporte*. p. 33 Disponível em: <http://xn--guia%20de%20boas%20prticas%20de%20proteo%20de%20dados%20no%20setor%20de%20transporte-g0g4qwn5453vbfa/>. Acesso em: 16 jan. 2023.

representar futuramente importante passo para uma possível autorregulação, nos termos do art. 50 da LGPD. Além disso, a Lei estabelece que a ANPD pode reconhecer a divulgar as regras firmadas a partir da iniciativa dos controladores e operadores quando da formulação de regras de boas práticas e de governança (art. 50, §3º), exigindo um papel de liderança e colaboração conjunta dos agentes de tratamento de dados pessoais.

Após estas considerações quanto à legislação setorial aplicada ao Transporte nacional e boas práticas, o item seguinte analisará a decisão proferida pelo Tribunal Superior do Trabalho em caso relativo à contratação de motoristas para que, com base no discutido até o momento, avaliar quais e como as premissas da LGPD foram utilizadas em um caso concreto e de interesse ao setor.

4. Setor de Transportes e LGPD na Justiça do Trabalho: breves considerações sobre o acórdão do TST nos E-RR-933-49.2012.5.10.0001

Um dos primeiros casos a ter repercussão que envolveu representantes do setor de transportes e os preceitos LGPD se refere ao acórdão proferido pela Subseção I Especializada em Dissídios Individuais (SDI-1) do TST, no julgamento dos Embargos de Declaração no Recurso de Revista nº 933-49.2012.5.10.0001[34].

No julgado, questionou-se a licitude da atividade de uma empresa de gerenciamento de risco, a GPS Logística e Gerenciamento de Riscos S.A., em formar banco de dados sobre as restrições creditícias de motoristas profissionais e o compartilhamento destas informações com empresas contratantes.

O Ministério Público do Trabalho (MPT), autor da Ação Civil Pública, requereu que a GPS se abstivesse dessa atividade, uma vez que existiriam outros meios para avaliar se as empresas se certificam de que seus patrimônios não correm riscos, "como o controle de mercadoria, instalação de rastreadores, escoltas etc.". A avaliação da licitude da empresa, portanto, afeta diretamente o modal rodoviário de transporte, uma vez que o escopo de sua atuação alcança empregados e candidatos a trabalho deste setor.

[34] Acórdão publicado em 25 de fevereiro de 2022. Ministro relator Alberto Bresciani. Disponível em: <https://consultadocumento.tst.jus.br/consultaDocumento/acordao.do?anoProcInt=2014&numProcInt=246606&dtaPublicacaoStr=25/02/2022%2007:00:00&nia=7779648>. Acesso em: 12. jun. 2023.

No âmbito da proteção de dados pessoais, a relevância da decisão se deve à análise da licitude da empresa exigir a adequação do tratamento de dados pessoais com a LGPD[35]. Por maioria, a Subseção I Especializada em Dissídios Individuais do TST proibiu que a GPS utilize banco de dados ou preste informações sobre restrições de créditos de candidatos a emprego em transportadoras de carga.

O Tribunal reconheceu a tutela inibitória e a natureza preventiva da demanda e considerou que a *ratio* presente na Lei 11.442/2007 limita o uso de dados disponíveis publicamente para fins de proteção do crédito, inviabilizando que estas informações sejam utilizadas para outras finalidades. Para a análise do caso concreto, considerou-se a Lei 11.442/2007, especialmente seu art. 13-A, veda o uso de "informações de bancos de dados de proteção ao crédito como mecanismo de vedação de contrato com o TAC e a ETC regulares para o exercício da atividade do Transporte Rodoviário de Cargas".

Note-se que, ao menos inicialmente, a LGPD não é considerada para chegar à conclusão relativa à proibição de uso de dados diversos à finalidade prevista legalmente, que podem provocar e/ou acentuar a discriminação contra os empregados. Esta conclusão, entretanto, é fortalecida a partir do reconhecimento de que, para avaliar a licitude de determinado tratamento de dados pessoais, deve-se considerar a LGPD. Assim, o voto condutor do Ministro Relator Alberto Bresciani considerou essencialmente dois aspectos centrais: o respeito aos princípios e às bases legais autorizativas previstas na LGPD.

Para tanto, o fundamento adotado parte da premissa de que a LGPD consagrou "o direito fundamental autônomo à proteção de dados pessoais e o direito à autodeterminação informativa" - que veio posteriormente a ser reconhecido como um direito fundamental na Constituição. Como diretrizes da LGPD, são indicados expressamente alguns dos seus princípios: finalidade, adequação, necessidade e não discriminação.

Para aferir a adequação do tratamento ao princípio da finalidade, analisou-se a base legal prevista para o tratamento de dados, referente à hipótese do art. 13-A da Lei 11.442/2007. Por conseguinte, ao se identificar a finalidade originária, entendeu-se pela ilegalidade do uso e do "fazer utilizar" - desse banco de dados para "qualquer outro fim que não a proteção ao fornecimento de crédito, salvo autorização em Lei".

[35] Em razão do escopo e limite do trabalho, não serão objeto de avaliação neste momento os fundamentos relativos à indenização por danos morais considerados pela decisão.

Ou seja, a avaliação sobre o tratamento ser compatível considerou, neste caso, a determinação prevista na Lei. 11.442/2007 que autoriza o tratamento de dados, e sobretudo as balizas impostas pela LGPD. É possível extrair dos fundamentos utilizados na decisão que a análise casuística realizada permitiu considerar se a nova finalidade pretendida seria específica e legítima e compatível com a finalidade original da coleta[36].

O princípio da não discriminação também foi relevante na análise pois se buscou evitar "a quebra da isonomia e de discriminação". No ponto, há menção a outras normas aplicáveis ao caso, tratando-se a nível nacional do art. 1º da Lei 9.029/1995, e, a nível de posicionamento internacional, da Convenção 111 da Organização Internacional do Trabalho, vigente no Brasil desde 1966. Portanto, essa avaliação indica o esforço pela aplicação coerente das normas que primeiramente tutelam os direitos dos cidadãos, ainda que estejam em uma relação de emprego ou trabalho e enquanto titulares de dados. As diferentes leis, dessa forma, se complementam no necessário exercício de diálogo das fontes.[37]

Veja-se que este posicionamento decorreu também da *ratio* adotada pelo Supremo Tribunal Federal (STF) nos autos da ADPF n. 6.529/2021[38], citada longamente na decisão do TST, em que se reconheceu a exigência de comprovação da adequação aos princípios, como o da finalidade, para que os dados fossem tratados - no caso, desde que comprovados o interesse público e sendo vedada qualquer uso que fosse contrário a este fim, como para atender interesses pessoais ou privados.

Portanto, em um exercício de harmonização das fontes jurídicas, a proteção conferida aos titulares pela LGPD perpassa por avaliar a hipótese que autoriza o tratamento, prevista em dispositivos normativos que são anteriores à vigência da LGPD, além de se considerar a legitimidade do tratamento de acordo com a LGPD. Essa avaliação é importante para fortalecer a proteção aos indivíduos, evitando usos que provocam e acentuam discriminações (indevidas e ilegais), em especial quando dados sensíveis estiverem envolvidos, e proteja o direito à autodeterminação informativa dos indivíduos.

---

[36] A respeito, consulte: TAVARES, Giovanna Milanez. O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD. Rio de Janeiro: Processo, 2021.

[37] MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo à Erik Jaime. In: MARQUES, Cláudia Lima (Coord.). *Diálogo das fontes:* do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012.

[38] STF. ADI n. 6.529/DF, Relatora: CÁRMEN LÚCIA, Data de Julgamento: 11/10/2021, Tribunal Pleno, Data de Publicação: 22/10/2021.

Ainda não houve trânsito em julgado do acórdão, mas acredita-se que as premissas nele estipuladas são importantes para valoração dos princípios que regem a temática da proteção de dados pessoais, em uma sociedade que progressivamente lida com os desafios do alto fluxo e processamento de informações. Com estas premissas, será possível permitir maior segurança jurídica às atividades empresariais que realizam o tratamento de dados pessoais, principalmente em um setor tão essencial à economia como o setor de transportes.

Considerações Finais

O direito social ao transporte e o direito fundamental à proteção de dados, previstos na Constituição Federal, podem ser percebidos como a base para a garantia de proteção ao titular-usuário, sem desconsiderar o incentivo ao contínuo desenvolvimento econômico do país. Ambos os direitos foram promulgados pela Constituição Federal em um período inferior a dez anos e a LGPD, enquanto lei principiológica, inaugura um marco normativo com novas e necessárias premissas para que o tratamento de dados ocorra legalmente, exigindo-se o estrito cumprimento aos princípios e bases legais que o autorizam para proteção dos cidadãos.

O setor de transportes, enquanto atividade regulada através da atuação de diferentes agências, possui regras específicas sobre variados temas. A análise de algumas leis a nível federal permitiu identificar que disposições sobre dados pessoais podem ser encontradas de forma dispersa no ordenamento jurídico brasileiro. Estas normas se somam à LGPD para permitir o adequado tratamento de dados pessoais, e podem, por vezes, corresponder a obrigações específicas aos agentes de tratamento, como bases legais para dados sensíveis ou não.

Iniciativas como a elaboração de guias setoriais de boas práticas são relevantes e devem ser incentivadas, acompanhadas de treinamento e atualização periódicas, em especial considerando que a ANPD possui a tendência de atuar cada vez mais para a implementação e fiscalização do cumprimento da LGPD no Brasil.

O "Código de Boas Práticas do Setor de Transporte" elaborado pelo Sistema CNT é um bom exemplo de medida que se propõe a estabelecer balizas para uma futura autorregulação, por requerer dos próprios agentes a refletirem sobre seus processos atuais e práticas que podem ser aprimoradas. Medidas voltadas à autorregulamentação, aliada ao fortalecimento da ANPD,

merecem ser objeto de próximos estudos, que acompanhem as ações destes atores enquanto representantes do setor público e privado que tratam os dados pessoais.

No âmbito do Poder Judiciário, os fundamentos extraídos a partir da avaliação da legalidade do tratamento contida no acórdão do TST objeto de análise são um importante exemplo de como os princípios da finalidade e não discriminação podem e devem ser considerados para enfrentar discussões práticas, operacionalizando efetivamente a proteção dos titulares. Nesse sentido, também são incentivados novos estudos que analisem como essa e outras questões vêm sendo endereçadas pelo Judiciário brasileiro, a fim de garantir o fortalecimento da LGPD e a garantia aos direitos dos titulares previstos em leis e na Constituição Federal.

Portanto, verifica-se que, mesmo recente, já existem importantes iniciativas voltadas à consolidação da LGPD no setor de transportes, garantindo-se a inovação, desenvolvimento econômico e proteção dos dados pessoais no ordenamento jurídico por meio da harmonização entre diferentes fontes previstas em leis e regulamentos próprios. Este processo exige a contínua cooperação de diferentes agentes, e os representantes do setor de transportes podem atuar em colaboração para a criação de boas práticas e para o diálogo com a ANPD em prol do desenvolvimento de parâmetros adequados aos desafios enfrentados no tratamento de dados pessoais dos diversos modais.

Referências bibliográficas

ALBANO, João Fortini. *Vias de Transporte*. Porto Alegre: Bookman, 2016.

ANAC. *Autorização para viagens de menores desacompanhados dos pais em voos domésticos poderá ser feita em formato digital*. Versão atualizada em 30 de jul. 2021. Disponível em: https://www.gov.br/anac/pt-br/noticias/2021/autorizacao-para-viagens-de-menores-desacompanhados-dos-pais-em-voos-domesticos-podera-ser-feita-em-formato-digital. Acesso em: 18 de set. 2023.

ANPD. *Relatório de Impacto à Proteção de Dados Pessoais* (RIPD). Versão atualizada em 6 abr. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3>. Acesso em 19 set. 2023.

ARTICLE 29 WORKING PARTY - WP29. *Guidelines on consent under Regulation 2016/679*. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf>. Acesso em: 18 set. 2023.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: as funções e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BOWCUT, Steven. *Transportation Industry*. Disponível em: <https://cybersecurityguide.org/industries/transportation/>. Acesso em 21 mar. 2023.

BRASIL. ANTT. *Resolução n. 5846/2019*. Disponível em: <https://anttlegis.antt.gov.br/action/ActionDatalegis.php?acao=detalharAto&tipo=RES&numeroAto=00005846&seqAto=000&valorAno=2019&orgao=DG/ANTT/MI&codTipo=&desItem=&desItemFim=&cod_menu=5408&cod_modulo=161&pesquisa=true>. Acesso em: 17 set. 2023.

BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 16 jan. 2023.

BRASIL. *Decreto n. 7.373*, de 11 de dezembro de 2014, que institui o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (e-Social). Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Decreto/D8373.htm?utm_term%5B0%5D=s-Assinatura-Eletronica_Assinatura-Documentos&utm_term%5B1%5D=documentos%20digitais>. Acesso em: 14 jun. 2023.

BRASIL. *Decreto n. 8.033*, de 27 de junho de 2013, que regulamenta as disposições legais que regulam a exploração de portos organizados e de instalações portuárias. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8033.htm>. Acesso em: 14 jun. 2023.

BRASIL. *Decreto n. 8.071*, de 14 de agosto de 2013, que regulamenta as disposições legais que regulam a exploração de portos organizados e de instalações portuárias. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8071.htm. Acesso em: 14 jun. 2023.

BRASIL. *Decreto-Lei n. 5.452*, de 1º de maio de 1943, que aprova a Consolidação das Leis do Trabalho. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em: 14 jun. 2023.

BRASIL. *Emenda Constitucional n. 90*, de 15 de setembro de 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc90.htm>. Acesso em: 21 mar. 2023.

BRASIL. *Emenda Constitucional n. 115*, de 10 de fevereiro de 2022. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 21 mar. 2023.

BRASIL. *Lei n. 9.506*, de 23 de setembro de 1997, que institui o Código de Trânsito Brasileiro. Disponível em: <https://www.planalto.gov.br/ccivil_03/LEIS/L9503Compilado.htm>. Acesso em: 14 jun. 2023.

BRASIL. *Lei n. 11.442*, de 5 de janeiro de 2007, que dispõe sobre o transporte rodoviário de cargas por conta de terceiros e mediante remuneração. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/Lei/L11442.htm>. Acesso em: 14 jun. 2023.

BRASIL. *Lei n. 13.103*, de 2 de março de 2015, que dispõe sobre o exercício da profissão de motorista e disciplina a jornada de trabalho e o tempo de direção do motorista profissional. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13103.htm>. Acesso em: 14 jun. 2023.

BRASIL. *Lei n. 13.709*, de 14 de agosto de 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 16 jan. 2023.

BRASIL. *Lei n. 14.071*, de 13 de outubro de 2020, que modifica a composição do Conselho Nacional de Trânsito e amplia o prazo de validade das habilitações. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14071.htm>. Acesso em: 14 jun. 2023.

BRASIL. *Lei n. 13.812*, de 16 de março de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13812.htm#:~:text=LEI%20N%C2%BA%2013.812%2C%20DE%2016%20DE%20MAR%C3%87O%20DE%202019&text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,da%20Crian%C3%A7a%20e%20do%20Adolescente). Acesso em: 17 set. 2023.

BRASIL. *Lei n. 14.599*, de 19 de junho de 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14599.htm>. Acesso em: 19 set. 2023.

BRASIL. *Supremo Tribunal Federal*. ADI 4.615/CE. Ministro relator Roberto Barroso, Julgado em Sessão Virtual entre 13 a 19 de setembro de 2019. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15341579166&ext=.pdf>. Acesso em 16 mar. 2023.

BRASIL. *Supremo Tribunal Federal* ADI n. 6.529/DF, Relatora: CÁRMEN LÚCIA, Data de Julgamento: 11/10/2021, Tribunal Pleno, Data de Publicação: 22/10/2021.

BRASIL. *Tribunal Superior do Trabalho*. Processo E-RR-933-49.2012.5.10.0001. Acórdão publicado em 25/2/2022. Ministro relator Alberto Bresciani. Disponível em: <https://consultadocumento.tst.jus.br/consultaDocumento/acordao.do?anoProcInt=2014&numProcInt=246606&dtaPublicacaoStr=25/02/2022%2007:00:00&nia=7779648>. Acesso em: 12. jun. 2023.

CNT. *Guia de Boas Práticas de Proteção de Dados no Setor de Transporte*. Disponível em: <http://xn--guia%20de%20boas%20prticas%20de%20proteo%20de%20dados%20no%20setor%20de%20transporte-g0g4qwn5453vbfa/>. Acesso em: 16 jan. 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, v. 12, n. 2, p. 91-108, jul/dez. 2011.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

FRAZÃO, Ana. CARVALHO, Angelo Prata de. MILANEZ, Giovanna. Curso de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2022

IX JORNADA DE DIREITO CIVIL (2022). Comissão "Direito Digital e Novos Direitos". *Enunciado 689*. Disponível em: < https://www.cjf.jus.br/enunciados/enunciado/1828>. Acesso em: 5 jul. 2023.

MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo à Erik Jaime. In: MARQUES, Cláudia Lima (Coord.). Diálogo das fontes: do conflito à coordenação de normas do direito brasileiro. São Paulo: *Revista dos Tribunais*, 2012.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 16ª ed. São Paulo: Saraiva Educação, 2021.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de

aplicação em três níveis. *Caderno Especial LGPD*. São Paulo: Ed. RT, novembro. 2019, p. 35-56.

MENDES, Laura Schertel; DONEDA, Danilo. 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, 2018.

MENDES, Laura Schertel. MATTIUZZO, Marcela. FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *In:* DONEDA, Danilo (coord.); MENDES, Laura Schertel (coord.) SARLET, Ingo Wolfgang (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 421-446.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor* - Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista De Direitos E Garantias Fundamentais*, 19(3), 2018, p. 159–180. Disponível em: <https://doi.org/10.18759/rdgf.v19i3.1603>. Acesso em: 5.jul.2023.

MULHOLLAND, Caitlin Sampaio. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *Revista Jur. Puc. Rio*, 2021. Disponível em: <https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf.>. Acesso em: 5 jul. 2023.

NISSENBAUM, Helen. *Privacy in context*: Technology, policy, and the integrity of social life. Stanford University Press, 2020.

SILVA, José Afonso. *Curso de Direito Constitucional Positivo*. 43ª ed. São Paulo: Malheiros Editores, 2014.

TAVARES, Giovanna Milanez. *O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD*. Rio de Janeiro: Processo, 2021.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com* - Revista Eletrônica de Direito Civil, v. 9, p. 1-38, 2020

VASCONCELLOS, Eduardo Alcântara de. *Transporte e meio ambiente*: conceitos e informações para análise de impactos. São Paulo: Ed. Annablume, 2006.

REQUISITOS PARA O USO SECUNDÁRIO DE DADOS PESSOAIS PELO PODER PÚBLICO COM BASE NA LEI GERAL DE PROTEÇÃO DE DADOS E NO GUIA ORIENTATIVO DA ANPD

Rodrigo Toledo Costa de Almeida[1]

Resumo: O artigo tem como objetivo discutir os requisitos para o tratamento secundário de dados pessoais no âmbito do Poder Público, diante da ausência de regulação clara e específica na Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, a partir de uma pesquisa bibliográfica e documental, o artigo dá destaque ao Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público publicado pela Autoridade Nacional de Proteção de Dados (ANPD). Por fim, são tecidas breves considerações acerca da possibilidade do uso secundário de dados pessoais no âmbito do Poder Público nos casos de incompatibilidade entre a finalidade originária e secundária, a partir de critérios propostos pela doutrina nacional.

Palavras-chave: Proteção de dados pessoais; Uso-secundário; Poder Público; ANPD; LGPD.

Abstract: *The article aims to discuss the requirements for secondary personal data processing in the public sector, in light of the absence of clear and specific regulation in the Brazilian Data Protection Law (LGPD). Through literature and documentary research, the article highlights the Orientation Guide on Personal Data Processing by the Public Sector published by the Brazilian Data Protection Authority (ANPD). Finally, brief considerations are made about the possibility of secondary use of personal data in the public sector in cases of incompatibility between the original and new purpose, based on criteria proposed by national doctrine.*

Keywords**:** *Personal data protection; Secondary use of data; Public sector; ANPD; LGPD.*

[1] Bacharelando do 9° semestre de Direito na Universidade Federal da Bahia. Membro do Observatório de Estudos sobre LGPD da UNB. Membro do Grupo de Estudos em Direito & Tecnologia da Universidade Federal de Minas Gerais. Pesquisador Voluntário no Privacy Lab do Centro de Direito, Internet e Sociedade (CEDIS-IDP).

Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709 de 14 de agosto de 2018) tem como objetivo regular o tratamento de dados pessoais, por pessoa natural ou jurídica de direito público ou privado, para a proteção da liberdade, privacidade e o livre desenvolvimento da personalidade das pessoas (arts. 1° e 3°, LGPD).

Historicamente, o desenvolvimento das leis que versam sobre proteção de dados pessoais visava a limitação do poder estatal no processo de formação do Estado Social, principalmente após o impacto das Grandes Guerras (DONEDA, 2006). Naquele contexto, a coleta de dados constituiu uma forma de garantir a titularização de direitos, como por exemplo através da arrecadação tributária. Contudo, com a expansão das ideias de Estado de bem-estar social e o próprio desenvolvimento da democracia, o Estado passou a tratar mais dados com o objetivo de atingir finalidades sociais (WIMMER, 2021).

Ao longo dos anos, os governos passaram a acompanhar a evolução tecnológica, passando a adotar, cada vez mais, tecnologias digitais como forma de modernização do Estado (WIMMER, 2021). No Brasil, apesar de ter ocorrido a mesma tendência de uso exponencial de dados pessoais pelo Estado, só houve a criação do instituto de proteção de dados a partir de 2018, com a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD).

É nesse contexto de modernização do Estado que se apresentam os grandes desafios de interpretação e aplicação das normas referentes à proteção de dados ao setor público. Isso decorre, principalmente, pelo desafio de se equilibrar a garantia do direito fundamental à proteção de dados e outros interesses decorrentes de princípios constitucionais aplicáveis à Administração Pública, como o da publicidade e da eficiência (art. 37, CF).

Recentemente, este equilíbrio foi colocado em xeque diante do surgimento da COVID-19 e da necessidade de controle e adoção de medidas pelo governo para minimizar e combater a pandemia. Isso porque, buscando estratégias para responder à pandemia, houve a necessidade de compartilhamento de dados pessoais, o que acentuou o debate acerca do uso secundário de dados pessoais com finalidades distintas da coleta original.

Em território brasileiro, é possível citar o Sistema de Monitoramento Inteligente utilizado pelo Governo de São Paulo, em parceria com empresas de telefonia móvel, para fins de mapeamento de calor, por meio de geolocalização (ZANATTA, et al, 2020). Percebe-se que o compartilhamento de dados para fins de pesquisa estatística e controle de distanciamento

social tornou mais evidente os debates acerca do compartilhamento de dados pelo Poder público e o uso secundário de dados, nos casos de finalidades distintas da original.

Foi nesse contexto que a Autoridade Nacional de Proteção de Dados (ANPD) publicou o *Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público* (Guia), em 28 de janeiro de 2022. O documento, que tem por objetivo fomentar a cultura da proteção de dados e orientar a Administração Pública na adequação à LGPD, traz diretrizes, exemplos, para tratamento adequado de dados pessoais e boas práticas ao setor público (BRASIL, 2022). Um dos pontos trazidos pelo Guia diz respeito ao compartilhamento de dados pessoais pelo Poder Público e ao seu uso secundário.

Diante da complexidade do tema, o presente artigo visa compreender a extensão dos requisitos apontados pela ANPD quanto ao uso secundário de dados pessoais, bem como as consequências da regulamentação dada pelo Guia para fins de segurança jurídica. Além disso, pretende-se verificar a presença ou omissão de informações acerca da incompatibilidade entre a finalidade do tratamento original e a secundária.

Para tanto, adotou-se a metodologia de revisão bibliográfica, com análise legislativa e regulamentar sobre o tratamento de dados pessoais pelo Poder Público, com destaque ao Guia Orientativo da ANPD sobre Tratamento de Dados Pessoais pelo Poder Público.

A primeira seção explorará os contornos do princípio da finalidade e do Tratamento de Dados pelo Poder Público. Na sequência, será abordado o compartilhamento de dados a partir dos critérios estabelecidos pela LGPD. Por fim, o artigo traz os requisitos para o uso secundário de dados pessoais no âmbito do Poder Público, incluindo os estabelecidos no Guia da ANPD.

1. Princípio da Finalidade e o Tratamento de Dados Pessoais pelo Poder Público

O princípio da finalidade representa uma das bases de todo o sistema de proteção de dados pessoais, permitindo que o titular de dados saiba, previamente, os limites legais do tratamento dos seus dados. Nesse sentido, o art. 6º, inciso I, da LGPD, o conceitua como dever de realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.

Assim, a finalidade deve ser (i) legítima, isto é, seguir aquilo previsto na lei, principalmente pautando o tratamento em observância das bases jurídicas do tratamento de

dados; (ii) específica, delimitando os objetivos de forma precisa, clara e compreensível; (iii) explícita e informada, devendo permitir e garantir que o titular de dados tenha o entendimento inequívoco do tratamento, especialmente nas situações em que o consentimento for necessário (BONNA *et al*, 2022).

Na visão do professor Doneda (2015), o princípio da finalidade é o que mais representa as características da matéria de proteção de dados, uma vez que permite que o uso dos dados esteja intimamente ligado ao motivo que fundamenta sua coleta, criando-se uma espécie de elo entre a informação e a origem. Por outro lado, é esse mesmo princípio que limita a possibilidade de utilização secundária de dados pessoais sem o conhecimento do titular.

Quando o tratamento de dados pessoais é realizado pelo Poder Público, deve-se observar uma finalidade pública. Entretanto, antes de tecer considerações sobre essa finalidade, impõe-se conceituar "Poder Público".

O art. 23 da LGPD, que cita expressamente o art. 1º da Lei de Acesso à Informação (Lei nº 12.527/2011), considera que a norma será aplicada aos órgãos ou entidades dos entes federativos e dos três Poderes, incluindo as Cortes de Contas e o Ministério Público. Além disso, o conceito de Poder Público abarca as empresas públicas e as sociedades de economia mista, quando não atuarem em regime de concorrência, ou quando atuarem na operacionalização e execução de políticas públicas (art. 24, LGPD); ainda, é aplicável aos serviços notariais e de registro exercidos em caráter público em delegação do Poder Público (art. 23, §4º, LGPD).

Em relação à finalidade pública, o art. 23, *caput*, da LGPD determina que o tratamento de dados pessoais pelo Poder Público "*deverá ser realizado para 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.*" Determina, ainda, que o tratamento de dados pessoais pelo Poder Público deve ter como objetivos (i) o *de executar competências legais,* referindo-se à atuação legítima dos agentes públicos no exercício de suas atividades, sejam elas na esfera legislativa, administrativa ou jurisdicional, na observância e na medida em que a lei permite; ou (ii) para o *cumprimento das atribuições legais do serviço público*.

Apesar da dificuldade jurídica em conceituar serviço público, Di Pietro (2020, p. 292) o compreende como:

> [...] toda atividade material que a lei atribui ao Estado para que a exerça diretamente ou por meio de seus delegados, com o objetivo de satisfazer concretamente às necessidades coletivas, sob regime jurídico total ou parcialmente público.

Assim, observa-se que o princípio da finalidade ganha novos contornos quando no contexto do Poder Público. Isso porque, enquanto a finalidade prevista no art. 6º, I, da LGPD, refere-se a um princípio geral interpretativo, a finalidade pública prevista no art. 23, *caput*, da LGPD representa uma condição para o tratamento de dados pelo Poder Público (ALVES; VALADÃO, 2022).

2. Compartilhamento de Dados pelo Poder Público

Em relação ao compartilhamento de dados pessoais, a LGPD em art. 5º, XVI, conceitua o uso compartilhado como:

> […] 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.

Já, no Guia Orientativo apresentado pela ANPD, o uso compartilhado de dados pessoais é definido como "a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública" (ANPD, 2022).

O compartilhamento de dados pela administração pública é regulado especialmente no art. 25 da LGPD, que estabelece o dever de manutenção dos dados pessoais em formato estruturado e interoperável, para garantir a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e ao acesso das informações pelo público em geral (BRASIL, 2018). Essa imposição legal permite que os dados possuam utilidade, favorecendo o uso compartilhado de dados pela administração (CARDOSO, 2020).

Ademais, o art. 26 da LGPD dispõe acerca da possibilidade de uso compartilhado de dados pessoais pelo Poder Público, desde que atenda às finalidades específicas de execução de

políticas públicas ou advenha de atribuição legal do órgão ou entidade pública. Ressalta-se que o compartilhamento de dados pessoais não pode ser realizado indiscriminadamente, devendo ser respeitados os princípios previstos no art. 6º da LGPD (BRASIL, 2018).

Buscando trazer mais claridade e orientar os agentes de tratamento, a ANPD, em seu Guia, ilustra algumas hipóteses de compartilhamento de dados pessoais para fins de execução de política pública, como a coleta de dados de doenças infecciosas pela Secretaria de Saúde de um município, e posterior compartilhamento desses dados com órgãos de pesquisa para realização de estudos voltados para área de saúde pública (BRASIL, 2022).

A administração compartilha dados também quando executa suas atividades típicas e rotineiras, como exemplo do pagamento de servidores. Além disso, durante a pandemia foi utilizado o compartilhamento de dados para fins de *contact tracing*, isto é, rastreamento e identificação de pessoas infectadas a fim de evitar o contágio de doenças e o consequente isolamento parcial ou total de pessoas (ZANATTA *et al*, 2020)

Além disso, o Guia fixa, a título de orientação, os principais requisitos para o compartilhamento de dados pelo Poder Público, que devem ser observados durante a operação:

a) **Formalização e registro**: deve-se formalizar atividades de compartilhamento de dados pelo Poder Público, mediante a adoção de algumas medidas, como: (i) instauração de processo administrativo; (ii) celebração de ato formal (contratos, convênios ou instrumentos congêneres firmados entre as partes); (iii) expedição de decisão administrativa pela autoridade competente; e (iv) no caso de compartilhamentos frequentes de dados pessoais, a ANPD sugere a edição de ato normativo interno disciplinando os procedimentos de compartilhamento;
b) **Atenção ao objeto e finalidade da atividade de tratamento**: os dados devem ser indicados de forma objetiva e detalhada, observando estritamente o necessário para alcançar as finalidades do tratamento;
c) **Atribuição de base legal**: as atividades de compartilhamento devem estar em conformidade com alguma das bases legais do art. 7º ou 11 da LGPD, conforme o caso;
d) **Duração do tratamento**: é necessário que o instrumento que formaliza o compartilhamento indique a duração da operação e o ciclo de vida dos dados;
e) **Transparência e direitos dos titulares**: as operações de compartilhamento devem atender ao princípio da transparência, possibilitando aos titulares o acesso a

informações claras, precisas e facilmente acessíveis sobre a operação e sobre como exercer seus direitos;

f) **Prevenção e segurança**: é necessário que sejam asseguradas medidas de segurança, técnicas e administrativas aptas a protegerem os dados pessoais, nos termos dos arts. 6º, VII, e 46, da LGPD.

g) **Outros requisitos:** também devem ser levados em consideração outros requisitos a partir das circunstâncias do caso concreto, como por exemplo: (i) hipótese de novo compartilhamento ou transferência posterior dos dados pessoais; (ii) definição do ônus financeiro da operação; (iii) regras específicas relativas ao compartilhamento de dados entre entes públicos e entidades privadas; (iv) análise da necessidade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD); (v) identificação das funções e responsabilidades dos agentes de tratamento.

Deve-se destacar que todo processo de compartilhamento de dados deve ser precedido de uma ponderação ou avaliação sobre os riscos que essa operação pode ocasionar para os direitos fundamentais de liberdade, de privacidade, o livre desenvolvimento da personalidade da pessoa natural e a proteção de dados. Isso porque, o compartilhamento de dados pessoais, de modo geral, está relacionado a uma finalidade diversa da coleta original. Somado a isso, aumentam-se os riscos de incidentes de segurança em maior escala, o que permite o seu uso de forma inadequada e ilegítima (SCHERTEL; GASIOLA, 2022).

Diante das particularidades e do cenário da modernização estatal, resta evidente a necessidade de se aderir às diretrizes da ANPD e da LGPD acerca dos requisitos legitimadores que balizam o uso secundário de dados pelo Poder Público

3. Tratamento secundário de dados pessoais

Como já observado, o tratamento de dados pessoais está diretamente ligado a uma finalidade específica. Nesse sentido, fala-se em **finalidade originária** do tratamento quando os dados são tratados dentro da finalidade que justificou sua coleta.

Ocorre que o Poder Público se vê diante de um dilema diário: como conciliar a eficiência na promoção do interesse público e do bem comum com o respeito ao direito fundamental à

proteção de dados nos casos em que é necessário o tratamento e compartilhamento de dados pessoais para além dos limites estabelecidos pela finalidade primária do tratamento?

Nesse contexto, o uso secundário de dados pessoais - para uso diverso das finalidades que justificaram originalmente a sua coleta - deve ser feito mediante observação de condições e requisitos que legitimem o novo tratamento, a fim de assegurar os parâmetros protetivos constitucionais e os garantidos pela LGPD (BRASIL, 2018).

A LGPD não regula especificamente o tratamento secundário de dados pessoais, o que poderia contribuir para um cenário de insegurança jurídica (WIMMER, 2021). Entretanto, é possível observar alguns dispositivos na lei que permitem concluir pela possibilidade de uso secundário de dados pessoais (ALVES; VALADÃO, 2022).

O primeiro deles é o art. 6º, I, da LGPD, que, ao dispor sobre o princípio da finalidade, obsta o tratamento posterior de forma incompatível com a finalidade originária. A segunda possibilidade decorre do uso de dados cujo acesso seja público (art. 7º, §3º, LGPD) ou aqueles tornados manifestamente públicos pelo titular de dados (art. 7º, §4º, LGPD), mediante a observância dos "*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*" (art. 7°, §7º, LGPD).

Além disso, nos casos em que a base legal para o tratamento de dados for o consentimento e para que haja a mudança de finalidade e o uso secundário de dados, o controlador "*deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações*", conforme se extrai do art. 9º, § 2º, da LGPD (BRASIL, 2018).

A ANPD, a partir de seu Guia, reconheceu expressamente a possibilidade de tratamento secundário de dados e editou alguns requisitos para esse tipo de operação, como se verá adiante.

3.1. Requisitos para o uso secundário de dados pessoais conforme o Guia Orientativo da ANPD

A ANPD preocupou-se em fixar alguns parâmetros para o tratamento posterior de dados pessoas pelo Poder Público, recomendando a avaliação da compatibilidade entre a finalidade original e a do uso secundário, e observando os seguintes requisitos:

(i) **o contexto e as circunstâncias relevantes do caso concreto**, verificando a existência de conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior. Nesse sentido o Poder Público deve levar em consideração o contexto do tratamento de dados a partir das nuances de cada atividade, ou seja, se as características do tratamento posterior estiverem de acordo com o contexto e a finalidade originária. Ainda, a finalidade secundária deve ser específica, a fim de evitar compartilhamento de dados irrestritos e amplos, cumprindo assim com o princípio da finalidade (ALVES; VALADÃO, 2022).

(ii) **a natureza dos dados pessoais**, adotando-se posição de maior cautela quando envolver dados sensíveis. Nesse ponto é importante que seja avaliado se o processamento posterior envolve dados sensíveis.;

(iii) **as expectativas legítimas dos titulares de dados e os possíveis impactos do tratamento posterior sobre seus direitos.** Deve-se avaliar, aqui, a legítima expectativa dos titulares, isto é, considerar quais são suas intenções a partir de uma dimensão objetiva de padrão social de comportamento. Nesse sentido, deve-se entender qual seria o comportamento do titular de dados quando confrontado com o fluxo de suas informações pessoais (BIONI, 2019).

(iv) **o interesse público e a finalidade pública específica do tratamento posterior**, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos, nos termos do art. 23 da LGPD. O inciso *v*, estabelece que o tratamento posterior deve ser realizado para o atingimento de uma finalidade pública, nos termos do art. 23, *caput*, da LGPD. Ressalta-se também a necessidade de motivação do ato administrativo que decide sobre o compartilhamento e uso secundário de dados, para garantir não só a legitimação do ato, como também permitir a avaliação possível de sindicância administrativa ou judicial (ALVES; VALADÃO, 2022).

Nota-se, portanto, que os requisitos apresentados pela ANPD representam um verdadeiro norte para que os entes públicos possam garantir a efetiva proteção aos direitos do titular de dados quando do uso secundário de dados pessoais.

Contudo, em que pese o grande avanço proporcionado pelo Guia orientativo da ANPD, a Autoridade não se manifestou acerca do tratamento secundário de dados nos casos em que haja incompatibilidade com a finalidade original que justificou a coleta.

Sobre esse tema, defende a professora Wimmer (2021, p. 137) que é possível solucionar a incompatibilidade das finalidades do tratamento originário e secundário mediante "consentimento do titular ou com base em previsão legal específica, necessária e proporcional, observando-se o pleno respeito aos demais princípios e direitos associados à proteção de dados pessoais".

Cabe destacar, entretanto, que o uso do consentimento pelo Poder Público, segundo o Guia orientativo da ANPD (BRASIL, 2022), só pode ser admitido nos casos em que a utilização dos dados pessoais não ocorra de forma compulsória, bem como a atuação estatal não seja baseada no exercício de prerrogativas típicas, ou seja, derivadas do cumprimento de atribuições ou de deveres legais.

Assim, observa-se a possibilidade de compartilhamento e o uso secundário de dados pessoais pelo Poder Público, desde que sejam estabelecidas salvaguardas para o cumprimento dos direitos dos titulares de dados estabelecidos na LGPD e na Constituição Federal (Wimmer, 2021).

Considerações Finais

Ao longo deste artigo, pode-se perceber que o princípio da finalidade deve ser interpretado de forma qualificada, aderindo à ideia de finalidade pública e funcionando como balizador para o uso secundário de dados pessoais.

É certo que os critérios estabelecidos na LGPD somados às diretrizes na ANPD no Guia expressamente permitiram o uso secundário de dados, desde que compatíveis com as finalidades que justificaram a coleta original. Ressalta-se, ainda, que devem ser observados os princípios dispostos na LGPD, analisando o contexto do tratamento dos dados pessoais, a natureza dos dados coletados e os possíveis impactos do tratamento posterior aos direitos e liberdades do titular. Ademais, o compartilhamento e uso secundário de dados só poderá ser realizado para atingir o interesse público e uma finalidade pública do ente.

Por outro lado, é possível observar que o Guia orientativo não tratou acerca do uso secundário de dados pessoais quando as finalidades são incompatíveis com a original. Nesses

casos, deve-se procurar um novo consentimento ou uma outra base legal específica que fundamente o novo tratamento, desde que garantidas as salvaguardas e os direitos dos titulares.

Pensando na evolução da digitalização e do ecossistema de proteção de dados no país, a LGPD representa um marco para regulação de operações com dados pessoais realizadas por órgãos e entidades públicos, tanto de compartilhamento como de uso secundário de dados. Somado a isso, a ANPD tem papel de extrema importância ao orientar os agentes de tratamento, especialmente ao apresentar parâmetros objetivos e limites para o uso secundário de dados pessoais, contribuindo, assim, para garantir um cenário de segurança jurídica às operações realizadas pelo Poder Público.

Referências bibliográficas

ALVES, Fabricio; VALADÃO, Rodrigo. *Regime Jurídico do Tratamento secundário de dados pessoais pelo Poder Público*. IN. LIMA, Ana Paula Canto de; ALVES, Fabrício da Mota (Coord.) Comentários aos regulamentos e orientações da ANPD: a atuação administrativa da Autoridade Nacional de Proteção de Dados, 2022, p. 148.

BANDEIRA DE MELLO, Celso Antonio. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 62

BRASIL, Autoridade Nacional de Proteção de Dados. *Guia Orientativo sobre Tratamento de dados pessoais pelo Poder Público.* Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 16/01/2023.

BRASIL. Lei nº 13.709/2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25/01/2023.

BRASIL. Lei nº 12.527/2011. Lei de Acesso à Informação (LAI). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.Acesso em: 29/01/2023.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento.* Rio de Janeiro: Forense, 2019. p. 316 e 317.

BIONI, Bruno; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o seu Portal de Entrada? In: BIONI, B. (org.). Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021 p. 281-313.

CARDOSO, André Guskow. O regime e uso compartilhado de dados pessoais pela Administração Pública no âmbito da LGPD. Informativo Justen, Pereira, Oliveira e Talamini. Curitiba, nº 163, setembro de 2020. Disponível em: http://www.justen.com.br. Acesso em 20.03.2023.

CASADO, Eduardo Gamero. Interoperabilidad y administración electrónica: conéctense, por favor. Revista de Administración Pública. Madri, n. 179, p. 291-332, mai/ago. 2009.

Comentários à lei geral de proteção de dados pessoais [recurso eletrônico] / Alexandre Pereira Bonna...[et al.] ; coordenado por Guilherme Magalhães Martins, João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. - Indaiatuba, SP: Editora Foco, p.133, 2022.

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo* – 33. ed. – Rio de Janeiro: Forense, p. 292, 2020

DONEDA, Danilo. *Princípios de Proteção de Dados Pessoais*. In: LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). Direito & Internet III: Marco civil de internet. Quartier Latin, 2015. t. I. p. 378.

DONEDA, Danilo. Da Privacidade à Proteção de Dados. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, G. M.; LONGHI, J. V. R. (Org.). Direito digital: direito privado e internet. 2. ed. Indaiatuba: Foco, 2019. p. 35-54.

FALEIROS JÚNIOR, José Luiz de Moura. Administração pública digital: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. Indaiatuba: Foco, 2020.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A Administração Pública entre transparência e proteção de dados. In: Revista de Direito do Consumidor. vol. 135. ano 30. p. 179-201. São Paulo: RT, maio/jun. 2021.

GOMES, Maria Cecília O. Relatório de impacto à proteção de dados: Uma breve análise da sua definição e papel na LGPD. In: Revista do Advogado. v. 39, n. 144, p. 174–183, nov., 2019.

GONÇALVES, Tânia Carolina Nunes Machado. Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal: desafios, modelos e principais impactos com a nova Lei. Orientador Prof. Dr. Marcelo Dias Varella. – Brasília, 2019. Dissertação (Mestrado em Direito) – Centro Universitário de Brasília (UniCEUB), 2019.

LGPD: *Lei Geral de Proteção de Dados comentada* [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. E ampl. – São Paulo: Thomson Reuters Brasil, 2020, p.305.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip; ROTEMBERG, Marc (Org). Technology and privacy: the new landscape. Cambridge: MIT Press, 1997. p. 219-242.

MURARI, Georgia Anastácia Campana; SCHIAVON, Isabela Nabas; BARRETOS, Ronaldo de Almeida. Dados pessoais: tratamento realizado pelo Poder Público à luz da Lei Geral de Proteção de Dados. In: Revista Judiciária do Paraná. n. 22, Curitiba: BoniJuris, nov. 2021, p. 245-256.

SANTANNA, Gustavo da Silva. A necessária relação entre interoperabilidade e compartilhamento de dados, transparência administrativa e privacidade: uma análise do comportamento da Administração Pública a partir da LGPD. In: CRAVO, D. C.; CUNDA, D. Z. G.; RAMOS, R. (orgs.). Lei Geral de Proteção de Dados e o Poder Público. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021, p. 85-102.

SCHERTEL, Laura e GASIOLA, Gustavo. *Inconstitucionalidade do Decreto 10.046: limites do compartilhamento de dados.* Disponível em: conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico#_ftnref7. Acesso em: 22/01/2023.

WIMMER, Mirian. Proteção de dados pessoais no Poder Público: incidência,

bases legais e especificidades. In: Revista do Advogado. v. 39, n. 144, nov., 2019, p. 126-133.

WIMMER, Miriam. *Limites e possibilidades para o uso secundário de dados pessoais no Poder Público: lições da pandemia*. Revista Brasileira de Políticas Públicas, Brasília, v. 11, n. 1. p.122-142, 2021.

WIMMER, Miriam. *O regime jurídico do tratamento de dados pessoais pelo Poder Público.* Tratado de proteção de dados pessoais. coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021, p.424

ZANATTA, R. A.; BIONI, B.; KELLER, C. I.; FAVARO, I. Os Dados e o Vírus: Tensões jurídicas em torno da adoção de tecnologias de combate à Covid-19. Revista Brasileira de Direitos Fundamentais & Justiça, [S. l.], v. 14, n. 1, p. 231–256, 2020.

USO DE DADOS COMO UM CATALISADOR ECONÔMICO: UMA BREVE ANÁLISE DA INTERSEÇÃO ENTRE A PROTEÇÃO DE DADOS E O DIREITO DA CONCORRÊNCIA

Igor Marques Caldas Machado[1]

Resumo: Trata-se de um breve estudo acerca da atuação das autoridades de Defesa da Concorrência do Brasil e da União Europeia, considerando o estado atual do tratamento de dados pessoais como um recurso fundamental para o desenvolvimento dos mercados tradicionais e, em especial, os mercados digitais. O artigo traz considerações acerca das noções gerais da natureza e do tratamento dos dados, passando a uma posterior análise sobre como os dados podem ser empregados para maximizar os resultados comerciais de empresas que atuam digitalmente e de que forma as autoridades antitruste brasileira e europeia têm se posicionado quanto a esta utilização.

Palavras-chave: dados; mercados digitais; concorrência; LGPD

Abstract: *This is a brief study on the performance of the Brazilian and European Union Competition Defense authorities, considering the current state of data use as a fundamental resource for the development of traditional markets and, specially, digital markets. The paper explores the general aspects of the nature and processing of data, moving on to a further analysis of how data can be used to maximize the commercial results of companies that operate digitally and what were the results of recent cases judged by the antitrust authorities of Brazil and the European Union.*

Keyworsds**:** *data; digital markets; competition; LGP*

[1] Igor Marques Caldas Machado é integrante do Ferro, Castro Neves, Daltro e Gomide Advogados. Graduando em Direito da UnB, editor de artigos da Revista dos Estudantes de Direito da UnB, membro do Observatório da LGPD, pesquisador bolsista pela FAP-DF e pesquisador voluntário pelo CNPq.

Introdução

Os dados representam um ativo de altíssimo valor. A obtenção, conservação e utilização dessas informações são formas de exercer o poder econômico, político e social. (FRAZÃO, 2022)

Em uma sociedade em constante transformação, impulsionada pela adoção de novas tecnologias que têm o poder de aumentar a qualidade de produtos e que fomentam a inovação constante, o manuseio dos dados se mostra como uma importante ferramenta econômica. Assim, na atualidade, os dados se tornaram tão importantes para a economia que podem ser considerados como recursos de infraestrutura, uma vez observados seus usos funcionais para o impulsionamento dos mercados tradicionais - como educação, saúde e segurança - e criação de novos mercados - como os mercados digitais (OCDE, 2014).

O tratamento de dados, no contexto contemporâneo, tomou proporções cada vez maiores, (i) maximizando o volume de dados processados; (ii) a velocidade em que estes dados são coletados e usados; (iii) a variedade de informações agregadas; e (iv) o valor dos dados para a economia (GRUNES, 2016). Este conjunto de fatores é o que se conceitua, atualmente, como "*Big Data*", tendo também desencadeado a necessidade de se atentar ao uso de dados de forma cautelosa.

O *Big Data* é um ponto crucial para a discussão entre a Proteção de Dados e o Direito da Concorrência, vez que seus efeitos refletem diretamente sobre a forma pela qual os agentes econômicos conseguem impulsionar seus modelos de negócios a partir do gerenciamento de informações que conectam os consumidores diretamente aos vendedores de produtos e prestadores de serviços, por meio do direcionamento digital de seus interesses de consumo.

Por óbvio, quanto ao tratamento de dados, há no mínimo dois agentes: aqueles que fornecem seus dados e aqueles que os adquirem. Em economias digitais, contudo, é coerente inferir que os mercados não se resumem a apenas dois lados, considerando os possíveis múltiplos agentes pertencentes a esta cadeia (mercados de múltiplos lados), uma vez que as plataformas digitais, comumente, reúnem consumidores, anunciantes e fornecedores, seja de produtos ou serviços (FONSECA JÚNIOR, 2022).

Assim, em se tratando de serviços digitais, o fornecimento de dados é crucial para que sejam criados os chamados *profilings* (perfilamento), os quais, nos ditos de Laura Schertel, caracterizam-se como:

> "[U]m registro sobre uma pessoa que expressa uma completa e abrangente imagem sobre a sua personalidade. Assim, a construção de perfis compreende a reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter uma imagem detalhada e confiável, visando, geralmente, à previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências do consumidor." (SCHERTEL, 2014)

Com efeito, a perfilização proporciona uma experiência individualizada para cada consumidor e se torna cada vez mais assertivo na medida em que ocorre a retroalimentação entre o fornecimento de informações dos usuários e o gerenciamento dos dados pelas plataformas digitais.

Para além da retroalimentação individualizada, há de se considerar o chamado *feedback loop*, isto é, a retroalimentação generalizada decorrente do acúmulo dos dados de todos os usuários os quais utilizam determinada plataforma. O *feedback loop* é um dos resultados do tratamento de dados em larga escala e possibilita que as grandes plataformas possuam produtos cada vez mais completos, em vista à gestão dos interesses, métodos de retenção da atenção e designs mais atrativos aos usuários nos espaços virtuais. (OCDE, 2016)

Sendo assim, o Direito da Concorrência e a Proteção de Dados, cada vez mais, compartilham preocupações sobre os limites e os cuidados que os agentes econômicos devem ter em mente ao coletar, armazenar e gerir os dados destes consumidores. Destaca-se, nesse sentido, o Acordo de Cooperação Técnica firmado entre o CADE e a ANPD, o qual visa, dentre um de seus objetivos, combater eventuais atividades lesivas à ordem econômica. Neste artigo, serão brevemente tratadas algumas preocupações, as quais serão divididas em três capítulos: (i) noções preliminares sobre uso de dados; (ii) economia digital e a função dos dados como um recurso de infraestrutura; e (iii) possíveis preocupações antitruste e atuação da autoridade de defesa da concorrência do Brasil.

1. Noções preliminares sobre o uso de dados

A Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018, conceituou os dados pessoais como informações relativas "a pessoa natural identificada ou identificável". Por seu caráter expansionista, a LGPD dispõe da natureza da "informação" nas dimensões objetivas

e subjetivas do indivíduo, isto é, desde aspectos relacionados ao nome, idade e raça, até opiniões, preferências de consumo e interesses (FRAZÃO, 2022, p. 52).

Ainda, para tratar sobre as repercussões jurídicas do uso dos dados, é necessário aferir sua titularidade. Isso porque a titularidade permite que sejam exercidos conjuntos de direitos atrelados a um determinado bem jurídico, tais como o controle e a disposição dos dados pessoais (MAIA, 2020).

A já comentada LGPD traz como titular dos dados, por meio de seu art. 5, inciso V, a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". Em outras palavras, são direitos do titular (i) exercer o controle sobre quais informações poderão ser armazenadas; (ii) e ter a seu dispor o conjunto de informações que foram coletadas, com fulcro na transparência que os agentes que coletam os dados devem ter com estes indivíduos, conforme expresso por meio do art. 6º, inciso IV da LGPD, o qual define que os agentes de tratamento de dados devem observar a "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".

Alinhado ao princípio da transparência, encontra-se o da finalidade. O Princípio de Finalidade é externado no art. 6º, inciso I, da LGPD. Por meio deste, institui-se a necessidade de que os agentes de tratamento observem a "*realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*". Assim, o tratamento de dados deve o observar as informações e finalidades comunicadas previamente ao titular, sendo possível a alteração da finalidade originária apenas excepcionalmente.

Este conjunto de princípios e normas expostas na LGPD são ferramentas norteadoras para os agentes econômicos e as pessoas naturais acerca de seus respectivos direitos, bem como limitam a atuação irrestrita dos agentes de tratamento de dados em desacordo com as normas de Proteção de Dados, permitindo a solidificação de um ambiente virtual seguro para os usuários e concorrencialmente harmônico para os atores econômicos.

2. Economia digital e a função dos dados como um recurso de infraestrutura

Os recursos de infraestrutura são empregados para múltiplos fins e podem ser utilizados para o desenvolvimento de bens e serviços, bem como para fins de ordem privada, pública ou social. (FRISCHMANN, 2012).

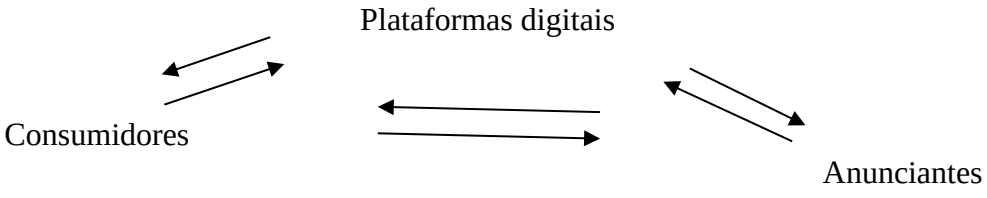
Sob esta perspectiva, os dados podem ser vislumbrados como recursos. A utilização da informação para fins de desenvolvimento econômico, cada vez mais, representa um grande diferencial mercadológico para os agentes que investem na racionalização e processamento de dados. Isso porque, conforme mencionado acima, o tratamento destes recursos direciona ao usuário final os bens e serviços que estejam alinhados com suas próprias preferências de consumo, em conformidade com o perfilamento realizado pelos agentes econômicos. Não por acaso, anúncios direcionados e marketing digital são usados cada vez mais por diversos atores privados e públicos via tráfego pago.

Assim, exponencialmente, as empresas têm adotado o uso dos dados pessoais como a chave diferencial de seus respectivos modelos de negócios (GRUNES, STUCK, 2016), além de outras formas de aumento de eficiência, inovação de processos e integração de produtos e serviços em suas respectivas cadeias de valor em virtude da coleta e processamento de um grande número de dados. (OCDE, 2017)

Com a capacidade de evoluir os serviços tradicionais, como educação e saúde, os serviços digitais se apropriam cada vez mais destes recursos para fomentar seus próprios negócios, potencialmente ampliando suas participações de mercado e criando serviços inovadores a partir de demandas emergentes dos consumidores.

O tratamento de dados guarda íntima conexão com as relações de consumo, considerando que tais informações são capazes de aumentar a rentabilidade dos serviços e produtos que estão sendo oferecidos aos usuários. Neste vínculo, há a necessidade do constante suprimento de informações por parte do utilizador e, assim, o consumidor deixa de ser visto como apenas um agente passivo (aquele que apenas consome o que lhe é oferecido), mas se torna um agente ativo, pois seus interesses direcionam a distribuição do bem de consumo (BIONI, 2021).

Os modelos de negócio atuais que utilizam do Big Data como um ponto focal para o alcance direto aos consumidores, no geral, podem ser esquematizados da seguinte maneira:



Ou seja, a relação entre os usuários e os agentes econômicos é normalmente tríplice**.** As **plataformas digitais** oferecem aos **consumidores** um conjunto de serviços que podem ser usados de maneira "gratuita", com a contrapartida ao fornecimento de dados pessoais como: nome, idade, país em que reside, preferências de consumo (decorrentes das pesquisas e cliques).

Ainda, as plataformas oferecem aos **anunciantes** espaços privilegiado – isto é, locais que sejam pontos focais da visualização do consumidor quando este utiliza a plataforma digital – para divulgação de anúncios em suas plataformas e o processamento dos dados dos consumidores, de modo a criar o perfil de cada consumidor. Destarte, os anunciantes, que possuem um conjunto de bens ou serviços para vender, compram espaços privilegiados e seus anúncios são direcionados aos consumidores que possuam o perfil de consumo alvo de seus negócios.

3. Possíveis preocupações antitruste e atuação das autoridades de defesa da concorrência em mercados digitais e proteção de dados dos usuários

A junção dos interesses dos usuários com anúncios personalizados a estes perfis tem o poder de potencializar as interações e as relações comerciais. Este fenômeno é o que fundamenta a publicidade direcionada de ordem comportamental (BIONI, 2021).

Cabe destacar que os usuários – em sua relação com os agentes econômicos que captam seus dados – estão resguardados tanto pelo Código de Defesa do Consumidor (CDC), o qual disciplina, por meio da Seção IV da Lei 8.078 de 1990, os parâmetros que devem ser seguidos pelos bancos de dados e cadastros dos consumidores em vistas a tutelar aos indivíduos o direito de possuir controle sobre quais de suas informações são armazenadas, de forma clara e transparente, quanto pela LGPD que, nos termos de seu art. 45, ressalta expressamente a aplicação do CDC nos casos em que a relação entre o agente e o titular for de consumo. É nesta seara que são vistos alguns litígios concorrenciais envolvendo o armazenamento e a forma de gestão de dados.

Para além da seara consumerista, antes de adentrar especificamente no que o Conselho Administrativo de Defesa Econômica (CADE) tem entendido sobre o tema, cabe traçar breves considerações sobre o olhar da política antitruste quanto aos agentes econômicos que realizam tratamento de dados pessoais na perspectiva da *Big Data*.

O relatório "Competition Policy for the Digital Era", elaborado pela Comissão Europeia, aduz que as principais preocupações, no tocante aos mercados digitais, devem ser referentes às "teorias do dano e identificação de estratégias anticompetitivas" (CRÉMER; MONTJOYE; SCHWEITZER), i.e., em um contexto em que os serviços digitais se transformam em velocidade disruptiva, as autoridades antitruste deveriam verificar qual a capacidade de um determinado agente econômico de afetar a concorrência de forma desleal ao ponto de ser necessária a intervenção estatal.

Ainda, os mercados digitais, por sua natureza diversa dos mercados tradicionais, carregam peculiaridades que dificultam a atuação antitruste, dentre os quais, destacam-se, para os fins deste artigo, (i) sua estrutura diferenciada do ambiente digital; (ii) a primazia dos dados como elementos essenciais; (iii) a concorrência baseada na economia comportamental (FONSECA JÚNIOR, 2022); (iv) os fortes efeitos de rede (BRASIL, 2020, p. 12).

Assim, analisando o item (iii) acima destacado, o CADE tem se debruçado sobre a questão do uso dos dados dos usuários em vistas a combater um possível abuso de posição dominante – qual seja, a utilização do poder de mercado para distorcer o processo competitivo (NETO, CASAGRANDE, 2016) – concernent à conduta de agentes econômicos que coletam grande volume de informações, em razão de sua dominância, para alavancar seus respectivos negócios.

Algumas das principais discussões em tela são relacionadas ao tratamento de uma grande quantidade de dados pelas plataformas para (i) aumentar ou manter poder de mercado; (ii) fechar o mercado aos concorrentes; e (iii) criar barreiras à entrada de novos *players* nos mercados digitais. (FERNANDES, 2022).

O CADE já analisou mercados digitais em recentes oportunidades, trazendo importantes considerações quanto ao funcionamento de algumas das faces dessa nova modalidade de mercado.

3.1. Fusões e aquisições em mercados digitais

Por serem marcados pelo dinamismo e pela inovação, os mercados digitais possuem características que, por vezes, os diferenciam dos mercados tradicionais, tais como os diversos empreendimentos embrionários ou *startups* que, apesar de muito novos, têm grande potencial econômico. Neste sentido, são comuns as fusões e aquisições de empresas que ainda não

alcançaram índices elevados de faturamento, mas que possuem alto potencial econômico pelo emprego de tecnologias e ideias disruptivas.

Para que seja obrigatória a submissão de um ato de concentração ao CADE, contudo, os faturamentos das empresas envolvidas na operação devem possuir patamares específicos (de um lado R$ 750 milhões e, de outro, R$ 75 milhões), que, eventualmente, não são alcançados, de modo que aquisições que têm o potencial de impactar o mercado digital não são equer analisadas pela autoridade brasileira. Este problema já está sendo endereçado, por exemplo, na União Europeia, porquanto a autoridade competente, *European Comission* (EC), estabeleceu mecanismos diferenciados que não vinculam a submissão dos atos de concentração ao faturamento das partes envolvidas, necessariamente.

É nesse contexto que foi analisada, recentemente, a aquisição de uma empresa que possuía grande quantidade de dados de consumidores relacionados à saúde e preferências *fitness* por uma *Big Tech.* Esta, por sua vez, também possui uma vasta quantidade de dados de seus usuários, de forma geral, estando presente em diversos segmentos digitais, como buscas online, anúncios, merchandising, organização pessoal e coorporativa, entre outros.

Na Europa, a EC demonstrou preocupação com as consequências da obtenção de uma extensa quantidade de dados de saúde pela Big Tech e como isso poderia ser utilizado para personalização de anúncios (massificando e melhorando a efetividade do perfilamento), aumentando as barreiras à entrada de novos players no mercado e, eventualmente, diminuindo a viabilidade de a concorrência alcançar a qualidade dos serviços da empresa adquirente, o que afetaria anunciantes e consumidores, diante da redução do espaço competitivo.

A aquisição, face a tais preocupações, só foi viabilizada mediante um conjunto de compromissos (remédios) firmados pela adquirente, de modo a garantir que a operação não teria o potencial de prejudicar o espaço concorrencial Europeu. Alguns dos compromissos foram: (i) a adquirente não utilizaria a base de dados da adquirida em seus serviços de anúncio; (ii) a adquirente manteria uma separação técnica entre sua base de dados e a base de dados da adquirida; e (iii) usuários da European Economic Area (‘EEA’) teriam a escolha de compartilhar seus dados coletados para os demais serviços da adquirente.

Além disso, a EC garantiu que o cumprimento dos compromissos firmado seria monitorado desde sua implementação até o efetivo resultado, demonstrando a preocupação em

manter os dados de seus usuários em segurança, nos moldes definidos pela General Data Protection Regulation (GDPR).

3.2. Abuso de posição dominante e arquitetura digital dos mercados

O CADE tem se mostrado atento às demandas emergentes da relação entre a proteção dos dados dos usuários e a defesa da concorrência. Em junho de 2019, o Tribunal do CADE apurou suposta conduta anticompetitiva praticada pelo Google referente às formas de visualização e arquitetura de ambientes digitais (design das páginas e dos sites). Da análise das informações prestadas na ocasião do julgamento, é possível inferir que os usuários tendem a priorizar sistemas operacionais, plataformas digitais ou sites que possuam uma interface de fácil visualização e que proporcionem uma navegação fluida.

Por conseguinte, agentes que detêm plataformas que conectam os consumidores e as empresas prestadoras de serviços ou produtos, dispõem dos anúncios em locais de visualização privilegiada, de modo a aumentar a atratividade dos produtos e o apelo dos serviços a serem comercializados. Assim, algumas das perguntas que vêm à mente diante deste contexto são: como o tratamento de dados é realizado nestas situações? E quais seriam as preocupações que o CADE deveria ter em relação a estes agentes econômicos digitais?

Conforme já discutido, quanto mais usuários, maior será o volume de dados tratados por uma determinada plataforma digital. As plataformas de buscas que possuírem as maiores bases de dados, por causa do efeito de *feedback loop*, serão as mais procuradas pelos consumidores e mais disputadas pelos anunciantes. Nesses casos, convém à autoridade tomar um especial cuidado, pois a grande quantidade de dados armazenados pode proporcionar ao agente (plataforma), em exercício de ação exclusionária ou discriminatória, o poder de gerenciar as barreiras à entrada de novos players no mercado, em face da produção de efeitos de rede (RUBINFELD, 2017) ou de permitir o abuso da posição dominante por *players* consolidados.

Neste sentido, se por um lado os agentes econômicos são livres para estabelecer quais são as condições para a exibição dos anúncios digitais, por outro, uma vez que ocupam posição dominante, há de se observar os critérios para seleção de tais anúncios em vistas a evitar possíveis discriminações entre as ofertas dos anunciantes e as provenientes de sites que aparecem de modo orgânico nas pesquisas.

Isso porque, a depender da forma de escolha de arquitetura de visualização, uma plataforma de busca poderá ser capaz de (i) aumentar os custos dos agentes, pois, normalmente, os anunciantes e demais sites são dependentes das plataformas de buscas para alcançar os consumidores; e (ii) afetar a atratividade dos elementos da página e influenciar a quantidade de acessos dos sites, ocasionando uma perda efetiva do número de possíveis consumidores e, consequentemente, lesando a viabilidade econômica de um determinado negócio (DEE/CADE, 2018).

É importante destacar que, apesar das ressalvas que a Autoridade de Defesa da Concorrência possui com os mercados digitais, sua atuação é visivelmente cautelosa, vez que nos recentes Processos Administrativos referentes à possíveis condutas ilícitas, entendeu-se que os comportamentos supramencionados não afetaram negativamente o ambiente concorrencial, mas apenas resultaram na inovação de suas arquiteturas digitaus e de seus designs de produto.

Deste modo, o CADE entendeu que essas mudanças representariam benefícios aos consumidores, decorrente de melhorias na experiência do uso das plataformas de busca, salientando, ainda, que em mercados digitais caracterizados por intensa inovação "*a intervenção da autoridade antitruste deve se dar com bastante cautela, sob pena de inibição do esforço inovador, que é característico desses mercados*" (SG/CADE, 2018).

Considerações finais

O avanço científico propiciou a evolução dos mercados tradicionais e a criação de novos negócios. Os mercados digitais seriam uma das várias expressões da exploração da computação. Assim, diante do uso de novas tecnologias, quase a totalidade dos agentes econômicos desenvolveram métodos para maximização do potencial econômico com o uso de dados para o gerenciamento dos seus empreendimentos.

Nesse sentido, os dados, por serem recursos de infraestrutura, foram percebidos como um fator crucial para o desenvolvimento das economias dos países, considerando o progresso disruptivo do conhecimento científico e o aumento da qualidade de produtos e serviços, inclusive em setores essenciais, como educação, saúde e segurança. Para além disso, a coleta de dados dos consumidores, por meio das redes, proporcionou a criação pelas empresas de softwares inovadores e capazes de realizar o perfilamento dos usuários, de maneira

individualizada, os quais permitiram, a seu turno, que os resultados comerciais entre as plataformas, anunciantes e consumidores fossem catalisados.

Com o passar dos anos, tais inovações, apesar de essenciais, despertaram o interesse das autoridades antitruste e de proteção de dados, pois o uso desregulado dos dados pessoais demonstrou ter o potencial de afetar tanto a concorrência, quanto os consumidores. Se os dados possuem valor inestimável, estes não podem estar sob monopólio de apenas um agente econômico, sendo necessário o estabelecimento de limites regulatórios que assegurem a sua utilização de forma a atender os interesses públicos, na forma do respectivo ordenamento jurídico vigente.

Na União Europeia, a EC requereu que fossem tomadas medidas para garantir a proteção dos dados de seus usuários, em consonância com a GDPR. No caso do Brasil, o CADE já teve a oportunidade de analisar, tanto em controle de condutas, quanto em controle de concentração, os mercados digitais, elaborando documentos de trabalho e pareceres que demonstram que a autoridade de defesa da concorrência brasileira está atenta às demandas emergentes do uso de dados, em vista à necessidade de resguardo dos usuários e proteção à integridade do cenário concorrencial, em harmonia com as normas dispostas na LGPD.

Para além disso, o CADE terá de enfrentar, em um futuro próximo, um crescente número de casos envolvendo os ecossistemas digitais, os quais demandarão um cuidado regulatório especial. Haja vista que, se por um lado o excesso de controle da autoridade poderia mitigar as inovações e o potencial econômico dos negócios, por outro, a ausência de controle poderia resultar em altas concentrações dos mercados, diminuindo a concorrência e proporcionando um aumento de monopólios.

Ante o conjunto de fatores aqui expostos, a cooperação entre a ANPD e o CADE será bem-vinda, pois terá o condão de "estabelecer a atuação coordenada em casos de infração à ordem econômica que envolvam dados pessoais", proporcionando maior previsibilidade e rigor técnico quando da análise de possíveis infrações à ordem econômica. Sabendo, portanto, que os mercados digitais são altamente dinâmicos, será necessária a constante vigília – por parte das autoridades, profissionais e pesquisadores – quanto ao uso, coleta e tratamento de dados.

Referências bibliográficas

FRAZÃO, Ana. Curso Geral de Proteção de dados pessoais: fundamentos da LGPD / Ana Frazão, Angelo Prata de Carvalho, Giovanna Milanez – 1. ed. – Rio de Janeiro: Forense, 2022.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – 2. ed. – [3. Reimpr.] – Rio de Janeiro: Forense, 2021.

OCDE. (2014). Data-driven Innovation for Growth and Well-Being: Interim Synthesis Report.

STUCKE, Maurice; GRUNES, Allen. Big data and competition policy.

CRÉMER, Jacques; MONTJOYE, Yves-Alexandre de; SCHWEITZER Heike. Report on "Competition policy for the digital era". Bruxelas: Comissão Europeia, 2019, p. 3 e 4. Disponível em: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

OCDE (2017), The Next Production Revolution: Implications for Governments and Business, OECD Publishing, Paris, https://doi.org/10.1787/9789264271036-en

FERNANDES, Victor de Oliveira. Direito da Concorrência das Plataformas Digitais: entre o abuso de poder econômico e inovação – São Paulo: Thomson Reuters Brasil, 2022.

OCDE. Big data: bringing competition policy to the digital era. Background Paper by the Secretariat, p. 10, abr. 2016.

BRASIL, Ministério da Justiça e Segurança Pública. Departamento de Estudos Econômicos do CADE. Processo Administrativo no 08012.010483/2011-94. Disponível em < https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEFhBt-n3BfPLlu9u7akQAh8mpB9yNfCKqMPoDc8VR9_E4rWsD9KKso3ZsZRcsAMkWKngKZ4epIfAT_OhMxFfZSQOtL-FUyktD2K_9tJLB0wouY3Dpl>

RUBINFELD, Daniel L.; GAL, Michal. Acess Barriers to Big Data. 59 Arizona Law Review 339, 2017.

FONSECA JÚNIOR, Marco Antonio. A política antitruste brasileira e sua capacidade de enfrentamento dos mercados digitais: uma proposta de regulação concorrencial das plataformas digitais. 2022. 297 f., il. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2022.

MAIA, Roberta Mauro Medina. A titularidade de dados pessoais prevista no art. 17 da LGPD: direito real ou pessoal? In: TEPEDINO, Gustavo; Frazão, Ana; OLIVA; Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2020.

FRISCHMANN, B. M. (2012), Infrastructure: The Social Value of Shared Resources, Oxford University Press.

NETO, C. M. da S.; CASAGRANDE, P. L. Direito concorrencial: doutrina, jurisprudência e legislação. São Paulo: Saraiva, 2016, p. 138.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. P. 111.

Superintendência-Geral recomenda arquivamento de investigação contra o

Google. Conselho Administrativo de Defesa Econômica, Brasília, 20.11.2018. Disponível em https://www.gov.br/cade/pt-br/assuntos/noticias/superintendencia-geral-recomenda-arquivamento-de-investigacao-contra-o-google

BRASIL. Ministério da Justiça e Segurança Pública. Cade. Documento de trabalho no 005/2020. Concorrência em mercados digitais: uma revisão dos relatórios especializados. Cade, 2020d. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de- conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2020/documento- de-trabalho-n05-2020-concorrencia-em-mercados-digitais-uma-revisao-dos-relatorios-especializados.pdf. Acesso em: 10 fev, 2021.

ANPD e CADE assinam Acordo de Cooperação Técnica. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica.

INTERSECÇÕES ENTRE A LGPD E O DIREITO DO CONSUMIDOR

Lívia Rodrigues Alves [1]

Luis Eduardo de Souza Leite Trancoso Daher [2]

Resumo: O presente artigo busca analisar a intersecção entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Direito do Consumidor no Brasil. O artigo analisa a atuação dos Programas de Proteção e Defesa do Consumidor (Procons), os modelos de consentimento previsto na LGPD e no Código de Defesa do Consumidor (CDC) e a competência concorrente entre a Autoridade Nacional de Proteção de Dados (ANPD) e Secretaria Nacional do Consumidor (Senacon), a fim de compreender a intersecção entre as duas áreas. A análise foi feita a partir de revisão bibliográfica.

Palavras-chave: LGPD; Direito do Consumidor; ANPD; Senacon.

Abstract: *This article aims to analyze the intersection between the Brazilian Data Protection Law (LGPD) and Consumer Law in Brazil. The article analyzes the performance of Consumer Protection and Defense Programs (Procons), the consent models provided for in the LGPD and the Consumer Protection Code (CDC) and the concurrent competence between the Brazilian Data Protection Authority (ANPD) and the National Consumer Office (Senacon), in order to understand the intersection between the two areas. This analysis was based on a bibliographical review.*

[1] Lívia Rodrigues Alves é Bacharel em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG), Pós-Graduada em Direito Processual e Pós-Graduanda em Segurança da Informação, Pesquisadora no Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS. IDP), Membro do Observatório da LGPD da Universidade de Brasília (UnB) e é analista em Segurança da Informação, atuando com Privacidade e Proteção de Dados e Governança em Segurança da Informação.

[2] Luis Eduardo de S. L. T. Daher é Bacharel em Direito pela Universidade Federal Fluminense (UFF), Pós-Graduando em Direito Digital pelo Instituto de Tecnologia e Sociedade e Universidade do Estado do Rio de Janeiro (ITS/UERJ), Pesquisador no Grupo de estudos sobre as Interações Humano-Algoritmo da Cátedra Oscar Sala, do Instituto de Estudos Avançados da Universidade de São Paulo (USP), Membro do Observatório da LGPD da Universidade de Brasília (UnB) e é advogado, atuando em temas relacionados a Direito Digital, Proteção de Dados, Propriedade Intelectual, Direito Empresarial e Contratual.

Keywords: *LGPD; Consumer Law; ANPD; Senacon.*

Introdução

A proteção dos direitos coletivos e difusos é um tema cada vez mais relevante no âmbito do Direito, especialmente no contexto brasileiro. Desde a Constituição Federal de 1988 (CF), a tutela coletiva tornou-se um dos pilares do Estado Democrático de Direito no país, com o reconhecimento dos direitos difusos, coletivos e individuais homogêneos. A partir daí, diversas normas e órgãos de fiscalização foram criados para garantir a efetividade dessa proteção, como o Código de Defesa do Consumidor (Lei nº 8.078/90 ou CDC) e os Procons.

Mais recentemente, devido ao avanço da tecnologia e à crescente utilização de sistemas que permitem o armazenamento e o compartilhamento de informações pessoais, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou LGPD) trouxe à tona a importância da garantia da privacidade e da proteção dos dados pessoais dos cidadãos brasileiros, exigindo ainda mais atenção e atuação dos órgãos fiscalizadores.

Nesse contexto, a primeira parte deste artigo tem como objetivo analisar a evolução histórica da tutela coletiva e da legitimação dos órgãos fiscalizadores do direito dos consumidores no Brasil, em especial os Procons, destacando a importância desse mecanismo para a proteção dos direitos coletivos e individuais e trazendo exemplos de demandas administrativas de tais órgãos, a fim de demonstrar a sua atuação.

Na segunda parte do artigo, trataremos do instituto do consentimento relacionado às duas legislações, tanto à LGPD quanto ao CDC, incluindo suas características e finalidades, adotando como ponto de partida o panorama geral entre as duas normas.

Na sequência, abordaremos a competência concorrente entre a Autoridade Nacional de Proteção de Dados (ANPD) e Secretaria Nacional do Consumidor (Senacon), apresentando reflexões sobre possíveis conflitos e a necessária coordenação dos dois órgãos para viabilizar a tutela dos interesses tutelados que se interseccionam.

Por fim, abordaremos casos mais recentes de trabalho conjunto entre tais órgãos, como (i) a Nota Técnica nº 4/2019, (ii) o Acordo de Cooperação Técnica firmado entre a ANPD e Senacon, (iii) a análise de adequação da política de privacidade do WhatsApp, que mobilizou a atuação conjunta da ANPD, da Senacon, do Conselho Administrativo de Defesa Econômica

(CADE) e do Ministério Público Federal (MPF), por meio da elaboração de uma nota técnica, e (iv) o guia "Como Proteger seus Dados Pessoais", uma cartilha explicativa e simplificada elaborada por iniciativa conjunta de ambos os órgãos.

1. A LGPD e a atuação dos Procons

A evolução histórica da tutela coletiva e da legitimação dos órgãos fiscalizadores tem sido objeto de intensos debates e reflexões no âmbito do Direito. No Brasil, a tutela coletiva tem suas raízes históricas na CF, que consagrou a proteção dos direitos coletivos e difusos como um dos pilares do Estado Democrático de Direito.

Ada Pellegrini Grinover entende que os interesses difusos são interesses comuns de pessoas vinculadas "a fatores conjunturais ou extremamente genéricos, a dados de fato frequentemente acidentais e mutáveis"[3]. Entendidos como direitos relativos ao meio ambiente, à saúde, culturais e à tutela dos consumidores.

A partir da sua previsão na CF, o sistema jurídico brasileiro reconheceu a existência de interesses difusos, coletivos e individuais homogêneos, dando origem a uma nova concepção de tutela dos direitos. Com a elaboração do CDC, houve a normatização dos interesses e direitos metaindividuais tripartidamente,[4] reafirmando os instrumentos processuais para a tutela coletiva e os legitimados concorrentes para a defesa desses direitos.

O CDC assegurou "a efetiva prevenção e reparação dos danos patrimoniais e morais, individuais, coletivos e difusos" (art. 6º, VI), "o acesso aos órgãos judiciários e administrativos com vistas à prevenção ou reparação de danos patrimoniais e morais, individuais, coletivos e difusos" (art. 6º, VII) e "a tutela individual e coletiva dos interesses e direitos dos consumidores" (art. 81, *caput*).

Visando a garantir a efetividade dessa proteção, órgãos fiscalizadores foram criados, como os Procons e o Ministério Público. Tais órgãos possuem a missão de promover a defesa dos direitos coletivos e difusos, por meio da fiscalização e aplicação de sanções em casos de violação.

---

[3] GRINOVER, Ada Pellegrini. *Novas tendências na tutela jurisdicional dos interesses difusos.* Revista da Faculdade de Direito. Universidade de São Paulo, 1984. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67016. Acesso em: 10 de fev. de 2023.GRINOVER, 1984. p. 284.

[4] São objeto de tutela metaindividual: direitos difusos, coletivos em sentido estrito e individuais homogêneos.

Os Procons, órgãos de proteção ao consumidor, estão presentes em todos os estados brasileiros e no Distrito Federal (DF) e têm como principal missão a defesa dos interesses dos consumidores, por meio da fiscalização e aplicação de multas, em casos de violação do CDC.

A atuação dos Procons, por meio da aplicação do CDC, foi aprimorada ao longo dos anos, em resposta às demandas e às mudanças do mercado de consumo. O Sistema Nacional de Defesa do Consumidor (SNDC), criado em 1995, articulou a atuação dos Procons, estaduais e municipais, Delegacias de Defesa do Consumidor, do Ministério Público, Organizações Civis de Defesa do Consumidor, Defensoria Pública e Juizados Especiais Cíveis, estes que atuam integradamente com a Senacon.

Desta forma, tanto a CF quanto o CDC efetivaram direitos coletivos e asseveraram delineamentos jurídicos para que a tutela dos direitos difusos, coletivos e individuais homogêneos pudesse ser eficaz.

Na mesma esteira, a LGPD, em conjunto com o CDC, visa a diminuir os impactos nas relações que envolvem o tratamento de dados pessoais.

A LGPD, promulgada em 2018, visa a proteger a privacidade e os dados pessoais dos cidadãos brasileiros em resposta às constantes mudanças na era digital e utilização dos dados pessoais como ativos.

Como bem pontuado por Laura Schertel, "a revolução da tecnologia da informação alterou radicalmente a realidade social, penetrando em todas as esferas da atividade humana e, por conseguinte, criando novas relações a serem reguladas pelo sistema jurídico."[5]

Para Bruno Bioni, "com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (*marketing*) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação"[6]. Assim, com o avanço da tecnologia e a crescente utilização de sistemas que permitem o armazenamento e o compartilhamento de informações, a LGPD se tornou um instrumento de extrema importância para a garantia do direito à privacidade e à proteção de dados pessoais.

Ademais, como bem explica Bruno Bioni, após os avanços da tecnologia e utilização relevante do uso de dados pessoais, o consumidor passa a ser um ativo na economia da

---

[5] MENDES, Laura Schertel. *Transparência e Privacidade: Violação e proteção da informação pessoal na sociedade de consumo*. Dissertação de Mestrado - Faculdade de Direito da Universidade de Brasília. Brasília 2008. p. 9. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf. Acesso em: 06 de fev. de 2023.

[6] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* 3ª ed. Rio de Janeiro: Forense, 2021. p. 12.

informação, já que "o consumidor não apenas consome (*consumption*), mas, também produz o bem de consumo (*production*)".[7]

Desde a promulgação da LGPD, a atuação dos Procons estaduais e municipais, tem se mostrado fundamental para garantir o cumprimento da LGPD. Os Procons seguem investigando eventuais violações à privacidade e proteção de dados pessoais, quando relacionadas às relações de consumo, bem como protegendo os direitos dos consumidores em caso de abuso, instaurando processos administrativos com consequente aplicação de multas.

Um exemplo dessa atuação dos Procons em temas de Proteção de Dados envolvendo consumidores é o caso da empresa Decolar. Em janeiro de 2020, o Procon de São Paulo, mediante processo administrativo, multou a empresa em valor superior a um milhão[8] por precificar os seus serviços de acomodação de forma discriminatória, utilizando a localização geográfica do usuário.

Outro caso aconteceu em janeiro de 2023. O Procon do Estado de São Paulo notificou a rede social Twitter questionando sobre o vazamento de dados de milhões de usuários da plataforma.[9] O órgão requereu que a empresa: (i) explicasse quais medidas técnicas e organizacionais adota para atender ao disposto na LGPD; (ii) esclarecesse qual a finalidade e base legal para o tratamento de dados; (iii) informasse como foi obtido o consentimento do usuário, por quanto tempo os dados ficariam armazenados, qual finalidade do tratamento e a política de descarte dos dados; e (iv) informasse os motivos que desencadearam o vazamento de dados, e quais medidas foram tomadas para conter o episódio e mitigar os riscos.

Assim, é importante destacar que a atuação dos Procons e a implementação da LGPD devem ser vistas como medidas complementares, que têm como objetivo garantir a proteção dos direitos dos consumidores em relação à privacidade e segurança de seus dados pessoais. Além disso, diante dos casos expostos, verifica-se que o problema enfrentado pelo tratamento irregular de dados pessoais é cada vez mais complexo e multidisciplinar. Por isso, órgãos do consumidor e ANPD precisam atuar em conjunto.

Por fim, também é fundamental que as empresas e a sociedade em geral reconheçam a importância da proteção dos dados pessoais e se empenhem em adotar práticas que garantam a privacidade e a segurança desses dados.

---

[7] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* 3ª ed. Rio de Janeiro: Forense, 2021. p. 13.
[8] Disponível em: https://www.procon.sp.gov.br/procon-sp-multa-decolar/. Acesso em: 08 de jan. de 2023.
[9] Disponível em: https://www.procon.sp.gov.br/procon-sp-notifica-twitter/ Acesso em: 08 de jan. de 2023.

2. O consentimento no CDC e na LGPD

Se, nas relações de consumo, em regra, há nexos de assimetria e desbalanceamento de poderes e possibilidades entre os atores principais, no contexto relacionado à proteção de dados pessoais, não é diferente. O debate sobre o consentimento, tanto no CDC quanto na LGPD tem origem neste desequilíbrio de forças, nesta discrepância entre as possibilidades dos titulares de direitos e deveres nas relações econômicas e informacionais. Muitas vezes, como já esclarecido neste artigo, as figuras de consumidor e titular de dados se confundem, visto que, em regra, os consumidores são também titulares de dados e os mercados econômico e informacional se retroalimentam.

Desta forma, pode-se dizer que o consentimento tem muita importância nos dois casos, efetivando a autodeterminação informacional e reforçando aspectos relacionados à autonomia privada dos indivíduos. No entanto, ainda que haja esta correlação de sujeitos de direito, o modelo de consentimento trazido na LGPD e no CDC não é o mesmo.

Mesmo que tratado de maneira implícita no CDC, o consentimento é um dos pilares fundamentais nas relações de consumo, representando a manifestação de vontade do consumidor em adquirir um produto ou serviço, com base em informações claras, precisas e verdadeiras fornecidas pelos fornecedores.

O consentimento no CDC está diretamente conectado com as relações contratuais firmadas, de maneira que aplica-se a anulabilidade do contrato em caso de vícios desta manifestação de vontade. De acordo com Claudia Lima Marques, se na formação do contrato houver vício no âmbito da vontade de uma das partes, o negócio jurídico é passível de anulação, conforme destaca a teoria dos vícios do consentimento, presente no Código Civil Brasileiro, nos arts. 138 a 165 (MARQUES, 2016, p. 70).

A história do CDC revela um processo evolutivo que acompanhou o desenvolvimento do país e as mudanças no cenário econômico e social. Nesse sentido, conforme explica Bruno Bioni, “toda normatização ali desenhada desemboca para que o consumidor seja capacitado para autodeterminar as suas informações pessoais”.[10]

[10] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3ª ed. Rio de Janeiro: Forense, 2021, p.125.

O art. 6º, III, do CDC[11] estabelece como um dos direitos básicos do consumidor o fornecimento de informação adequada e clara sobre os produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem.

Além disso, o CDC protege os consumidores contra práticas comerciais enganosas e abusivas, que podem induzir o consumidor a erro e afetar o exercício do consentimento. Um exemplo é a prática a que se refere o art. 37[12], que trata da publicidade enganosa e abusiva, reforçando a ideia de que o consentimento do consumidor deve ser livre e informado.

Desta feita, o consentimento do consumidor no CDC, em sua natureza, está intrinsecamente relacionado à ideia de erro destacada, de maneira que caso o consumidor não possua as informações completas e acessíveis ou seja comprometido por uma visão distorcida do negócio, haveria, de certa maneira, um vício no consentimento, mesmo que este não necessite ser fornecido ativamente. Sobre isto, cabe destacar os ensinamentos da grande Claudia Lima Marques:

> Note-se, porém, que a teoria dos vícios do consentimento continua a estar presente mesmo na nova concepção social de contrato, tanto que algumas de suas ideias vão ser usadas como base para novas figuras e obrigações impostas pelas leis intervencionistas. Assim, a ideia de erro, como falsa visão da realidade, que leva uma pessoa a contratar em circunstâncias em que normalmente - se tivesse a verdadeira visão da realidade - não contrataria, será uma das fontes da nova figura do direito do consumidor, o dever de informar, que foi imposto de maneira abrangente aos fornecedores de bens e serviços pelo novo Código brasileiro. (MARQUES, 2016, p.283)

Ainda, o CDC estabelece normas de proteção ao consumidor no âmbito das relações contratuais, garantindo que contratos sejam claros, objetivos e equilibrados. O consentimento está implícito nessa proteção, uma vez que os consumidores devem concordar com os termos e condições estabelecidos nos contratos de consumo.

A evolução do consentimento no CDC revela o processo contínuo de aperfeiçoamento, que acompanha as transformações da sociedade e visa a garantir cada vez mais a autonomia, a

[11] CDC. Art. 6º São direitos básicos do consumidor: III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem.
[12] CDC. Art. 37. É proibida toda publicidade enganosa ou abusiva.

liberdade de escolha e a proteção dos direitos do consumidor. Essa trajetória histórica evidencia o compromisso em fortalecer as relações de consumo, assegurando que o consentimento seja exercido de maneira informada e livre, e demonstra a relevância do CDC como instrumento fundamental na busca por um equilíbrio entre consumidores e fornecedores no mercado.

Já com relação à LGPD, o consentimento configura-se como apenas uma das bases legais que permitem o tratamento de dados, ou seja, é uma das hipóteses autorizadoras que justificam o processamento dos dados pessoais. É a base que demanda maior cuidado e de mais difícil operacionalização, controle, manutenção e autenticação de validade.

De acordo com Bruno Bioni e Maria Luciano, o consentimento sofreu uma espécie de hipertrofia em suas qualificadoras. Agora, este não se qualifica mais apenas como informado, de modo que deve ser, além disso, livre, específico, inequívoco e expresso.[13]

O consentimento informado é aquele em que o titular tem plena ciência do escopo do que está sendo concedido, de forma que deve haver transparência e clareza nas informações prestadas pelo controlador, que devem ser disponibilizadas de maneira adequada e ostensiva, de modo a atender o princípio do livre acesso, previsto no art. 9º da LGPD[14].

Quanto à necessidade de ser livre, isso se refere ao fato de que o consentimento deve ser fornecido de maneira completamente voluntária, sem qualquer tipo de coerção por parte dos agentes de tratamento.

Já o consentimento específico pressupõe a granularização e individualização, e deve ser concedido especificamente para cada finalidade determinada pelo agente de tratamento.

Ainda, para que o consentimento seja inequívoco, não deve haver qualquer resquício de dúvida quanto a sua validade. O agente de tratamento deve ser capaz de comprovar que se trata de uma indicação inequívoca, uma autorização clara e positiva do titular.

Por fim, para que o consentimento seja expresso, ele deve ser fornecido por uma ação clara, que indique de maneira efetiva a concordância com o tratamento de dados proposto,

[13] BIONI, Bruno Ricardo; LUCIANO, Maria. *O Consentimento Como Processo: em Busca do Consentimento Válido.* In: TRATADO DE PROTEÇÃO DE DADOS PESSOAIS. Bruno et al. (Orgs.). São Paulo: Thomson Reuters Brasil, 2020. p. 244-245.

[14] LGPD. 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.

podendo ser concedido por meio de uma declaração escrita, oral ou com o preenchimento de um formulário eletrônico, por exemplo.

3. A competência concorrente da Senacon e da ANPD

Na intersecção entre a proteção de dados pessoais e as relações de consumo, há duas entidades de extrema relevância, que devem coordenar suas ações em virtude da competência concorrente que lhes foi atribuída: ANPD e Senacon. Estes dois órgãos foram encarregados de prezar pela ordem, fiscalizar o cumprimento de suas respectivas leis setoriais e, acima de qualquer instância, proteger o indivíduo vulnerável frente a qualquer violação de seus direitos, tanto o titular de dados quanto o consumidor (muitas vezes, eles são os mesmos), cada uma no seu respectivo âmbito de atuação.

A Senacon é um órgão estatal vinculado ao Ministério da Justiça e Segurança Pública. Dentre suas funções, destacam-se o planejamento, a elaboração, a coordenação e execução da Política Nacional das Relações de Consumo, além de fiscalizar e aplicar sanções relacionadas a violações do CDC.

Já a ANPD foi criada por meio da Lei nº 13.853/2019 e, em 2022, foi transformada em autarquia de natureza especial pela Lei nº 14.460. Seu papel central é zelar pelo cumprimento da LGPD, fiscalizar e aplicar sanções em matéria de proteção de dados pessoais, bem como exercer diversas outras funções descritas no art. 55-J da LGPD.

A própria LGPD prevê a articulação da ANPD com outros órgãos e entidades que exerçam competências sancionatórias e normativas (art. 55-J, §§ 3º e 4º)[15], como é o caso da Senacon. Essa cooperação é necessária devido ao caráter concorrente da atuação das entidades em demandas específicas, que transpassam temáticas comuns, como na hipótese relacionada ao Direito do Consumidor[16].

[15] LGPD. Art. 55-J. § 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. § 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.

[16] A disposição sobre a cooperação entre as autoridades está descrita no art. 55-J, §§ 3º e 4º da LGPD, que foi incluído pela Lei nº 13.853/2019.

É importante destacar que se a atuação entre os órgãos de defesa do consumidor e da ANPD não for bem coordenada, isto é, se houver incerteza sobre quem deve atuar no caso concreto, há o risco de deixar os tutelados sem a proteção devida.

O CDC, por um lado, confere poder fiscalizatório à Senacon, assim como a ANPD tem esse poder garantido pela LGPD. A existência dessas duas entidades pode gerar uma duplicidade de competência em algumas demandas, e até uma sobreposição de iniciativas.

Neste sentido, a Senacon editou a Nota Técnica nº 4/2019[17], para tentar sanar questões relacionadas à Medida Provisória nº 869/2018 (MP), que alterava a LGPD para criar a ANPD. A Senacon criticou o fato de que, segundo a MP, as competências da ANPD para assuntos relacionados à proteção de dados pessoais deveriam prevalecer sobre competências correlatas de outras entidades, dando preferência ao órgão de proteção de dados sob o pretexto de evitar questões relacionadas à dupla penalização.

Para a Senacon, no entanto, "a nova competência preponderante da ANPD poderia colocar em risco o andamento e *enforcement* dos processos administrativos em andamento – sem prejuízo de outros que possam porventura serem instaurados –, motivo pelo qual não faz sentido que a Senacon seja privada de atuar no âmbito de uma matéria que é inerente às suas competências".

A Nota Técnica pontua que, nos termos do *caput* do art. 52 da LGPD, as sanções administrativas ali previstas são passíveis de aplicação somente pela ANPD, mas, de acordo com o entendimento da Senacon, a sua aplicação não substitui as sanções administrativas, civis ou penais previstas no CDC e na legislação específica.

Assim, nos parece que a ANPD não poderia atuar de forma exclusiva na fiscalização de questões relacionadas a dados pessoais e direitos consumeristas. Deve haver uma atuação compartilhada e sistematizada para garantir que todas as camadas de direitos dos indivíduos sejam tuteladas, sem deixar, em nenhuma hipótese, que se negligencie direitos de qualquer teor, sejam eles consumeristas ou relacionados à proteção dos dados pessoais.

Entendemos que o esforço da Senacon para reverter as disposições de preferência e exclusividade atribuídas à ANPD faz sentido e foi justificado na própria Nota Técnica, sob o

[17] Disponível em: https://consumidor.mppr.mp.br/arquivos/File/NotaTecnica04_2019_Senacon.pdf. Acesso em: 05 de jan. de 2023.

argumento de que grande parte dos bancos de dados são constituídos por dados de consumo, originados de relações de consumo, matéria de atuação da Senacon.

O órgão trouxe ainda um ponto de suma importância na relação de concorrência entre a Senacon e a ANPD: diferentemente do consumidor europeu, os brasileiros estão começando a entender a importância e o valor econômico de sua privacidade e de seus dados pessoais, de modo que a aplicação do CDC é especialmente importante nesse estágio de desenvolvimento sociocultural.

Nesse contexto, em 2021, foi celebrado Acordo de Cooperação Técnica (ACT) entre a ANPD e Senacon, por meio do qual a Senacon firmou o compromisso de compartilhar com a ANPD reclamações de consumidores relacionadas à proteção de dados[18]. O Acordo fez parte do Planejamento Estratégico da ANPD para o triênio 2021-2023 e teve como principal premissa promover o fortalecimento de uma cultura de proteção de dados pessoais no país.

O ACT cita como objeto a promoção de ações conjuntas sobre assuntos de interesse recíproco[19]. Dentre as sete ações inseridas nele, destacamos as letras (a), (c), (e) e (f), que focam no apoio recíproco das instituições, uniformização de entendimentos e coordenação de ações, promoção de estudos e desenvolvimento conjunto, bem como cooperação na atividade fiscalizatória, de maneira a garantir o diálogo constante e a possibilidade de uma atuação que garantirá a tutela dos dados pessoais e dos direitos consumeristas.

Vale ressaltar que, conforme mencionado, a atuação conjunta tratada no ACT deve ser bem coordenada para que não haja problemas relacionados a conflito de competências e iniciativas. Ambos os órgãos devem prezar pelo diálogo e por estabelecer limites prévios para a atuação na matéria, por exemplo, por meio de portarias e resoluções internas.

---

[18] Disponível em:https://www.gov.br/anpd/pt-br/acesso-a-informacao/acordo_anpd_senacon_assinado.pdf. Acesso em: 10 de jan. de 2023.

[19]As ações conjuntas elencadas no Acordo são: (a) apoio institucional e intercâmbio de informações relativas às suas respectivas esferas de atuação; (b) compartilhamento de informações agregadas e de dados estatísticos quanto a reclamações de consumidores relacionadas à proteção de dados pessoais, em especial, aquelas registradas no Sistema Nacional de Informações de Defesa do Consumidor - SINDEC e nas bases de dados do Consumidor.gov.br; (c) Uniformização de entendimentos e coordenação de ações, inclusive no que tange ao endereçamento de reclamações de consumidores e à atuação no caso de incidentes de segurança envolvendo dados pessoais de consumidores; (d) desenvolvimento de indicadores conjuntos relacionados à proteção de dados pessoais no âmbito das relações de consumo; (e) elaboração conjunta e intercâmbio de estudos, análises, notas técnicas e projetos de pesquisa sobre direitos do consumidor e proteção de dados pessoais; (f) desenvolvimento, organização e promoção de ações conjuntas de formação e de capacitação, incluindo cursos, seminários e elaboração de materiais informativos; e (g) cooperação quanto a ações de fiscalização relacionadas à proteção de dados pessoais no âmbito das relações de consumo.

Ainda em relação à cooperação entre ANPD e Senacon, destaca-se o caso da análise de adequação da política de privacidade do WhatsApp, que mobilizou a atuação conjunta das duas entidades, além do Conselho Administrativo de Defesa Econômica (CADE) e do Ministério Público Federal (MPF), por meio da elaboração de uma nota técnica conjunta[20].

A análise foi fruto de um trabalho que começou em maio de 2021 com o exame das políticas de privacidade lançadas à época, com o intuito de verificar a adequação destas frente à LGPD. O principal ponto controvertido do caso foi a previsão de compartilhamento de informações entre WhatsApp e Facebook e outros aplicativos do grupo, como Instagram e Messenger[21]. Foram expedidas três[22] notas técnicas e uma recomendação conjunta[23], conforme destaca o infográfico disponibilizado pela própria ANPD[24].

Ao final, todas as autoridades envolvidas coordenaram suas ações de forma conjunta buscando o aprimoramento das Políticas de Privacidade do WhatsApp e tutelando os direitos dos titulares de dados pessoais (e consumidores, neste caso).

Considerações Finais

Conforme exposto, o presente artigo apresenta, num primeiro momento, a evolução histórica da proteção coletiva e legitimação dos órgãos de fiscalização no Brasil. Além disso, demonstra que as figuras de consumidor e titular de dados muitas vezes se confundem e os mercados econômico e informacional estão amplamente interligados atualmente.

---

[20] Disponível em; https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf.Acesso em:13 de fev. de 2023.

[21] Disponível em: https://www.techtudo.com.br/noticias/2021/01/whatsapp-muda-politica-de-privacidade-e-compartilha-dados-com-o-facebook.ghtml. Acesso em: 13 de fev. de 2023.

[22] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsapp_ocr.pdf https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTcnica19.2021.CGF.ANPD.pdf https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf.Acesso em: 13 de fev. de 2023.

[23] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/AtodeRecomendaoConjunta.pdf. Acesso em: 13 de fev. de 2023.

[24] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-a-analise-de-adequacao-da-nova-politica-de-privacidade-do-aplicativo-a-lgpd. Acesso em: 13 de fev. de 2023.

Num segundo momento, o artigo trata dos dois modelos de consentimento previstos no CDC e na LGPD, visto que sua compreensão é fundamental para garantir a autodeterminação informacional e reforçar aspectos relacionados à autonomia do indivíduo.

De um lado, o consentimento no CDC, mesmo que implícito, é um pilar fundamental nas relações de consumo. De outro, na LGPD, o consentimento é uma das bases legais que autorizam o tratamento de dados pessoais. A evolução desse instituto na legislação brasileira evidencia o compromisso no fortalecimento da proteção dos direitos dos consumidores e dos titulares de dados na promoção de um ambiente equilibrado e justo nas relações comerciais e informacionais.

Com relação à atuação concorrente entre ANPD e Senacon, restou claro que é de suma importância a coordenação de ações e a elaboração prévia de atos normativos que determinem o escopo de atuação de cada órgão de forma mais concreta, a fim de que não se deixe a parte mais vulnerável da relação sofrer prejuízos com a falta de tutela ou com duplas penalizações.

Por fim, destaca-se que o desenvolvimento da cultura de proteção de dados pessoais e direitos do consumidor depende intimamente da ampla discussão da temática, sendo de suma importância a reflexão a respeito da necessária complementaridade das duas áreas, sempre considerando as particularidades de cada matéria e sua inegável intersecção.

Referências bibliográficas

ANPD; Cade; MJSP; MPF. *Recomendação. 2021*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/AtodeRecomendaoConjunta.pdf. Acesso em: 06 de janeiro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; SECRETARIA NACIONAL DO CONSUMIDOR; CONSELHO NACIONAL DE DEFESA DO CONSUMIDOR. *Como Proteger seus Dados Pessoais: guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a Senacon.* Brasília: Ministério da Justiça, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 24 de janeiro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Nota Técnica nº 02/2021/CGTP/ANPD.* 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsapp_ocr.pdf. Acesso em: 13 de fevereiro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *ANPD conclui a análise de adequação da nova Política de Privacidade do WhatsApp à LGPD.* 2022. Disponível em:

https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-a-analise-de-adequacao-da-nova-politica-de-privacidade-do-aplicativo-a-lgpd. Acesso em: 13 de fevereiro de 2023

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Nota Técnica nº 19/2021/CGF/ANPD*. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTcnica19.2021.CGF.ANPD.pdf. Acesso em: 13 de janeiro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Nota Técnica nº 49/2022/CGF/ANPD*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf. Acesso em:13 de fevereiro de 2023.

BRASIL. **Código de defesa do consumidor**. Lei 8.078 de 11/09/90. Brasília, Diário Oficial da União, 1990.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018. Acesso em 10 de janeiro de 2022.

BIONI, Bruno Ricardo; LUCIANO, Maria. *O Consentimento Como Processo: em Busca do Consentimento Válido*. In: *Tratado de Proteção de Dados Pessoais*. Bruno et al. (Orgs.). São Paulo: Thomson Reuters Brasil, 2020.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3ª ed. Rio de Janeiro: Forense, 2021.

CARDOSO, Pedro. *WhatsApp muda política de privacidade e compartilha dados com o Facebook*. TechTudo, 2021. Disponível em: https://www.techtudo.com.br/noticias/2021/01/whatsapp-muda-politica-de-privacidade-e-compartilha-dados-com-o-facebook.ghtml. Acesso em: 13 de fevereiro de 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. *Nota Técnica nº 4/2019/GAB-Senacon/Senacon/MJ*. 2019. Disponível em: https://consumidor.mppr.mp.br/arquivos/File/NotaTecnica04_2019_Senacon.pdf. Acesso em: 05 de janeiro de 2023

GRINOVER, Ada Pellegrini. *Novas tendências na tutela jurisdicional dos interesses difusos*. Revista da Faculdade de Direito. Universidade de São Paulo, 1984. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67016. Acesso em: 10 de fevereiro de 2023.

MARQUES, Claudia Lima. Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais - 8. ed. rev. atual. e ampl. São Paulo : Editora Revista dos Tribunais. 2016.

MENDES, Laura Schertel. *Transparência e Privacidade: Violação e proteção da informação pessoal na sociedade de consumo*. Dissertação de Mestrado - Faculdade de Direito da Universidade de Brasília. Brasília 2008. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf. Acesso em: 06 de fevereiro de 2023.

APLICAÇÃO DA LGPD NO DIREITO ELEITORAL

Gustavo Vieira de Sousa[1]
Isabella Maria Farias Carvalho[2]

Resumo: O presente artigo pretende analisar as discussões sobre a proteção de dados pessoais em processos eleitorais, com ênfase no contexto brasileiro. Nesse sentido, pretende-se entender como o TSE e a ANPD têm trabalhado em conjunto para que as tecnologias atuais, que facilitam o tratamento de dados pessoais, não afetem a proteção dos direitos ao voto e à privacidade dos eleitores brasileiros. Para analisar esse problema de pesquisa, utilizou-se de método dedutivo e das técnicas de pesquisa de revisão bibliográfica e análise documental. O artigo conclui ser essencial o contato entre a Justiça Eleitoral e a ANPD para o desenvolvimento de estratégias para a regulação do uso dos dados pessoais na seara eleitoral, sendo incompleta a regulação feita de forma separada.

Palavras-chave: dados pessoais; eleições; justiça eleitoral.

Abstract: *This article aims to analyze the discussions about the protection of personal data in electoral processes, with emphasis on the Brazilian context. In this sense, it is intended to understand how the TSE and the ANPD have worked together to ensure that current technologies, which facilitate the processing of personal data, do not affect the protection of the rights to suffrage and privacy of Brazilian voters. To analyze this research problem, the deductive method and the research techniques of bibliographic review and document analysis were used. The article concludes that the contact between the Electoral Justice and the ANPD is essential for the development of strategies for the regulation of the use of personal data in the electoral field, since a separate regulation is incomplete.*

[1] Pós-graduado em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito. Aluno do curso de pós-graduação lato sensu do Centro Universitário de Brasília - UniCEUB/ICPD.
[2] Bacharela em Direito pela Universidade de Brasília. Pós-graduanda em Direito Penal e Processual Penal pela Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios. Pesquisadora Voluntária no Projeto IDP Privacy Lab 2023 (CEDIS).

Keywords: *personal data; elections; electoral justice.*

Introdução

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - "LGPD") estabeleceu um marco regulatório no Brasil para a proteção de direitos de titulares de dados pessoais. Em âmbito constitucional, a partir da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, a proteção de dados pessoais adquiriu o *status* de direito fundamental, insculpido na Constituição Federal de 1988 (CF/88)[3].

A Constituição Federal também dispõe sobre direitos eleitorais, estabelecendo como cláusula pétrea o direito ao voto direto, secreto, universal e periódico[4]. De tempos em tempos, o fenômeno das eleições domina o cenário nacional e os partidos políticos utilizam diversas ferramentas para angariar votos aos seus representantes, por meio de campanhas políticas.

Em um cenário no qual tais campanhas políticas utilizam ferramentas e técnicas de marketing baseadas no tratamento de dados pessoais, surge a necessidade de compreender a aplicação da LGPD no contexto das eleições, especialmente diante das "limitações estruturais, conceituais e operacionais para lidar com um novo cenário de ferramentas de marketing político digital baseado na coleta, tratamento, análise e uso de dados pessoais"[5].

O presente artigo busca observar como o Tribunal Superior Eleitoral (TSE) e a Autoridade Nacional de Proteção de Dados (ANPD) atuaram em conjunto nas eleições de 2022 para que as atividades de tratamento de dados pessoais não afetassem a proteção dos direitos ao voto e à privacidade dos eleitores brasileiros. O texto está dividido em 3 partes: na primeira é realizada uma breve análise da estrutura e da atuação da justiça eleitoral brasileira, na segunda é realizada a mesma análise para a Autoridade Nacional de Proteção de Dados e, por fim,

[3] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[4] Art. 60. A Constituição poderá ser emendada mediante proposta: (...) § 4º Não será objeto de deliberação a proposta de emenda tendente a abolir: (...) II - o voto direto, secreto, universal e periódico;

[5] MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. Proteção de Dados nas Eleições: democracia e privacidade. Grupo de Estudos em Proteção de Dados e Eleições, 2020.

observa-se como essas estruturas foram movimentadas para atuarem de forma conjunta nas Eleições de 2022.

1. Breve análise da estrutura e da atuação da justiça eleitoral brasileira

Inicialmente, o Poder Legislativo foi o responsável pelo andamento das eleições e dos mandatos, bem como pela análise da elegibilidade e das investiduras políticas de seus membros, decidindo nas lides que surgissem[6].

Com a promulgação do primeiro Código Eleitoral, em 1932, tal sistema foi substituído pelo de jurisdição especializada, passando a matéria eleitoral para responsabilidade de um órgão especializado dentro da estrutura do Poder Judiciário. Dessa forma, a Justiça Eleitoral é a instituição independente responsável pelo andamento das eleições e pela resolução dos conflitos surgidos no contexto dessas. Na Constituição de 1934, a Justiça Eleitoral foi constitucionalizada, status que foi mantido na Constituição de 1988[7].

A Justiça Eleitoral tem natureza federal, é mantida pela União, é assessorada pela Polícia Judiciária Federal para a instauração e condução de inquéritos policiais para a análise de crimes eleitorais e, diferentemente dos demais órgãos que compõem o Poder Judiciário, não possui corpo próprio e independente de juízes, contando com magistrados oriundos de outros tribunais, que têm investidura temporária na seara eleitoral - prazo de 2 anos que pode ser renovado por somente um período subsequente[8], como o intuito de manter a imparcialidade da Justiça Eleitoral[9].

Ressalta-se, ademais, que assim como em outras searas do Poder Judiciário, a Justiça Eleitoral também conta com princípios para as suas análises, estando entre eles os seguintes: democracia, democracia representativa, Estado Democrático de Direito, soberania popular, moralidade, probidade, anterioridade ou anualidade eleitoral, dentre outros[10].

Com relação às suas competências, a Justiça Eleitoral concentra quatro funções referentes ao processo eleitoral. São elas: competência administrativa[11], competência

[6] Gomes, José Jairo. Direito Eleitoral. 12. ed. – São Paulo: Atlas, 2016, pp. 88-89.
[7] Art. 92, inciso IV da CF/88.
[8] Art. 121, § 2º da CF/88.
[9] Gomes, José Jairo. Direito Eleitoral. 12. ed. – São Paulo: Atlas, 2016, p. 90.
[10] Ibid, p. 64.
[11] Art. 41, §2°, LE.

jurisdicional[12], competência normativa[13] e competência consultiva[14]. Essas competências buscam construir uma governança eleitoral independente, especializada e não vinculada ao Poder Executivo[15].

1.1. Competências da Justiça Eleitoral

A Justiça Eleitoral do Brasil possui competências relacionadas às atividades eleitorais e concentra quatro funções referentes ao processo eleitoral. São elas: competência administrativa[16], competência normativa[17], competência consultiva[18] e competência jurisdicional[19]. Essas competências buscam construir uma governança eleitoral independente, especializada e não vinculada ao Poder Executivo[20].

Primeiramente, dentro de sua competência administrativa, inexistindo conflito a ser resolvido, a Justiça Eleitoral desempenha o papel de organizar e administrar o processo eleitoral, podendo aqui agir em sentido contrário ao princípio processual da demanda - isto é, pode agir de ofício, independentemente de provocação do interessado. Exemplos de exercício de tal função são a expedição de título eleitoral, a designação de locais de votação e autorização para a transmissão de propaganda partidária[21].

A competência administrativa compreende o exercício do poder de polícia, isto é:

> Atividade da administração pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de

[12] Art. 22, 29 e 35, II, III e VIII, CE.
[13] Art. 1°, parágrafo único e art. 23, IX, CE e art. 105, caput, LE.
[14] Art. 23, XII e art. 30, VIII, CE.
[15] COSTA, Rafael. As funções da Justiça Eleitoral. Revista Brasileira de Direito Eleitoral – RBDE | Belo Horizonte, ano 8, n. 15, p. 131-148, jul./dez. 2016; BARRETO, Álvaro. A Justiça Eleitoral brasileira: modelo de governança eleitoral. Paraná Eleitoral, v.4, n.2, p.189-216.
[16] Lei das Eleições. Art. 41, §2°.
[17] Lei das Eleições. Art. 1°, parágrafo único e art. 23, IX, e art. 105, caput.
[18] Lei das Eleições. Art. 23, XII e art. 30, VIII.
[19] Lei das Eleições. Art. 22, 29 e 35, II, III e VIII.
[20] COSTA, Rafael. "As funções da Justiça Eleitoral". Revista Brasileira de Direito Eleitoral – RBDE | Belo Horizonte, ano 8, n. 15, p. 131-148, jul./dez. 2016; BARRETO, Álvaro. "A Justiça Eleitoral brasileira: modelo de governança eleitoral". Paraná Eleitoral, v. 4, n. 2, pp. 189-216.
[21] GOMES, José Jairo. Direito Eleitoral. 12. ed. – São Paulo: Atlas, 2016, pp. 91-92.

> concessão ou autorização do Poder Público, à tranquilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos[22].

Ou seja, o Poder de Polícia fundamenta a faculdade do Estado de intervir na ordem pública, limitando a liberdade das pessoas.

A competência jurisdicional, em oposição à administrativa, caracteriza-se pela existência de conflito a ser resolvido, cabendo o princípio processual da demanda, ou seja, deve haver provocação do interessado. Devem estar presentes as condições da ação e os requisitos de interesse, legitimidade e possibilidade jurídica do pedido, além dos pressupostos processuais de jurisdição, citação válida, capacidade postulatória, capacidade processual e competência do juiz, não podendo haver litispendência e coisa julgada. Exemplos de exercício da função jurisdicional são a aplicação de multas pela realização de propaganda eleitoral ilícita e cassação de registro eleitoral. Ademais, não é incomum que a competência jurisdicional surja de conflitos originados do exercício da competência administrativa, tendo em vista a superveniência de conflito[23].

O Poder Judiciário, em regra, não tem competência normativa. No entanto, a Justiça Eleitoral adquiriu tal competência por previsão do legislador no Código Eleitoral. A normatividade da Justiça Eleitoral é manifestada por meio das resoluções do TSE[24]. Outra competência que em regra não é do Poder Judiciário é a consultiva, tendo em vista que, normalmente, somente se pronuncia sobre casos concretos trazidos pelas partes interessadas.

No entanto, de forma a prevenir litígios que poderiam comprometer a regularidade e a legitimidade do processo eleitoral, a Justiça Eleitoral, representada tanto pelo TSE quanto pelos Tribunais Regionais Eleitorais (TREs), analisa e responde, de forma fundamentada, a consultas. Os requisitos legais para a apresentação da consulta são a legitimidade do ente que consulta e a ausência da conexão da questão com situações concretas. A resposta à consulta não é vinculante, mas pode orientar a ação dos órgãos da Justiça Eleitoral e servir de fundamento para decisões administrativas ou judiciais[25].

[22] BATISTA JÚNIOR, Onofre Alves. O poder de polícia fiscal. Belo Horizonte: Mandamentos, 2001.
[23] Ibid, pp. 92-93.
[24] Ibid, p. 94.
[25] GOMES, José Jairo. Direito Eleitoral. 12. ed. – São Paulo: Atlas, 2016, pp. 94-95.

1.2. Tribunal Superior Eleitoral

O Tribunal Superior Eleitoral (TSE) é o órgão de jurisdição nacional da Justiça Eleitoral composto por no mínimo sete membros escolhidos dentre os ministros do STF, os ministros do STJ e advogados de notável saber jurídico e idoneidade moral indicados pelo STF[26]. Com relação aos advogados, o Código Eleitoral (CE)[27] prevê que estes não podem ser ocupantes de cargos públicos não estáveis, não podem ser diretores, proprietários ou sócios de empresas beneficiadas em virtude de contrato com a Administração Pública e não podem exercer mandato de caráter político. Ademais, como exposto anteriormente, ressalta-se que de forma a favorecer a imparcialidade dos órgãos da Justiça Eleitoral, os membros do TSE não são vitalícios, mas gozam das demais garantias previstas na Constituição[28].

De acordo com o CE[29], o TSE delibera por maioria de votos, em sessão pública, com a presença da maioria de seus membros. No entanto, as decisões do TSE para a cassação de registro de partidos políticos e em recursos que levem à anulação geral de eleições ou perda de diplomas só poderão ser tomadas com a presença de todos os membros do Tribunal. Caso algum juiz esteja impedido, o substituto ou o suplente será convocado. Caso a convocação não seja possível, o TSE já entendeu que o julgamento pode seguir com o quórum incompleto[30].

Com relação às competências do TSE, o art. 21 do CE dispõe que cabe a este (i) processar e julgar originariamente o registro e a cassação de registro de partidos políticos, os conflitos de jurisdição entre TREs e juízes eleitorais de diferentes estados, os crimes eleitorais, os habeas corpus e os mandados de segurança em matéria eleitoral relativos a atos do presidente, dos ministros de estado e dos ministros dos TREs, as impugnações à apuração do resultado geral das eleições, dentre outros; e (ii) julgar os recursos interpostos das decisões dos TREs, inclusive os que versarem sobre matéria administrativa. Com relação a este segundo ponto, no entanto, entende-se não ser cabível ao TSE apreciar recurso contra decisão de natureza estritamente administrativa dos TREs, pois tal matéria não está contemplada no art. 121, § 4º, da Constituição Federal.

A CF/88 prevê que somente caberá recurso das decisões dos TREs quando (i) forem proferidas contra disposição expressa da CF/88 ou da lei; (ii) quando houver divergência na

[26] Art. 119 da CF/88.
[27] Art. 16, § 2º do CE.
[28] Art. 95 da CF/88.
[29] Art. 19 do CE.
[30] GOMES, José Jairo. Direito Eleitoral. 12. ed. – São Paulo: Atlas, 2016, p. 96.

interpretação de lei entre dois ou mais tribunais eleitorais; (iii) quando tratarem de inelegibilidade ou expedição de diplomas nas eleições federais ou estaduais; (iv) quando anularem diplomas ou decretarem a perda de mandatos eletivos federais ou estaduais; ou (v) quando denegarem *habeas corpus*, mandado de segurança, *habeas data* ou mandado de injunção.

O art. 22 do CE prevê demais competências privativas do TSE, tais como elaborar o seu regimento interno, aprovar o afastamento do exercício dos cargos efetivos dos juízes dos tribunais regionais eleitorais, aprovar a divisão dos estados em zonas eleitorais ou a criação de novas zonas, responder, sobre matéria eleitoral, às consultas que lhe forem feitas em tese por autoridade com jurisdição federal ou órgão nacional de partido político, requisitar *força federal* necessária ao cumprimento da lei, de suas próprias decisões ou das decisões dos tribunais regionais que o solicitarem, e para garantir a votação e a apuração, e tomar quaisquer outras providências que julgar convenientes à execução da legislação eleitoral.

De acordo com o art. 121, § 3º da CF/88, são irrecorríveis as decisões do TSE, salvo as que contrariarem a Constituição e as denegatórias de *habeas corpus* ou mandado de segurança.

Ressalta-se que dentre suas atribuições e competências, o TSE possui a faculdade de "tomar quaisquer outras providências que julgar convenientes à execução da legislação eleitoral". É exatamente com relação a esta faculdade que o TSE, em virtude da crescente difusão de meios tecnológicos disponíveis, optou por realizar Acordos de Cooperação visando dar transparência, efetividade e segurança ao processo eleitoral, como será abordado a seguir.

1.3. Partidos Políticos e Dados de Eleitores

Atualmente, o Brasil possui dois principais marcos legais que fundamentam as análises sobre proteção de dados pessoais. São eles: o Marco Civil da Internet ("Lei nº 12.965/2014" ou "MCI") e a Lei Geral de Proteção de Dados Pessoais ("Lei nº 13.709/2018" ou "LGPD"). Além disso, quando o direito eleitoral é abordado, tanto a Lei das Eleições ("Lei nº 9.504/1997") quanto as Resoluções do Tribunal Superior Eleitoral ("TSE") são aplicáveis.

Antes de explorar os detalhes sobre o tratamento de dados por partidos políticos, é necessário compreender a aplicabilidade da legislação de proteção de dados a esses. Os partidos

políticos são pessoas jurídicas de direito privado[31] e tratam dados pessoais de eleitores, filiados, militantes, simpatizantes, funcionários e outros[32]. Desta forma, é possível depreender que eles estão incluídos no escopo do art. 1º da LGPD, uma vez que a lei "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado". Ou seja, a própria redação do diploma legal possibilita a aplicabilidade da LGPD aos partidos políticos.

No entanto, as regulamentações setoriais, especialmente as Resoluções do TSE, devem ser analisadas tanto à luz do direito à proteção de dados quanto à luz do direito eleitoral. Se por um lado os partidos precisam utilizar dados pessoais para que tenham as finalidades de seus estatutos cumpridas, por outro lado, existe a grande preocupação em atrair novos eleitores para o centro das disputas, angariando votos e potencializando a reverberação de opiniões no contexto das eleições.

Nesse sentido, é importante destacar que em processos eleitorais, o direito à proteção de dados deve ser observado pelas campanhas dos partidos caso haja qualquer operação de tratamento de dados pessoais[33].

A partir da compreensão de que o direito à proteção de dados pessoais seja aplicável aos partidos políticos, surge a problemática de como fazer cumprir a legislação e proteger, de forma eficaz, os dados pessoais dos eleitores. As principais questões que serão abordadas neste artigo dizem respeito ao tratamento automatizado de dados e ao envio de propaganda eleitoral.

No âmbito das campanhas políticas que recorrem a processos automatizados de tratamento de dados pessoais, faz-se necessário o respeito às disposições da LGPD "que desempenha papel crucial para o estabelecimento de uma relação de confiança entre candidatas ou candidatos e eleitoras ou eleitores, bem como para assegurar a estes as condições necessárias para uma escolha autônoma e bem-informada" (TSE, 2021).

[31] CF/88. Art. 17. É livre a criação, fusão, incorporação e extinção de partidos políticos, resguardados a soberania nacional, o regime democrático, o pluripartidarismo, os direitos fundamentais da pessoa humana e observados os seguintes preceitos: (...) § 2º Os partidos políticos, após adquirirem personalidade jurídica, na forma da lei civil, registrarão seus estatutos no Tribunal Superior Eleitoral.

[32] ARCHEGAS, João Victor. Relatório de Boas Práticas: Proteção de Dados e Partidos Políticos no Brasil. ITS Rio, 2021.

[33] MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. Proteção de Dados nas Eleições: democracia e privacidade. Grupo de Estudos em Proteção de Dados e Eleições, 2020.

A principal questão que surge a partir do tratamento automatizado de dados pessoais é o risco inerente de discriminação. Ana Frazão indica que "para avaliar os riscos de discriminações indevidas é fundamental examinar (i) a qualidade, a atualização e a licitude dos dados usados para o julgamento; (ii) a licitude e a legitimidade do julgamento em si; e (iii) a pertinência e a congruência entre esses dados e as finalidades pretendidas pelo tratamento"[34].

Laura Schertel sintetiza algumas formas de discriminação algorítmica, de modo que as mais preocupantes no contexto eleitoral seriam a "discriminação por generalização", que acontece pela classificação equivocada de pessoas a determinados grupos e a "discriminação pelo uso de informações sensíveis", uma vez que para sua classificação há de se basear em características endógenas ou destacar grupos historicamente discriminados[35].

Isto é, nem todos os dados podem ser utilizados para finalidades comerciais ou políticas. Ainda assim, os que podem, devem ser utilizados para finalidades lícitas e congruentes.

Já em relação ao envio de propaganda eleitoral, existem algumas hipóteses nas quais a legislação eleitoral permite quais e como os dados pessoais podem ser tratados para essa finalidade.

A Lei das Eleições autoriza que candidatos, partidos e/ou coligações possam enviar propaganda eleitoral via mensagens eletrônicas, com a comprovação de que os endereços eletrônicos tenham sido cadastrados de forma gratuita pelo candidato, partido ou coligação. Isto é, não há a possibilidade de uso de dados pessoais que tenham sido coletados de forma onerosa[36].

A Resolução TSE nº 23.610/2019, regulamentou a forma pela qual a coleta de endereços eletrônicos fosse realizada, em especial, determinando a exigência do consentimento do titular. Para esses casos, como bem destacado na obra *Proteção de Dados nas Eleições: democracia e privacidade*, "não só os dados pessoais têm que ser coletados de forma gratuita, como também

[34] FRAZÃO, Ana; DE CARVALHO, Ângelo Prata; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022.

[35] SCHERTEL MENDES, L.; MATTIUZZO, M. DISCRIMINAÇÃO ALGORÍTMICA: CONCEITO, FUNDAMENTO LEGAL E TIPOLOGIA. Direito Público, [S. l.], v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 29 maio. 2023.

[36] Lei nº 9.504/1997. Art. 57-B. A propaganda eleitoral na internet poderá ser realizada nas seguintes formas: (...) III - por meio de mensagem eletrônica para endereços cadastrados gratuitamente pelo candidato, partido ou coligação.

deve ser obtido o consentimento do titular nos termos da LGPD, ou seja, o consentimento informado, livre e inequívoco"[37].

Ainda no âmbito da Resolução TSE nº 23.610/2019, existe a determinação de descadastramento obrigatório para candidatos, partidos e coligações. Isto é, quando enviadas mensagens eletrônicas ou instantâneas, o titular deve ser capaz de se opor ao tratamento e se descadastrar da lista. Isto significa que, em última instância, o eleitor pode revogar seu consentimento, garantindo assim o seu direito à autodeterminação informativa[38].

O tratamento de dados pessoais sensíveis é outro problema que deve ser enfrentado, uma vez que dados sobre opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político[39], por exemplo, exigem a observância de critérios mais rigorosos, com a implementação de salvaguardas capazes de proteger os titulares de dados.

Nesse sentido, destaca-se a importância que seja implementado um tratamento diferenciado e mais rigoroso aos dados pessoais sensíveis, em virtude do alto potencial de discriminações[40].

Desta forma, há um crescente desafio aos partidos políticos, candidatos e coligações para que, no âmbito do tratamento de dados pessoais de eleitores, sejam capazes de implementar mecanismos capazes de efetivar e dar segurança, de forma concreta, aos dados pessoais de eleitores.

---

[37] MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. Proteção de Dados nas Eleições: democracia e privacidade. Grupo de Estudos em Proteção de Dados e Eleições, 2020.

[38] Vide Laura Schertel Mendes e Gabriel C. Soares da Fonseca que, ao analisarem as funções do consentimento, entendem que este não é o único mecanismo para o exercício da autodeterminação informativa, mas que também precisam ser incorporados nos sistemas, códigos, arquiteturas e procedimentos tecnológicos, aumentando a confiança dos indivíduos no sistema e no tratamento de dados realizado e permitir que o titular de dados possa configurar e determinar suas preferências acerca do que é feito com os desdobramentos virtuais de sua personalidade.

[39] Art. 5º (...) 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;

[40] FRAZÃO, Ana; DE CARVALHO, Ângelo Prata; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022.

2. Breve análise da estrutura e da atuação da Autoridade Nacional de Proteção de Dados (ANPD)

Como previsto no art. 5º, inciso XIX da LGPD, a ANPD é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. A ANPD foi criada e incluída na LGPD pela Lei nº 13.853, de 2019, tendo sua estrutura sido aprovada em agosto de 2020[41], logo após a entrada em vigor imediata da LGPD.

A ANPD é composta[42] pelo Conselho Diretor, que é o órgão máximo de direção, pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, por uma Corregedoria, uma Ouvidoria, uma Procuradoria e por unidades administrativas e unidades especializadas necessárias à aplicação do disposto na LGPD.

Inicialmente a ANPD teve natureza de órgão da administração pública federal e a sua estrutura esteve vinculada à Presidência da República. No entanto, o § 1º do Art. 55-A da LGPD já previa que a vinculação da ANPD à Presidência era transitória, podendo essa ser transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. Dessa forma, com o intuito de conferir à Autoridade autonomia administrativa e financeira, foi promulgada a Lei nº 14.460, de 25 de outubro de 2022, que transformou a ANPD em autarquia de natureza especial.

De acordo com a ANPD, a independência da Autoridade traz maior segurança jurídica para os indivíduos e organizações, contribui para a facilitação do comércio internacional e para o aumento da competitividade, além de trazer relevantes impactos para a sociedade e para as empresas, proporcionando (i) compatibilidade com outros regimes regulatórios ao redor do mundo, (ii) alinhamento com melhores práticas internacionais, e (iii) aprimoramento da condição do País para o ingresso em organismos e blocos internacionais, a exemplo da Organização para a Cooperação e Desenvolvimento Econômico - OCDE[43].

Dentre as competências da ANPD estão: (i) elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (ii) fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo

[41] Decreto nº 10.474, de 26 de agosto de 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em 27 de fev de 2023.
[42] Art. 55-C da LGPD.
[43] ANPD torna-se autarquia de natureza especial. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial. Acesso em 27 de fev de 2023.

administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (iii) apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (iv) promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (v) 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; (v) celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos; e (vi) articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação[44].

3. Atuação da ANPD e da Justiça Eleitoral nas Eleições de 2022

Com o intuito de prevenir que disparos em massa de propaganda eleitoral e de conteúdo falso e fraudulento fossem realizados, o TSE firmou diversos acordos com as principais plataformas digitais no Brasil. Esses acordos dão guarida ao Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral, instituído por meio da Portaria TSE nº 510/2021. O Programa possui a "finalidade de combater, de modo ininterrupto, a desinformação relacionada à Justiça Eleitoral e aos seus integrantes, ao sistema eletrônico de votação e ao processo eleitoral em suas diferentes fases"[45].

Além das plataformas digitais, o TSE também firmou um acordo de cooperação técnica com a ANPD, com o objetivo de "alinhar as diretrizes da LGPD às leis eleitorais, produzir conjuntamente materiais educativos e conciliar a proteção de dados pessoais ao cenário eleitoral"[46]. O acordo entre a ANPD e o TSE vem na seara da inserção digital maciça e o tratamento automatizado de informações pessoais dos eleitores. Ao formalizar essas intenções, destaca-se a necessidade do estabelecimento de controles necessários para evitar discriminações ilícitas ou abusivas.

---

[44] Art. 55-J da LGPD.

[45] Portaria nº 510/2022. Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2022/portaria-no-510-de-25-de-maio-de-2022. Acesso em: 23 de fevereiro de 2023.

[46] Acordo de Cooperação Técnica nº 4/2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/TSEANPDacordocooperacaotecnica.pdf. Acesso em: 23 de fevereiro de 2023.

No início do ano de 2022, onde foram disputadas as eleições gerais, a ANPD e o TSE publicaram o *Guia Orientativo - Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral*[47]. O Guia traz uma série de orientações práticas sobre a aplicação da LGPD nas eleições de 2022, além de explicar e esclarecer sobre os aspectos obrigatórios da lei no contexto eleitoral. O texto também faz uma série de recomendações e boas práticas a serem seguidas pelos candidatos, partidos políticos e coligações.

Entre os principais pontos mencionados pelo Guia, destaca-se a necessidade de observância das bases legais, o modo de se evitar desvios de finalidade no tratamento de dados pessoais, recomendações sobre responsabilização e prestação de contas, direitos dos titulares de dados e ações de prevenção e segurança.

Nas eleições de 2022 foi possível observar que o próprio TSE analisou com cautela a questão dos dados pessoais dos eleitores.

No Referendo na Representação nº 0600966-36.2022.6.00.0000, o TSE constatou que os dados pessoais estavam sendo tratados com finalidades distintas do que havia sido informado aos titulares:

> Como relatado, os usuários, na página inicial do sítio e com grande destaque, são convidados a fornecerem seus dados pessoais a pretexto de serem "voluntário no combate às fake news", mas, na verdade, estão fornecendo suas informações para uso de campanha eleitoral, **em evidente desvio de finalidade, com claríssima violação à boa-fé objetiva e com flagrante indução em erro** somente perceptível aos que se dispõem a clicar no discreto link de política de usuário, quando, para surpresa geral, são direcionados ao site de campanha de Luiz Inácio Lula da Silva, com a informação de que passaram a ser voluntários e de que forneceram suas informações para recebimento de material de campanha.[48]

[47] Guia Orientativo - Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf. Acesso em: 23 de fevereiro de 2023.

[48] BRASIL. Tribunal Superior Eleitoral. Referendo na Representação nº 0600966-36.2022.6.00.0000 - Brasília - DF. Acórdão de 27/09/2022. Relatora Min. Maria Claudia Bucchianeri. Publicado em Sessão de 27/09/2022. Disponível em: https://inter03.tse.jus.br/sjur-pesquisa/pesquisa/actionBRSSearchServers.do?tribunal=TSE&livre=%27LGPD%27. Acesso em: 23 de fevereiro de 2023.

Todo esse esforço conjunto contribui para elucidar como as ações de partidos políticos, candidatos e coligações podem ser tomadas com responsabilidade e transparência, de modo a respeitar a legislação de proteção de dados e estar em conformidade com o direito eleitoral.

Considerações Finais

Existem muitas interseções entre a proteção de dados pessoais e o direito eleitoral, interseções essas que tendem a aumentar com o crescimento do uso das plataformas digitais para a divulgação de propagandas eleitorais e para o contato com eleitores. Dessa forma, torna-se essencial o contato entre a Justiça Eleitoral e a ANPD para o desenvolvimento de estratégias para a regulação do uso dos dados pessoais na seara eleitoral, algo que já começou a ser feito por meio do acordo de cooperação técnica firmado entre a ANPD e o TSE e por meio da publicação do Guia Orientativo - Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral, que orientou diversas práticas nas eleições de 2022.

Algumas questões têm recebido maior atenção, como o envio de propaganda eleitoral via mensagens eletrônicas, algo já regulamentado pelo TSE, que chegou a prever a necessidade de que o titular dos dados pessoais se oponha ao tratamento de seus dados e consiga se descadastrar, e como a necessidade de observância das bases legais e dos direitos, não podendo estes serem tratados para finalidades distintas das informadas aos titulares.

No entanto, ainda existem muitas questões a serem enfrentadas com maior profundidade, como a utilização de dados pessoais sensíveis e as questões que podem vir a surgir a partir da disseminação de *fake news* e o uso de novas tecnologias, como a inteligência artificial.

Conclui-se, portanto, que há um início positivo na regulação do uso de dados pessoais no campo eleitoral, com uma colaboração importante entre a ANPD e a Justiça Eleitoral. No entanto, tal vínculo precisa ser mantido e fortalecido de forma que as autoridades estejam previamente preparadas para as questões que vão surgir nas próximas eleições e que nem os titulares dos dados pessoais nem as eleições sejam vulnerabilizadas.

Existem complexidades no uso de dados pessoais no âmbito eleitoral que não podem ser observadas unilateralmente, sob o risco de serem adotadas abordagens que vulnerem direitos dos titulares de dados pessoais, os eleitores. De tal forma, é extremamente necessário que a

parceria entre o TSE e a ANPD se estenda e que a estrutura eleitoral e de proteção de dados trabalhem em conjunto para as próximas eleições.

Referências bibliográficas

ARCHEGAS, João Victor. Relatório de Boas Práticas: *Proteção de Dados e Partidos Políticos no Brasil*. ITS Rio, 2021.

BATISTA JÚNIOR, Onofre Alves. *O poder de polícia fiscal*. Belo Horizonte: Mandamentos, 2001.

BRASIL. Tribunal Superior Eleitoral. Referendo na Representação nº 0600966-36.2022.6.00.0000 - Brasília - DF. Acórdão de 27/09/2022. Relatora Min. Maria Claudia Bucchianeri. Publicado em Sessão de 27/09/2022. Disponível em: https://inter03.tse.jus.br/sjur-pesquisa/pesquisa/actionBRSSearchServers.do?tribunal=TSE&livre=%27LGPD%27. Acesso em: 23 de fevereiro de 2023.

SCHERTEL MENDES, L.; MATTIUZZO, M. DISCRIMINAÇÃO ALGORÍTMICA: CONCEITO, FUNDAMENTO LEGAL E TIPOLOGIA. Direito Público, [S. l.], v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 29 maio. 2023.

COSTA, Rafael. *"As funções da Justiça Eleitoral"*. Revista Brasileira de Direito Eleitoral – RBDE | Belo Horizonte, ano 8, n. 15, p. 131-148, jul./dez. 2016; BARRETO, Álvaro. "A Justiça Eleitoral brasileira: modelo de governança eleitoral". Paraná Eleitoral, v. 4, n. 2, pp. 189-216.

FRAZÃO, Ana; DE CARVALHO, Ângelo Prata; MILANEZ, Giovanna. *Curso de proteção de dados pessoais:* fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022.

GOMES, José Jairo. *Direito Eleitoral*. 12ª ed. São Paulo: Atlas, 2016.

MENDES, L. S.; FONSECA, G. C. S. da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. REI - REVISTA ESTUDOS INSTITUCIONAIS, [S. l.], v. 6, n. 2, p. 507–533, 2020. DOI: 10.21783/rei.v6i2.521. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 29 maio. 2023.

MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. *Proteção de Dados nas Eleições*: democracia e privacidade. Grupo de Estudos em Proteção de Dados e Eleições, 2020.

TSE. Guia orientativo: *aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. Brasília, Tribunal Superior Eleitoral, 2021.

O ATO CONJUNTO Nº 4 E A APLICAÇÃO DA LGPD: A POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS NO ÂMBITO DO TRIBUNAL SUPERIOR DO TRABALHO E DO CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO

Rafaella Bacellar Marques[1]

Resumo: O presente artigo analisa como se estruturaram as regulamentações de adequação à LGPD no âmbito do Tribunal Superior do Trabalho (TST) e do Conselho Superior da Justiça do Trabalho (CSJT), a partir da instituição da política de Privacidade e Proteção de Dados (PPDP) estabelecida pelo Ato Conjunto nº 4. Com efeito, busca-se compreender como o tratamento de dados ocorre nos órgãos supramencionados que compõem a Justiça Trabalhista e o cumprimento da orientação dada pelo Conselho Nacional de Justiça (CNJ) por meio do Regulamento nº 73/2020, o qual norteia os órgãos do Judiciário quanto à adoção de medidas iniciais para adequação à Lei Geral de Proteção de Dados (LGPD).

Palavras-chave: Ato Conjunto n. 4; Política de Privacidade e Proteção de Dados Pessoais; LGDP; TST; CSJT

Abstract: *This article analyzes how the regulations to adapt to the LGPD were structured within the Superior Labor Court (TST) and the Superior Labor Justice Council (CSJT), from the institution of the Privacy and Data Protection Policy (PPDP), established by The Joint Act N. 4. The purpose is to understand how data processing takes place in the aforementioned bodies that constitute the Labor Justice System and how they comply with the guidance given by the National Council of Justice (CNJ) through Regulation 73/2020, which instructs judicial bodies on adopting initial measures to comply with the General Data Protection Law (LGPD).*

[1] Rafaella Bacellar Marques é Graduanda em Direito pela Universidade de Brasília (UnB). Membro do Observatório da LGPD da UnB e da Liga Acadêmica de Processo Civil da UnB, pesquisadora voluntária pelo CNPq.

Keywords**:** *Joint Act n. 4; Privacy and Personal Data Protection Policy; LGDP; TST; CSJT*

Introdução

O presente artigo analisará as regulamentações existentes no âmbito do direito do trabalho acerca da proteção de dados que deve ser realizada pelo Tribunal Superior do Trabalho (TST) e demais tribunais que atendem demandas trabalhistas[2], bem como intenta verificar a existência de normas que prevejam a responsabilização do Tribunal em eventuais hipóteses de vazamento de dados.

Em 2021, do total de processos ingressados no Poder Judiciários, 11% (onze por cento) pertenciam à Justiça do Trabalho, segundo o relatório *Justiça em Números* de 2022 do Conselho Nacional de Justiça (CNJ)[3], havendo inegável relevância no estudo acerca do modo como todos os dados dos trabalhadores e daqueles envolvidos na máquina judicial estão sendo tratados no que concerne aos processos eletrônicos que tramitam nas varas desta justiça especializada, porquanto, na maioria das vezes, há dados sensíveis envolvidos nos processos trabalhistas.

A privacidade e a proteção de dados pessoais têm ganhado relevância nos últimos anos. No ano de 2016 com o Regulamento Europeu, em 2018 com a Lei Geral de Proteção de Dados Pessoais (LGPD) e em 2022, a partir da promulgação da Emenda Constitucional nº 115, é possível observar o crescimento gradativo do reconhecimento do direito da proteção de dados pessoais até o momento de ápice com a inclusão deste direito no rol de garantias e direitos fundamentais do art. 5º da Constituição Federal (CF).

Tal direito possui dupla função: (i) formal, que consiste na regulação das situações jurídicas relativas a dados pessoais; e (ii) material, que concerne à proteção dos titulares[4]. A LGPD propiciou garantias em relação ao tratamento de dados pessoais, "a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do

[2] "A Justiça do Trabalho é um ramo do Poder Judiciário brasileiro composto pelo Tribunal Superior do Trabalho (TST), 24 Tribunais Regionais do Trabalho (TRTs) e Juízes do Trabalho, sendo que a supervisão administrativa, orçamentária, financeira e patrimonial de primeiro e segundo graus é exercida pelo Conselho Superior da Justiça do Trabalho (CSJT)." Disponível em: <https://ww2.trt2.jus.br/institucional/o-trt-2/estrutura-e-funcionamento/#:~:text=A%20Justi%C3%A7a%20do%20Trabalho%20%C3%A9,exercida%20pelo%20Conselho%20Superior%20da> Acesso em: 12 de jun. de 2023.

[3]Confira-se:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnj.jus.br/wp-content/uploads/2022/09/justica-em-numeros-2022-1.pdf. Acesso em: 11 de junho de 2023.

[4] CORDEIRO, A. Barreto Menezes. Dados pessoais, conceito, extensão e limites. *Book Revista de Direito Civil – 2* (2018). Indb. P. 297. 23.05.2018.

cidadão quanto para que o mercado e o setor público possam utilizar esses dados pessoais"[5]. Nessa perspectiva, a partir da promulgação da LGPD (Lei nº 13.709/2018), há uma efetiva preocupação quanto ao estabelecimento de limites não só para o tratamento de dados pessoais realizado pelo setor privado, como também pelo Poder Público.

A necessidade de adequação da Administração Pública é expressa no art. 23 da Lei 13.709/2018, no qual consta previsão de que o tratamento de dados pessoais realizado pela esfera pública deverá ser exercido "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".

Dessa forma, as pessoas jurídicas de direito público, ao tratarem dados pessoais, ainda que com fundamento legal para o atendimento do interesse público, devem se submeter a uma série de parâmetros e diretrizes dispostos na LGPD. Logo, "os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e Ministério Público"[6] devem seguir os princípios e deveres impostos pela 13.709/2018, com observância de regulamentação a ser realizada por legislação específica ou por meio de atos normativos infralegais.

Nesse sentido, a Autoridade Nacional de Proteção de Dados (ANPD) publicou o *Guia Orientativo para o Tratamento de Dados Pessoais pelo Poder Público*[7] em janeiro de 2022. Na ocasião, reafirmou-se a necessidade de submissão do tratamento de dados realizado pelo Poder Público aos princípios orientadores da LGPD, sobretudo aos seguintes: finalidade, adequação, necessidade, transparência e livre acesso.

Ante o contexto normativo supracitado, o Poder Judiciário, para além do dever de verificação do cumprimento dos deveres legais impostos àqueles que realizam o tratamento de dados, passa a ter uma necessidade de auto adequação legal, instituindo limites ao tratamento de dados. Neste artigo, interessa o tratamento e a proteção da privacidade e dos dados pessoais dos trabalhadores que possuem processos que tramitem perante o TST, bem como dos

[5] MENDES, Laura Schertel; DONEDA, Danilo. 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*, Brasília, v. 120/2018, p. 555-587, nov./dez. 2018a. p. 577

[6] Art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação))

[7] BRASIL. Autoridade Nacional De Proteção de Dados. *Guia Orientativo de Tratamento de Dados Pessoais Pelo Poder Público.* Brasília/DF. Janeiro de 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 18 de fevereiro de 2023.

Ministros, colaboradores, jurisdicionados e administrados constantes dos sistemas informáticos e das bases de dados do TST e do Conselho Superior da Justiça do Trabalho (CSJT).

Após a promulgação da LGPD, o CNJ[8] expediu a Regulamentação nº 73, em 20 de agosto de 2020, que recomendava aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e iniciais para adequação às disposições contidas na LGPD e a criação de "um padrão nacional de proteção de dados pessoais existentes nas suas bases". Foi com base na regulamentação elaborada pelo CNJ que o TST, em conjunto com o CSJT, iniciou a movimentação para instituir a Política de Privacidade e Proteção de Dados Pessoais, a partir do Ato Conjunto nº 4.

O tema de interesse deste artigo foi definido em virtude da ausência de pesquisas específicas relacionadas à regulamentação da adequação à LGPD no âmbito da Justiça Trabalhista, mais especificamente do Tribunal Superior. Neste sentido, dado que o TST foi um dos primeiros Tribunais a regulamentar uma Política de Privacidade e Proteção de Dados pessoais, a qualidade da adequação feita se tornou o objeto deste estudo.

Ante o exposto, almeja-se examinar o procedimento de adequação do TST e do CSJT à LGPD, em especial quanto ao que determina o Ato Conjunto nº 4, as demais regulamentações criadas e, ainda, o papel da Comissão instituída, de modo a traçar um panorama de como tem se dado a aplicação da LGPD nessas instituições.

1. Adequação à LGPD pelo TST e pelo CSJT

1.1. Recomendação nº 73 de 20 de agosto de 2020

O Ato Conjunto nº 4 foi produzido em atenção à Recomendação nº 73 do Conselho Nacional de Justiça, em 20 de agosto de 2020. Nesta ocasião, o CNJ descreveu a necessidade de criação de um padrão nacional de proteção de dados pessoais a todos os órgãos do Poder Judiciário, com exceção do Supremo Tribunal Federal. Para isso, determinou a elaboração de um plano de ação capaz de atender os seguintes tópicos: (i) organização e comunicação; (ii)

[8] A hierarquia judiciária vincula todos os magistrados aos Tribunais Superiores, STF e STJ, e todos os magistrados do trabalho ao TST, sendo essa a função jurisdicional típica. Enquanto a função administrativa atípica é exercida sobretudo pelo CNJ, por meio da regulamentação efetuada em nível nacional, ficando a cargo deste ente o estabelecimento de regras e orientações aplicáveis ao Judiciário como um todo (LIMA, Adrianne; ALCASSA, Flávia; PAPPERT, Milena. LGPD no Direito do Trabalho. Editora Saraiva, 2022. E-book. ISBN 9786553621954. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553621954/. Acesso em: 12 jun. 2023).

direitos do titular; (iii) gestão de consentimento; (iv) retenção de dados e cópia de segurança; (v) contratos; e (vi) plano de respostas a incidentes de segurança com dados pessoais.

Ademais, como requisito para a criação do padrão nacional desejado, entendeu o CNJ ser necessário a disponibilização nos sítios eletrônicos, de forma ostensiva aos usuários, de informações básicas acerca da LGPD e um formulário para exercício de direitos dos titulares de dados pessoais. Além disso, o CNJ recomendou a elaboração e a disponibilização de forma acessível de uma Política de Privacidade para navegação no *website* de instituições públicas.

Se solicitou também o registro de tratamento de dados pessoais, contendoinformações sobre finalidade de tratamento, base legal, descrição dos titulares, categorias de dados e de destinatários, transferência internacional, prazo de conservação, medidas de segurança e política de segurança de informação.

Em atendimento à Recomendação nº 73, o TST iniciou um trabalho de adequação à LGPD. É necessário destacar que a atuação do CNJ se tornou essencial nos últimos anos no que se refere ao tratamento de dados pessoais pelo Poder Público, na medida em que se enseja a uniformização de adequação dos Tribunais à LGPD, sobretudo em face do seu caráter geral pela sua própria natureza de lei federal. Portanto, a partir das normativas do Conselho e da própria atuação da ANPD, se torna possível o tratamento de dados pessoais adequado no âmbito da Justiça do Trabalho.

1.2. Ato Conjunto nº 4 de 12 de março de 2021

O Ato Conjunto nº 4, datado de 12 de março de 2021, é a norma que regulamenta e institui a Política de Privacidade e Proteção de Dados Pessoais no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho.

Não obstante, antes mesmo da Recomendação dada pelo CNJ e da instituição da política de privacidade e proteção de dados pessoais estabelecidos pelo Ato Conjunto nº 4, já havia sido criado um Comitê, que será abordado em momento posterior deste artigo, para tratar dos assuntos referentes à proteção de dados.

Como premissa inicial a ser definida pelo Ato Conjunto nº 4, surge a necessidade de se definir um controlador, um dos tipos de agente de tratamento de dados pessoais. Vale dizer que atribuição da função de controlador e encarregado foi realizada inclusive em momento anterior, ainda em novembro de 2020, por força do Ato Conjunto nº 46/TST.CSJT.GP.

A figura do controlador veio disciplinada na LGPD, em seu art. 5º, VI, que o define como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", sendo seu elemento distintivo o poder de decisão. O controlador "é responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento"[9] (2021, p. 7), de acordo com a definição dada pela ANPD no *Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, documento de maio de 2021, em esclarecimento ao art. 5º, VI, da LGPD.

Dessa forma, segundo o Ato Conjunto nº 46, ratificado posteriormente pelo Ato Conjunto nº 4 (art. 1º, parágrafo único), são controladores o Tribunal Superior do Trabalho e o Conselho Superior da Justiça do Trabalho, representados por seu Ministro Presidente, em nome da União, tomando as decisões "referentes ao tratamento de dados pessoais sob sua responsabilidade" (art. 1º, Ato Conjunto nº 46).

Aos controladores cabe a expedição de normas administrativas e deliberação de pedidos em relação à proteção de dados pessoais. O Ato Conjunto nº 46 estabelece que os recursos administrativos das decisões do controlador devem ser encaminhados a Órgão Especial, entretanto, ainda inexiste regulamentação de qual seria a composição do referido órgão.

Portanto, os direitos dos titulares dos dados são exercidos em face do controlador, figura que detém a maior responsabilidade em relação ao tratamento dos dados. Ao controlador cabe ainda, segundo a ANPD, "fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, receber requerimento de oposição a tratamento" (2021, p.7).

A importância de se definir de pronto a figura do controlador no âmbito da política de proteção de dados de um Tribunal consiste na conceituação e distinção entre "os conceitos de controlador e operador são funcionais: eles visam alocar a responsabilidade de acordo com os papéis reais das partes"[10]. Assim, a verificação daquele a quem cabe a maior responsabilidade em caso de insegurança dos dados será mais eficiente a partir da definição dessas funções,

[9] BRASIL. Autoridade Nacional De Proteção de Dados. *Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e Encarregado.* Brasília/DF. Maio de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em 18 de fevereiro de 2023.

[10] *Guidelines 07/2020 on the concepts of controller and processor in the GDPR.* set. 2020, p. 9. Disponível em https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf. Acesso: 22 fev 2023.

orientação dada pelo *European Data Protection Board*: EDPB. Dessarte, a responsabilidade quanto ao tratamento de dados cabe ao TST e ao CSJT precipuamente.

Sobre a responsabilidade diferenciada do Poder Público no tratamento de dados pessoais, afirma Wimmer:

> Se a motivação e a legitimidade do governo ao tratar dados pessoais devem necessariamente ser compreendidas como distintas daquela dos agentes privados, sua responsabilidade é, também, maior, dado que eventual mau uso de dados pelo Estado produz impactos abrangentes não apenas sobre a esfera de direitos individuais, mas sobre a sociedade como um todo[11].

Nesse contexto, a determinação do Controlador por parte do Ato Conjunto nº 4 torna-se essencial sobretudo quando analisado o impacto que pode resultar do tratamento de dados realizados no âmbito do TST.

Destaca-se que o TST e o CSJT são entes despersonalizados, pois constituem meros órgãos públicos dentro da Administração direta da União, pertencentes ao Poder Judiciário. A LGPD faz referência em seu art. 23 ao tratamento de dados pelo Poder Público a ser realizado pelas pessoas referidas na Lei de Acesso à Informação (LAI), que trata em seu art. 1º, I, justamente de "órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;"[12].

Isto posto, a LGPD optou por atribuir as obrigações típicas de controlador a unidades administrativas despersonalizadas que integram a União enquanto pessoa jurídica de direito público, possibilidade garantidal por força da desconcentração administrativa, fenômeno que caracteriza a distribuição interna de competências.[13] O que significa que em caso de eventual situação de insegurança de dados pessoais, os responsáveis não serão propriamente estes

---

[11] WIMMER, Miriam. O Regime jurídico do tratamento de dados pessoais pelo poder público. *In:* BIONI, Bruno. *Tratado de Proteção de Dados Pessoais*. Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023. P. 282.

[12] BRASIL. Lei n 12.527 de 18 de novembro de 2011. *Diário Oficial da União*, Brasília, 18 nov. 2011a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/ L12527.htm>. Acesso em: 10 jan. 2023

[13] BRASIL. Autoridade Nacional De Proteção de Dados. *Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e Encarregado*. Brasília/DF. Maio de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em 18 de fevereiro de 2023.

órgãos, mas a União, a entidade que detém a personalidade jurídica, tanto o é, que há referência expressa no art. 1º do Ato Conjunto nº 4 à atuação do controlador ocorrer em nome da União.

Cabe pontuar que as pessoas naturais que trabalham no Tribunal Superior do Trabalho, ainda que no exercício do tratamento de dados, não são controladoras, pois são profissionais subordinados à pessoa jurídica. Dessa forma, é a pessoa jurídica de direito público que assume a responsabilidade por todos os atos praticados pelos seus agentes em face dos titulares dos dados, no caso em tela, levado à última consequência, a União.

O art. 25 do Ato Conjunto nº 4 estabelece o dever de cooperação tanto do TST quanto do CSTJ quando forem promovidas fiscalizações por terceiros legitimamente interessados, desde que respeitadas as seguintes condições: (i) informação acerca da fiscalização em tempo hábil; (ii) motivação objetiva e razoável; (iii) não criação de risco aos dados não abrangidos pela fiscalização; (iv) ausência de impacto, dano ou interrupção das atividades do TST ou CSTJ. A não cooperação, por outro lado, pode implicar responsabilidade civil, penal e administrativa, conforme se desprende do parágrafo único do art. 25.

Uma vez definida a figura do Controlador, a LGPD em seu art. 23, III, apresenta a necessidade de que seja indicado um encarregado. Este, por força do art. 5º, VIII, da LGPD, é pessoa indicada pelo controlador e operador para atuar como canal de comunicação, entre o controlador, titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O ato conjunto nº 46 estabelece que o encarregado deverá ser Juiz Auxiliar indicado pelo Presidente do TST e do CSJT (art. 2º, do Ato conjunto nº 46)[14].

O papel do encarregado de dados ou *Data Protection Officer* (DPO) – denominação que deriva do Regulamento Europeu – como se depreende do disposto na LGPD, é ser o canal de ligação entre os que realizam o tratamento de dados e aqueles que se submetem a este. Carvalho, Mattiuzzo e Ponce explicam que os canais de comunicação que se estabelecem a partir da figura do encarregado são essenciais, pois ensejam dois pontos positivos: "de um lado, eles possibilitam resolução de dúvidas de funcionários e colaboradores, bem como a orientação e

[14] BRASIL. Tribunal Superior do Trabalho; CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO (Brasil). Ato Conjunto n. 46/TST.CSJT.GP, de 4 de novembro de 2020. *Diário Eletrônico da Justiça do Trabalho:* caderno administrativo [do] Conselho Superior da Justiça do Trabalho, Brasília, DF, n. 3094, p. 1, 5 nov. 2020.

solução de questões relacionadas a situações limítrofes de aplicação da LGPD; de outro, viabilizam a comunicação de possíveis ilícitos."[15]

Outra figura prevista pela LGPD, em seu art. 5º, VII, é o operador, a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do Controlador". O operador também consta no Ato Conjunto nº 04, em seu art. 18, que apenas replica a definição dada pela Lei Geral de Proteção de Dados.

O operador (*data processor*), assim como o controlador, é um agente de tratamento. Enquanto este tem o poder de decisão, aquele realiza o tratamento de dados pessoais com base nas instruções recebidas pelo controlador[16].

Ademais, a fim de estabelecer regras de segurança acerca da proteção de dados, foi criado um Comitê– ComLGPD ou CLGPD – por força do ato nº 190 de 29 de maio de 2020[17]. Antes, a segurança de informações do TST ficava a cargo do Comitê Gestor de Segurança da Informação, por força do Ato nº 225/GP, que foi revogado com o ato nº 190/TST.GP.

O comitê chamado de CLGPD foi criado com a finalidade de estabelecer as regras de segurança, de boas práticas e de governança e o procedimento para a proteção de dados pessoais no âmbito da Corte.

O CLGPD é composto por: (i) encarregado pelo tratamento de dados pessoais; (ii) juiz auxiliar da Presidência do CSJT; (iii) represente da Secretaria-geral da Presidência do TST; (iv) um representante de cada uma dessas unidades – vice-presidência do TST; corregedoria-geral da justiça do trabalho; diretoria-geral da secreatia do TST, secretaria-geral judiciária do TST; Secretaria-Geral do CSJT; (v) secretário de gestão de pessoas do TST; (vi) secretário de Administração do TST; (vii) secretário de tecnologia da Informação e Comunicação do TST; (viii) ouvidor auxiliar; (ix) coordenador de integridade e gestão de riscos; (x) secretário de

[15] CARVALHO, Vinicius Marques de. MATTIUZZO, Marcela. PONCE, Paula Pedigoni. Boas práticas e governanças na LGPD. *In:* BIONI, Bruno. *Tratado de Proteção de Dados Pessoais*. Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023. P. 381.

[16] LEONARDI, Marcel. Transferência Internacional de Dados Pessoais. *In:* BIONI, Bruno. *Tratado de Proteção de Dados Pessoais*. Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023. P. 301.

[17] BRASIL. Tribunal Superior do Trabalho. Ato n. 190/TST.GP, de 29 de maio de 2020. *Boletim Interno [do] Tribunal Superior do Trabalho*, Brasília, DF, n. 22, p. 7-8, 5 jun. 2020.

tecnologia da Informação e Comunicação do CSJT; e (xi) coordenador de segurança cibernética.

O art. 5º do Ato Conjunto nº 383 de 29 de junho de 2022 (ato que alterou o Ato TST.GP nº 190, de 29 de maio de 2020) define que a CLGPD deverá se reunir uma vez por trimestre de forma ordinária, podendo ser convocada pelo coordenador de forma extraordinária. A coordenação é exercida pelo encarregado pelo tratamento de dados pessoais.

O Comitê reporta-se ao Controlador e tem como funções: (i) propor políticas de cumprimento das normas legais de proteção de dados e elaborar projeto para adequação dos processos do TST à LGPD; (ii) responder consultas formuladas pelos controladores de outros órgãos da Justiça do Trabalho; (iii) assessorar a alta administração do Tribunal em questões relevantes; entre outras atribuições. Tanto o Ato Conjunto nº 4, quanto o Ato Conjunto nº 46, estabelecem que o Comitê deverá oferecer parecer técnico nos pedidos administrativos relacionados à proteção de dados.

Por força do art. 24 do Ato Conjunto nº 4, cabe à ComLGPD a definição dos procedimentos e mecanismos de fiscalização. Ademais, o art. 16, caput e parágrafo único, estabelece que o encarregado, responsável por receber as reclamações dos titulares dos dados, dentre outras funções, previsto pelo art. 41 da LGPD, contará com o apoio da ComLGPD, sobretudo a partir do oferecimento de pareceres técnicos por parte da Comissão nos pedidos de titulares dos dados.

Avançando na análise do Ato Conjunto nº 4, o art. 6º, parágrafo único, faz previsão de que o Regimento Interno do Tribunal e do Conselho definirão quais as funções e atividades que fixarão as finalidades e os critérios para a proteção de dados pessoais. Além disso, vale pontuar que o Ato nº 4 reproduz os princípios previstos pelo art. 6º da LGPD, a exemplo da finalidade, adequação, necessidade, não discriminação, entre outros.

Como ponto de destaque, o art. 7º prevê a possibilidade de tratamento de dados pelo TST e pelo CSJT quando no exercício estrito de suas competências legais e constitucionais, independentemente do consentimento dos titulares. O exercício de atividades meramente administrativas não vinculadas ao exercício de tais competências, no entanto, exige-se obrigatoriamente o consentimento prévio dos titulares dos dados.

A possibilidade de tratamento de dados sem consentimento dos titulares ainda não foi regulamentada por nenhum ato posterior, de modo que ainda não estão claras as hipóteses

concretas em que a ausência do consentimento seria legítima, tampouco quais seriam as competências legais e constitucionais do TST e do CSJT e a sua distinção em relação às atividades meramente administrativas.

Bernardes e Alvim fazem uma crítica em relação aos conceitos de ampla abertura semântica constantes da redação da LGPD, a exemplo do art. 26, que faz referência a "finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas". Dessa forma, para esses autores, apesar de a LGPD tratar do tema do compartilhamento de dados pelo Poder Público, há uma deficiência na lei no que concerne à carência de detalhamento necessário acerca de conceitos jurídicos indeterminados[18]. Portanto, a densificação deveria advir da atividade regulatória, entretanto, quando se analisa o Ato Conjunto nº 04, quanto a este ponto, não houve o detalhamento esperado, persistindo ainda sem definição.

1.3. As demais instruções normativas e a inspiração no ato Conjunto nº04

Uma vez analisado o Ato Conjunto nº 04, interessa fazer breve comparativo com ato normativo feito para regulamentar o tratamento de dados pessoais realizados pelas instâncias ordinárias do Poder Judiciário submetidas hierarquicamente ao TST, a fim de demonstrar o espelho entre tais instruções normativas e o Ato Conjunto nº 04.

Nesse sentido, a resolução CSJT nº 309 de 24 de setembro de 2021 traça as diretrizes e orientações para a formulação de Políticas de Privacidade e Proteção de Dados Pessoais (PPDPs) no âmbito dos Tribunais Regionais do Trabalho. Sobre essa normativa, vale o destaque para a possibilidade de os portais do TRTs se utilizarem de arquivos (*cookies*) para registrar e gravar, no computador do usuário, as preferências e navegações realizadas, mediante a obtenção de consentimento do titular.

Segundo a resolução elaborada pelo CSJT, os regimentos internos de cada Tribunal, assim como as demais normas do Poder Judiciário, devem definir funções e atividades que constituem a finalidade do tratamento de dados pessoais. No que se refere à tomada de decisão

[18] BERNARDES, Rachel Rezende. ALVIM, Rafael da Silva. A Autodeterminação informativa e o uso secundário de dados pessoais pela Administração Pública: Quais sãos os limites? In: LIMA, Ana Paula Canto de. ROSAS, Eduarda Chacon. *LGPD 2022: debates e temas relevantes* – Recife, PE: Império Jurídico, 2022.

sobre o tratamento de dados pessoais, a figura do controlador, no âmbito dos Tribunais Regionais do Trabalho, deve ser realizada pelos Desembargadores Presidentes.

Os chamados Operadores, a exemplo dos fornecedores de produtos e de serviços aos Tribunais, ao tratarem dos dados pessoais a eles confinados pelos contratantes, devem aderir às PPDPs, e cumprirem com uma série de deveres, a exemplo de: (i) assinar contrato com cláusulas específicas sobre proteção de dados; (ii) apresentar evidências da aplicação de medidas de segurança de dados; (iii) manutenção dos registros de tratamento de dados, com condição de rastreabilidade; entre outros (art. 14 da Resolução CSJT nº 309). Os operadores podem ser "pessoas naturais ou jurídicas, de direito público ou privado, que realizarem operações de tratamento de dados em nome do respectivo controlador" (art. 18 da Resolução CSJT nº 309).

Cumpre destacar que o mesmo artigo que consta no ato conjunto nº 4, acerca da possibilidade de tratamento independentemente do consentimento dos titulares, desde que em exercício das competências legais e constitucionais, foi replicado na regulamentação pertinente aos Tribunais Regionais do Trabalho (art. 7, da Resolução CSJT n º 309).

É possível observar certa simetria na regulamentação a nível de Tribunal Regional do Trabalho, em relação àquela própria feita pelo TST, como, por exemplo, na função do encarregado, que será exercida por magistrados indicados pelo Presidente do Tribunal. Em caso de reclamação à Ouvidoria, esse deverá apresentar parecer com uma proposta de solução ao Presidente (controlador).

2. Lacuna na regulamentação da Política de Proteção de Dados

A regulamentação feita pelo TST além de pioneira, mostrou-se adequada em sua dimensão mais geral. Uma vez estabelecidas as regulamentações acerca das funções de cada comitê e de cada ente, no entanto, era necessário a devida previsão das consequências da eventual falha na Política de Privacidade e Proteção de Dados Pessoais. Dessa forma, trata-se sim de uma regulamentação adequada, contudo insuficiente.

A priori, uma vez que no processo eletrônico, todas as informações pessoais do empregado, bem como a descrição do evento que o levou a ajuizar ou ser parte em uma demanda com os respectivos documentos referentes ao ocorrido, constam nos autos do processo, dificilmente, estar-se-á diante de uma situação que não trate de dados sensíveis. Desse modo, para além da regulamentação dos dados pessoais coletados nos sites dos tribunais e dos dados

de seus servidores, era necessário realizar a regulamentação dos dados que constam nos processos eletrônicos que tramitam naquele determinado tribunal.

Nesse sentido vale citar a Regulamentação nº 363 do CNJ[19], na qual disciplina-se, em seu art. 1º, XII, as regras para o armazenamento e registro de dados, orientando os tribunais a determinar prazo de conservação, confira-se:

> Art. 1º Estabelecer medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) a serem adotadas pelos tribunais do país (primeira e segunda instâncias e Cortes Superiores), à exceção do Supremo Tribunal Federal, para facilitar o processo de implementação no âmbito do sistema judicial, consistentes em:
> XII – elaborar e manter os registros de tratamentos de dados pessoais contendo informações sobre: a) finalidade do tratamento; b) base legal; c) descrição dos titulares; d) categorias de dados; e) categorias de destinatários; f) eventual transferência internacional; e g) prazo de conservação e medidas de segurança adotadas, nos termos do art. 37 da LGPD;

A ausência de regulação específica sobre o tempo que os dados constarão no acervo do tribunal, no caso da regulamentação realizada pelo TST e CSJT, bem como o modo como serão registrados, se sempre em autos eletrônicos ou depois físicos, torna complexa a situação de fiscalizar se os dados estão sendo tratados de forma adequada, e ainda mais grave, saber quais as consequências de um possível vazamento de dados.

Segundo o Código de Boas Práticas da Organização Internacional do Trabalho, *Protection of workers' personal data*[20], os dados do trabalhador só devem constar no banco de dados do empregador por tempo suficiente e justificável pelos específicos propósitos aos quais foram coletados. Na medida em que são os mesmos dados a serem tratados no processo eletrônico, a dúvida que persiste é se a mesma recomendação se aplicaria ou não ao Poder Público.

Ademais, parece existir controvérsia quando se analisa a necessidade de confrontar o adequado tratamento de dados pessoais em face dos princípios da Administração Pública, como

---

[19]Confira-se: chrome-<extension://efaidnbmnnnibpcajpcglclefindmkaj/https://atos.cnj.jus.br/files/original181204202101196007 20f42c02e.pdf> Acesso em 12 jun. 2023.

[20] *Protection of workers' personal data*. An ILO code of practice Geneva, International Labour Office, 1997, 04.02.2 ISBN 92-2-110329-3. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 08 de jun. de 2023.P. 16.

a transparência e eventual direito ao esquecimento, estabelecendo qual regulamentação deve prevalecer. Problemas que deverão ser enfrentados em breve quando se fala em tratamento de dados pessoais realizado pelo Poder Judiciário.

Da mesma forma, a Regulamentação nº 363 do CNJ cita a necessidade de elaboração de planos de respostas a incidentes, o que não parece ter sido feito na regulamentação implementada pelo TST e pelo CSJT:

> Art. 1º (...)
>
> XI – implementar 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, nos termos do art. 46 e seguintes da LGPD, por meio: a) da elaboração de política de segurança da informação que contenha plano de resposta a incidentes (art. 48 da LGPD), bem como a previsão de adoção de mecanismos de segurança desde a concepção de novos produtos ou serviços (art. 46, § 1o);

Em parecer técnico CTGOV nº 01/20[21], o Conselho Superior da Justiça do Trabalho fez referência ao dever de o controlador comunicar, em prazo razoável, à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, descrito no art. 48 da LGPD. Contudo, trata-se de recomendação ou orientação dada em estudo realizado acerca da LGPD, sem qualquer caráter normativo ou determinação quanto aos conceitos mais abstratos da lei geral, a exemplo da fixação de prazo razoável.

Em artigo escrito por Marcos Sêmola, publicado no site do SERPRO[22], citado no parecer do CSJT, propõe-se a estruturação e implementação da LGPD em quatro fases, sendo a terceira delas *definir*. Nesta ocasião, deveria ser implementado o monitoramento e tratamento de crises, ao se definir uma estrutura para resposta a incidentes que envolvam a quebra da proteção de dados, o que incluiria relatórios legais exigidos pela LGPD. Tal medida foi definida no parecer do CSJT (p. 25) como uma diretriz a ser adotada com o objetivo de nortear ações que visem ao efetivo cumprimento da LGPD, o que indica uma certa ciência e uma provável implementação das regulamentações quanto aos incidentes de segurança.

---

[21] Confira-se: <file:///C:/Users/User%20Samsung/Downloads/Parecer%20T%C3%A9cnico%20CTGOV%2001-2020.pdf> Acesso em 13 de jun. de 2023.

[22] Disponível em: <https://www.serpro.gov.br/lgpd/noticias/escape-armadilhas-lgpd-lei-geral-de-protecao-de-dados-pessoais> Acesso em 13 de jun. 2023.

Desse modo, o Ato Conjunto nº 4 foi capaz de indicar os responsáveis pelo tratamento de dados, ao definir as figuras como a do controlador, operador e encarregado, bem como a criação do comitê enseja a atualização constante das políticas de fiscalização. Contudo, restam dúvidas quanto às consequências na realidade fática, a garantia da segurança ao titular do dado, ou até mesmo uma eventual reparação por dano causado. Por fim, é preciso considerar que milhares de processos tramitam justiça eletrônica, tornando difícil verificar, caso a caso, que cada dado está recebendo o tratamento adequado.

Há grandes lacunas na política desenvolvida, que tendem a deixar sobretudo o empregado numa posição de vulnerabilidade, vez que o empregador, na maioria das vezes, já é um controlador de dados no contrato de trabalho, passando à posição de titular de dados no momento do processo judicial. As instabilidades dos sites de Tribunais Superiores, a exemplo do site do Superior Tribunal de Justiça (STJ), e a invasão por *hackers*, despertam o alerta para que os tribunais tenham o cuidado de fazer a previsão das situações de crise, bem como do protocolo a ser seguido no caso de eventual vazamento, o que ainda não foi feito no caso da política desenvolvida pelo TST.

Considerações Finais

Tendo em vista o exposto, os desafios lançados com a promulgação da Lei Geral de Proteção de Dados, no ano de 2018, perpassam pela dificuldade de conciliação entre "os princípios tradicionalmente aplicáveis à Administração e aqueles contidos na própria LGPD"[23]. Por conseguinte, é imprescindível a regulamentação específica de como deve ocorrer a aplicação prática dos princípios e orientações no dia a dia de cada órgão da Administração.

No âmbito do TST, a regulamentação iniciada por volta de 2020, e que persiste a partir da edição de normas até o momento presente, tem-se mostrado adequada, pois cumpre com os requisitos estabelecidos pelo CNJ e os demais órgãos reguladores. É possível afirmar que, no mínimo, no âmbito, do Tribunal Superior do Trabalho foi alcançado o padrão mínimo de qualidade exigido pela Recomendação nº 73 de 2020.

[23] WIMMER, Miriam. O Regime jurídico do tratamento de dados pessoais pelo poder público. *In:* BIONI, Bruno. *Tratado de Proteção de Dados Pessoais*. Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023.

Com as funções devidamente estabelecidas, as práticas autorizadas descritas e ainda o procedimento de responsabilização em caso de eventual situação de insegurança dos dados pessoais, o Ato Conjunto nº 4 cumpre a sua função como norma regulamentadora, cuja aplicação prática ainda se delineará no futuro.

Há, porém, condições que devem ser cumpridas para que o Ato Conjunto nº torne-se uma norma efetivamente exequível. Ainda assim, dada a sua qualidade, o Ato Conjunto serviu como parâmetro para regulamentar ainda as instâncias que se subordinam ao Tribunal Superior do Trabalho, havendo verdadeiro espelhamento neste ato para a criação da resolução CSJT nº 309.

Contudo, apesar de ser uma norma adequada, na medida em que cumpre com o mínimo exigido pelo CNJ na Recomendação nº 73, ainda parece restar uma lacuna quanto à aplicação prática da LGPD, no que concerne às condições reais de proteção do titular do dado, sobretudo em caso de vazamento de dados contidos nos processos eletrônicos que tramitam no TST.

Por fim, evidencia-se a necessidade de adequação de todos os órgãos do Poder Público aos princípios definidos pela LGPD, como feito no âmbito do TST e do CSJT, sobretudo porque a privacidade não precisa se opor ao interesse público, mas sim atuar em complementaridade para com ele, trata-se do fundamento principal que justificou a regulamentação feita pela LGPD: a privacidade é uma proteção constitucional que interessa tanto ao indivíduo quanto à sociedade, que evita prejuízos decorrentes de atividades essenciais à vida em comunidade, como a atuação do Estado.

Referências bibliográficas

BERNARDES, Rachel Rezende. ALVIM, Rafael da Silva. A Autodeterminação informativa e o uso secundário de dados pessoais pela Administração Pública: Quais sãos os limites? *In*: LIMA, Ana Paula Canto de. ROSAS, Eduarda Chacon. *LGPD 2022: debates e temas relevantes* – Recife, PE: Império Jurídico, 2022.

BRASIL. Autoridade Nacional De Proteção de Dados. *Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e Encarregado.* Brasília/DF. Maio de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em 18 de fev. de 2023.

BRASIL. Autoridade Nacional De Proteção de Dados. *Guia Orientativo de Tratamento de Dados Pessoais Pelo Poder Público*. Brasília/DF. Janeiro de 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-

publico-anpd-versao-final.pdf. Acesso em 18 de fev. de 2023.

BRASIL. Conselho Nacional de Justiça. Relatório analítico Justiça em números de 2022. Brasília: CNJ, 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnj.jus.br/wp-content/uploads/2022/09/justica-em-numeros-2022-1.pdf. Acesso em: 11 de jun. de 2023.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA (Brasil). Recomendação nº 73, de 20 de agosto de 2020. *Diário da Justiça [do] Conselho Nacional de Justiça*, Brasília, DF, n. 272, p. 9-11, 21 ago. 2020.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA (Brasil) Resolução nº 363, de 12 de janeiro de 2021. *Diário da Justiça [do] Conselho Nacional de Justiça*, Brasília, DF. Disponível em: chrome-<extension://efaidnbmnnnibpcajpcglclefindmkaj/https://atos.cnj.jus.br/files/original1812042021011960072 0f42c02e.pdf> Acesso em 12 jun. 2023.

BRASIL, CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO (Brasil) Parecer Técnico CTGOV nº 01/2020. Disponível em: <file:///C:/Users/User%20Samsung/Downloads/Parecer%20T%C3%A9cnico%20CTGOV%2001-2020.pdf> Acesso em 13 de jun. de 2023.

BRASIL. Lei Geral de Proteção de Dados (2018). Lei nº13.709, de 14 de agosto de 2018. *Diário Oficial da União*, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 11 de jan. de 2023.

BRASIL. Lei nº 12.527 de 18 de novembro de 2011. *Diário Oficial da União*, Brasília, 18 nov. 2011a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/ L12527.htm>. Acesso em: 10 jan. 2023

BRASIL. Tribunal Superior do Trabalho; CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO (Brasil). Ato Conjunto n. 4/TST.CSJT.GP, de 12 de março de 2021. *Boletim Interno [do] Tribunal Superior do Trabalho*, Brasília, DF, n. 11, p. 2-7, 19 mar. 2021. Disponível em: https://hdl.handle.net/20.500.12178/182852, acesso em 17 de fev. de 2023.

BRASIL. Tribunal Superior do Trabalho; CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO (Brasil). Ato Conjunto nº 46/TST.CSJT.GP, de 4 de novembro de 2020. *Diário Eletrônico da Justiça do Trabalho: caderno administrativo [do] Conselho Superior da Justiça do Trabalho*, Brasília, DF, n. 3094, p. 1, 5 nov. 2020.

BRASIL. CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. Resolução nº 309/CSJT, de 24 de setembro de 2021. *Diário Eletrônico da Justiça do Trabalho: caderno administrativo [do] Conselho Superior da Justiça do Trabalho*, Brasília, DF, n. 3325, p. 40-43, 7 out. 2021.

BRASIL. Tribunal Superior do Trabalho. Ato nº 383/TST.GP, de 29 de junho de 2022. *Boletim Interno [do] Tribunal Superior do Trabalho*, Brasília, DF, n. 26, p. 9-11, 1º jul. 2022.

BRASIL. Tribunal Superior do Trabalho. Ato nº 190/TST.GP, de 29 de maio de 2020. *Boletim Interno [do] Tribunal Superior do Trabalho*, Brasília, DF, n. 22, p. 7-8, 5 jun. 2020.

BRASIL. Tribunal Superior do Trabalho; CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO (Brasil). Ato Conjunto nº 74/TST.CSJT.GP, de 24 de outubro de 2022. *Diário Eletrônico da Justiça do Trabalho: caderno administrativo [do] Conselho Superior da Justiça do Trabalho*, Brasília, DF, n. 3586, p. 1, 25 out. 2022.

CARVALHO, Vinicius Marques de. MATTIUZZO, Marcela. PONCE, Paula Pedigoni. Boas práticas e governanças na LGPD. *In:* BIONI, Bruno. *Tratado de*

Proteção de Dados Pessoais. Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023.

CORDEIRO, A. Barreto Menezes. Dados pessoais, conceito, extensão e limites. *Book Revista de Direito Civil* – 2 (2018). Indb. P. 297. 23.05.2018.

Guidelines 07/2020 on the concepts of controller and processor in the GDPR. set. 2020, p. 9. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf. Acesso: 22 de fev. de 2023.

LEONARDI, Marcel. Transferência Internacional de Dados Pessoais. *In:* BIONI, Bruno**.** *Tratado de Proteção de Dados Pessoais***.** Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023. P. 301.

LIMA, Adrianne; ALCASSA, Flávia; PAPPERT, Milena. LGPD no Direito do Trabalho. Editora Saraiva, 2022. E-book. ISBN 9786553621954. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553621954/. Acesso em: 12 jun. 2023.

MENDES, Laura Schertel; DONEDA, Danilo. 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*, Brasília, v. 120/2018, p. 555-587, nov./dez. 2018a. p. 577

Protection of workers' personal data. An ILO code of practice Geneva, International Labour Office, 1997, 04.02.2 ISBN 92-2-110329-3. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 08 de jun. de 2023.P. 16.

SÃO PAULO. TRT2. Estrutura e funcionamento. Disponível em: <https://ww2.trt2.jus.br/institucional/o-trt-2/estrutura-e-funcionamento/#:~:text=A%20Justi%C3%A7a%20do%20Trabalho%20%C3%A9,exercida%20pelo%20Conselho%20Superior%20da>. Acesso em: 12 de jun. de 2023.

WIMMER, Miriam. O Regime jurídico do tratamento de dados pessoais pelo poder público. *In:* BIONI, Bruno. *Tratado de Proteção de Dados Pessoais***.** Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 01 mar. 2023

SE VOCÊ NÃO PAGA PELO PRODUTO, O PRODUTO É VOCÊ: UMA ANÁLISE DO ACORDO DE COOPERAÇÃO TÉCNICA ENTRE CADE E ANPD

Sofia de Medeiros Vergara[1]

Resumo: O presente artigo discorre sobre os principais aspectos do Acordo de Cooperação Técnica nº 5/2021, firmado entre o Conselho Administrativo de Defesa Econômica (CADE) e a Autoridade Nacional de Proteção de Dados (ANPD). Para tanto, aborda brevemente o contexto maior em que se insere, isto é, das discussões acerca da intersecção entre o direito concorrencial e a proteção de dados para, em seguida, apresentar as principais medidas e características do acordo. Após, será evidenciada a experiência do Reino Unido em cooperação, a fim de estabelecer um parâmetro para analisar a pertinência do acordo brasileiro face à prática internacional.

Palavras-chave: Direito Concorrencial; Proteção de Dados; Acordo de Cooperação Técnica

Abstract: *This paper seeks to discuss the main aspects of the Technical Cooperation Agreement No. 5/2021, signed between the Administrative Council for Economic Defense (CADE) and the National Data Protection Authority (ANPD). To this end, the larger context in which the agreement operates will be briefly presented, that is, the discussions about the intersection between competition law and data protection, to then move on to the main measures and characteristics of the agreement. Afterward, some international experiences in cooperation will be highlighted, in order to establish an analysis parameter for the agreement.*

Keyworsds**:** *Competition Law; Data Protection; Technical Cooperation Agreement*

[1]Graduada em Direito pela Universidade de Brasília (UnB). Advogada em Massonetto, Horta e Bachur Advogados. Assistente da Coordenação de Pesquisa no Observatório de LGPD. Gerente da Competição WIA-CADE da Rede *Woman Inside Antitrust* (WIA). Membro da *Woman in Inside Trade Starters* (WIT *Starters*).

Introdução

Em 02 de junho de 2021, o Diretor-Presidente da Autoridade Nacional de Proteção de Dados (ANPD)[2] e Presidente do Conselho Administrativo de Defesa Econômica (CADE)[3] anunciaram a assinatura do Acordo de Cooperação Técnica nº 5/2021 ("Acordo"), destinado ao "aperfeiçoamento das ações voltadas à defesa, fomento e disseminação da concorrência no âmbito dos serviços de proteção de dados" (MJSP; CADE; ANPD, 2021, p. 1).

O referido acordo insere-se em um amplo contexto de discussões que têm ganhado cada vez mais destaque tanto na academia quanto no âmbito das autoridades concorrenciais ao redor do mundo: as repercussões práticas da inegável intersecção entre o direito concorrencial e a proteção de dados, especialmente no que tange os mercados digitais e as chamadas *big techs*. Tal intersecção ocorre na medida que o tratamento de dados gera efeitos não apenas na esfera individual dos titulares de dados, mas também pode ser utilizado como um instrumento de distorção do mercado, garantindo vantagens econômicas e facilitando a consolidação de posições dominantes para aqueles que as detêm.

Veja-se que, não obstante os benefícios e inovações trazidas com o desenvolvimento dos mercados digitais, o crescimento sem precedente das grandes empresas que atuam nesse nicho, principalmente como resultado da exploração massiva de dados pessoais, traz consigo preocupações não apenas em relação à competitividade do mercado em que estão inseridas, mas também quanto aos efeitos danosos que o tratamento de dados pode causar para a privacidade e segurança dos usuários.

Nesse sentido, o presente artigo busca entender como o Acordo de Cooperação Técnica nº 5/2021, celebrado entre as autoridades de proteção de dados e concorrencial, apresenta-se como uma solução para criação de um diálogo contínuo entre os dois campos do direito. Para tanto, o artigo será dividido em três frentes: (i) primeiramente, serão apresentadas de forma breve discussões acerca da intersecção entre o direito concorrencial e a proteção de dados, a fim de estabelecer o contexto em que o acordo se insere; (ii) em seguida, serão introduzidos os principais elementos do artigo, junto de breves considerações sobre o enfoque dado ao tema pelas autoridades envolvidas; (iii) após, será trazida a experiência britânica, pontuando-se o que é feito de forma similar ou diferente do acordo brasileiro. Ao final, virão as conclusões.

[2] Na época, o Sr. Waldemar Gonçalves Ortunho Júnior
[3] Na época, o Sr. Alexandre Barreto de Souza

1. A intersecção entre o Direito Concorrencial e a Proteção de Dados

Com o avanço das tecnologias disruptivas, diversos campos do direito voltaram sua atenção para os impactos da era digital. Para além da profunda alteração das relações sociais e econômicas, a revolução tecnológica também foi responsável pela criação de novos mercados, muitos destes dominados por empresas de tamanho sem precedentes, bem como se iniciaram importantes discussões e reflexões acerca da coleta e exploração de dados e as respectivas repercussões destas para a privacidade e a segurança dos usuários online.

Embora tradicionalmente a regulação antitruste tenha se afastado da regulação de privacidade, a proporção da ascensão das grandes plataformas digitais na economia tem borrado a linha que antes dividia as regulações (ECONOMIDES; LIANOS, 2020). É justamente no âmbito da exploração econômica dos dados que se poderia aventar uma interação entre competição e proteção de dados pessoais, especialmente quando se considera uma característica muito comum desses mercados: o produto ou prestação serviços à preço-zero. Isso porque, embora o usuário receba o benefício imediato do serviço de preço zero, em muitos casos desconhece os custos de curto ou longo prazo do compartilhamento de suas informações, uma vez que, de modo geral, não sabe como e por quem os dados serão usados (OCDE, 2015).

No mesmo sentido, consoante apontou a *Bundeskartellamt* (2017), a autoridade concorrencial alemã, em um caso de possível abuso de posição dominante envolvendo a empresa Facebook, a proteção de dados, a proteção ao consumidor e a proteção da competição se ligam na medida em que os dados são um fator crucial para a dominância econômica de uma empresa. Embora os chamados dadopólios (*data-opolies*) não possam exercer poder por meio de um injustificado aumento de preços, como ocorre com nos monopólios tradicionais, existem diversos danos potenciais que podem decorrer de um eventual abuso de posição dominante, dentre eles: diminuição da privacidade; redução da inovação e da dinâmica disruptiva dos mercados, uma vez que haveria menos incentivos para inovar num mercado dominado; além de preocupações políticas, morais e sociais (STUCKE, 2018).

Considerando então que o big data apresenta-se como uma nova fronteira entre os mercados tradicionais e os mercados digitais, estes últimos marcados pela disrupção e uma alta capacidade de concentração, faz-se necessário um olhar cauteloso para compreender qual seria o papel do direito concorrencial na promoção de um ambiente competitivo e inovador

(BAGNOLI, 2016), no qual não existe apenas uma preocupação com preço, mas também com a privacidade e a qualidade. Estes serviriam como verdadeiros parâmetros para aferição de eventuais falhas no mercado, o que por sua vez impacta diretamente o direito dos usuários.

Contudo, o diálogo entre os dois campos não é algo simples, uma vez que partem de objetos e pressupostos distintos. Isto é, enquanto o direito concorrencial foca nos direitos transindividuais, como a defesa da ordem econômica e da competição, a proteção de dados busca salvaguardar direitos subjetivos, como a privacidade e a segurança dos usuários. Neste sentido, resumem os autores Nicholas Economides e Ioannis Lianos (2020, p. 2):

> Os regulamentos de proteção de dados e privacidade geralmente adotam uma perspectiva de direitos fundamentais, vendo a privacidade como uma questão de direitos. [...] A lei da concorrência geralmente adota uma abordagem de falha de mercado e está preocupada se o consumidor ou o seu bem-estar (*consumer welfare*), podem sofrer com proteção de dados reduzida em um mercado disfuncional para aquisição de dados pessoais, em tal extensão que poderia sofrer com preços mais altos ou qualidade inferior.

Ainda que partam de pressupostos opostos, a defesa dos direitos dos usuários e a manutenção de um ambiente competitivo estão diretamente ligados e beneficiam-se de esforços mútuos e concomitantes nas duas áreas, a fim de atingir patamares razoáveis de proteção e competitividade.

Veja que a liberdade de escolha e o controle de seus dados por parte dos usuários são elementos fundamentais para a proteção de dados e a concorrência. Por exemplo, quando se está diante de termos "*take it or leave it*", especialmente em mercados que tendem ao monopólio como os mercados digitais, a escolha e o controle do usuário são severamente limitados. O fomento à concorrência, nesse caso, seria capaz de permitir uma maior proteção ao titular na medida em que os fornecedores passariam a competir pela aderência de usuários, fortalecendo as proteções de privacidade e segurança (CMA; ICO, 2021).

Desta maneira, são criadas sinergias entre a proteção de dados e o direito concorrencial que, quando aplicadas de forma razoável e adequada, podem enfrentar potenciais efeitos prejudiciais das condutas das empresas que atuam no âmbito da economia digital, movida a dados, sempre buscando a cautela com o objetivo de não criar empecilhos para a inovação.

Diversas são as formas pelas quais a interseção entre os dois campos do direito estudados pode ser estabelecida. Um exemplo é o Acordo de Cooperação Técnica nº 5/2021, assinado entre as autoridades brasileiras de proteção de dados e de concorrência, que dispõe de uma série de medidas e obrigações comuns com o propósito de garantir um espaço para o diálogo e o compartilhamento de informações e expertises entre as duas autoridades - é o que será melhor explorado no tópico a seguir.

2. O Acordo de Cooperação Técnica nº 5/2021

No mesmo sentido das sinergias entre o direito concorrencial e a proteção de dados discutidas no tópico *supra*, a assinatura do Acordo de Cooperação Técnica nº 5/2021 parte do pressuposto de que a cooperação e a atuação articulada entre as autoridades responsáveis – o CADE e a ANPD – proporciona maior efetividade para o alcance da proteção de dados, bem como permite enfrentar dificuldades relativas à instrução de processos dessa natureza, considerando a celeridade e engenhosidade com que as novas tecnologias se desenvolvem e os riscos que podem ensejar a livre concorrência (MJSP; CADE; ANPD, 2021).

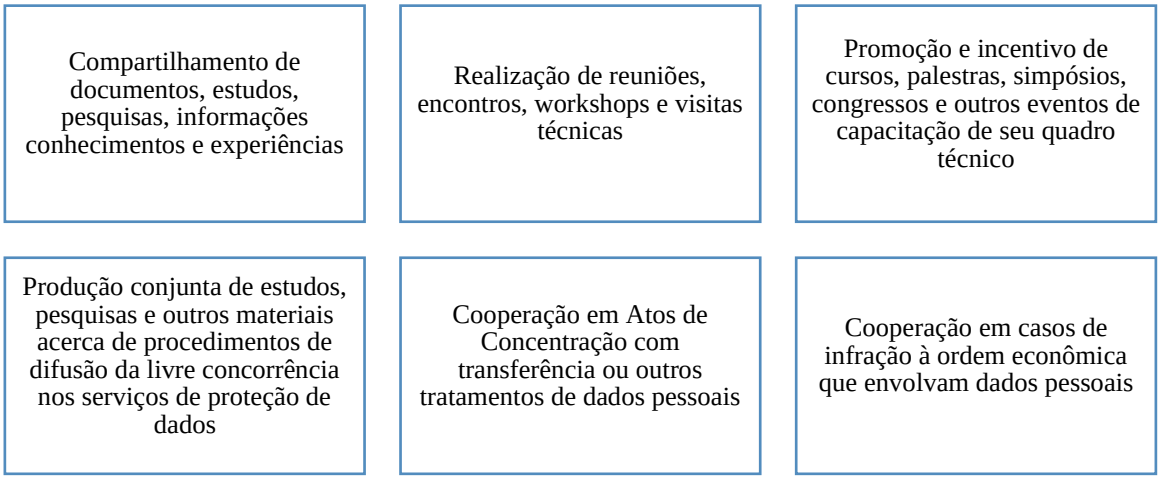
Nas reflexões apresentadas no tópico dois do Acordo ("Diagnóstico, abrangência e justificativa"), as autoridades destacam que o direito da concorrência foi uma das áreas jurídicas mais afetadas no contexto da economia movida a dados, uma vez que seu tratamento excessivo pode ensejar violações de direitos como privacidade e autodeterminação informativa por parte dos agentes econômicos que utilizam dos dados como instrumento para auferir vantagens econômicas e se sobrepor à concorrência. Tendo em vista a possibilidade de conversão dos dados pessoais em ativo econômico, em especial um ativo que pode ser usado como forma de distorcer a competição no respectivo mercado, as autoridades concluíram pela necessidade de compartilhar esforços para proteger concomitantemente o direito dos titulares e a livre concorrência (MJSP; CADE; ANPD, 2021).

Assim, conforme consta na Cláusula Primeira, o acordo tem como finalidade a instituição de cooperação técnica entre CADE e ANPD a fim de "viabilizar ações a serem adotadas pelas partes de forma conjunta e coordenada, quando da ocorrência de situações que interseccionam ambas as esferas de competência" (MJSP; CADE; ANPD, 2021, p. 2). Em outras palavras, o acordo busca, via compartilhamento de informações e expertises, estabelecer

um diálogo contínuo e unir forças que se propõem a combater atividades lesivas à concorrência e aos direitos dos titulares de dados pessoais.

Com efeito, a Cláusula Terceira do Acordo estipula algumas obrigações comuns ao CADE e à ANPD que não envolvem a transferência ou repasse de recursos financeiros entre as autoridades. Em síntese, são previstas as seguintes ações:

Figura 01 – Obrigações comuns estipuladas no Acordo de Cooperação Técnica entre o CADE e a ANPD



Fonte: Elaborado pela autora (2023)

É possível afirmar, do estudo do quadro acima, que as ações comuns previstas possuem dois enfoques principais: (i) um mais técnico, pautado na capacitação de seus funcionários e na elaboração e compartilhamento de pesquisas, estudos, informações, etc., indicando a importância da produção de subsídios técnicos para os julgamentos das autoridades, uma vez que a jurisprudência sobre o tema ainda é escassa e não parece haver um consenso sobre a melhor forma de lidar com as questões que decorrem dos mercados digitais; (ii) um mais prático, focado nos processos recebidos pelo CADE, tanto em um controle *ex ante*, no caso de atos de concentração, como no controle *ex post*, nos casos de infração à ordem econômica que envolvam dados pessoais, permitindo ampliar o escopo de análise dos processos submetidos ao crivo da autoridade.

Além das obrigações comuns, o Acordo estabelece competências, responsabilidades e obrigações específicas a cada uma das partes. São elas, resumida e comparativamente:

Figura 02 – Obrigações, competências e responsabilidades específicas estipuladas no Acordo de Cooperação Técnica entre o CADE e a ANPD

São competências, responsabilidades e obrigações:	
Do CADE:	Da ANPD
Compartilhar com a ANPD documentos, estudos, pesquisas, informações, conhecimentos e experiências em sua área de atuação, salvo em caso de prejuízo à análise ou investigação.	Compartilhar com o CADE documentos, estudos, pesquisas, informações, conhecimentos e experiências em sua área de atuação, salvo em caso de prejuízo à análise ou investigação.
Comunicar imediatamente à ANPD a respeito da instauração de processo administrativo em desfavor de agentes econômicos que atuem em setores regulados pela ANPD e que porventura possam tipificar conduta infracional a ser apurada pela ANPD, salvo em caso de prejuízo à análise ou investigação.	Comunicar imediatamente à ANPD a respeito da instauração de processo administrativo em desfavor de agentes econômicos que atuem em setores regulados pela ANPD e que porventura possam tipificar conduta infracional a ser apurada pela ANPD, salvo em caso de prejuízo à análise ou investigação.
Solicitar, quando julgar oportuno, análise e manifestação da ANPD acerca dos processos submetidos ao CADE e que digam respeito à proteção de dados pessoais.	Solicitar, quando julgar oportuno, análise e manifestação do CADE acerca dos processos submetidos ao controle da ANPD e que digam respeito às atividades lesivas à ordem econômica e ao fomento e à disseminação da cultura da livre concorrência nos serviços de proteção de dados.
Franquear à ANPD o acesso às informações constantes em seus bancos de dados, observadas restrições de sigilo e segurança.	Franquear ao CADE o acesso às informações constantes em seus bancos de dados, observadas restrições de sigilo e segurança.
Observar as restrições relativas à segurança da informação e ao sigilo estabelecidas pela	Observar as restrições relativas à segurança da informação e ao sigilo estabelecidas pelo

ANPD no acesso às informações constantes em seus bancos de dados.	CADE no acesso às informações constantes em seus bancos de dados.
Convidar a ANPD para reuniões, encontros, workshops, visitas técnicas, cursos, entre outros eventos organizados pelo CADE que envolvam a capacitação, treinamento, aperfeiçoamento ou reciclagem dos seus quadros técnicos, como participante ou palestrante.	Convidar o CADE para reuniões, encontros, workshops, visitas técnicas, cursos, entre outros eventos organizados pelo CADE que envolvam a capacitação, treinamento, aperfeiçoamento ou reciclagem dos seus quadros técnicos, como participante ou palestrante.
Informar à ANPD a respeito de reuniões, encontros, workshops, visitas técnicas, cursos, dentre outros eventos organizados pelo CADE que possam contribuir na capacitação, treinamento, aperfeiçoamento ou reciclagem dos quadros técnicos da ANPD no que concerne o combate de atividades lesivas à ordem econômica e o fomento e a disseminação da cultura da livre concorrência no campo da proteção de dados pessoais.	Informar ao CADE a respeito de reuniões, encontros, workshops, visitas técnicas, cursos, dentre outros eventos organizados pela ANPD que possam contribuir na capacitação, treinamento, aperfeiçoamento ou reciclagem dos quadros técnicos do CADE no que concerne o combate de atividades lesivas à ordem econômica e o fomento e a disseminação da cultura da livre concorrência no campo da proteção de dados pessoais.
Informar a ANPD qualquer fato, ato, negócio ou situação de que tomar conhecimento em virtude de sua atuação e que possa eventualmente caracterizar um indício de infração às normas de proteção de dados pessoais, em especial, as concernentes à livre concorrência e à ordem econômica.	Informar ao CADE qualquer fato, ato, negócio ou situação de que tomar conhecimento em virtude de sua atuação e que possa eventualmente caracterizar um indício de infração às normas que regem a livre concorrência e a ordem econômica, em especial, as concernentes a dados pessoais.
Relatar à ANPD eventual descumprimento de suas decisões ou dos termos de compromisso com ela firmados, que digam respeito à livre concorrência e à ordem econômica, que envolvam dados pessoais.	Relatar ao CADE eventual descumprimento de suas decisões ou dos termos de compromisso com ela firmados, que digam respeito à proteção de dados pessoais

Informar à ANPD o recebimento de propostas de termo de ajuste de conduta que versem acerca de dados pessoais, em especial as concernentes à livre concorrência e à ordem econômica, que envolvam dados pessoais	Informar ao CADE o recebimento de propostas de termo de ajuste de conduta que versem acerca de dados pessoais, em especial as concernentes à livre concorrência e à ordem econômica, que envolvam dados pessoais
Realizar, promover e incentivar palestras, conferências e outros eventos de capacitação, treinamento, aperfeiçoamento ou reciclagem de pessoal relacionados com a regulação de setores econômicos envolvidos ou com a promoção e defesa da livre concorrência nos mercados correspondentes, que envolvam dados pessoais.	Realizar, promover e incentivar palestras, conferências e outros eventos de capacitação, treinamento, aperfeiçoamento ou reciclagem de pessoal relacionados com a regulação de setores econômicos envolvidos ou com a promoção e defesa da livre concorrência nos mercados correspondentes, que envolvam dados pessoais
Realizar estudos, em parceria com a ANPD, sobre a definição de mercado relevante em casos que envolvam a questão da transferência de dados pessoais.	
Realizar estudos, em parceria com a ANPD, sobre a portabilidade de dados como ferramenta de defesa da concorrência.	
Realizar estudos, em parceria com a ANPD, sobre infrações à ordem econômica relacionadas à dados pessoais.	

Fonte: Elaborado pela autora (2023)

Verifica-se que, de modo geral, foram estipuladas obrigações contínuas e genéricas de compartilhamento de informações, promoção de eventos de capacitação e realização de estudos. Para além das obrigações mais gerais, foram expressamente delimitadas obrigações para elaboração de estudos específicos, sobre: (i) definição de mercado relevante em casos que envolvam a questão da transferência de dados pessoais; (ii) a portabilidade de dados como

ferramenta de defesa da concorrência; e (iii) infrações à ordem econômica relacionadas a dados pessoais.

3. Experiências internacionais de cooperação

Como visto, ainda que existam diferenças no escopo da proteção de dados e o direito concorrencial, o campo de interseção entre os dois direitos permite o estabelecimento de áreas de cooperação e sinergia. Por esta razão, diversas jurisdições, além do Brasil, iniciaram um processo de formalização de parcerias entre as autoridades responsáveis pela proteção de dados e defesa da ordem econômica.

A fim de contextualizar as discussões travadas no âmbito internacional, bem como criar um parâmetro comparativo para o Acordo de Cooperação Técnica nº 5/2021, esta seção apresentará brevemente algumas experiências de cooperação no Reino Unido.

3.1. Reino Unido

Em maio de 2021, a *Competition & Markets Authority* (CMA) – autoridade antitruste – e a *Information Commissioner's Office* (ICO) – autoridade de proteção de dados –, ambas do Reino Unido, publicaram uma declaração conjunta, na qual reconhecem a importância de alinhar as abordagens regulatórias com o fito de assegurar um ecossistema digital em que os usuários têm poder de escolha genuíno sobre o serviço ou produto que utilizem e um entendimento claro sobre como seus dados são utilizados pela plataforma (CMA; ICO, 2021).

Na verdade, antes mesmo da publicação da declaração, as duas autoridades já haviam formalizado um canal de cooperação. Diferente do que ocorreu no Brasil, a cooperação no Reino Unido se deu de forma mais institucional, a partir da criação de um fórum, o *Digital Regulation Cooperation Forum* (DRCF) em 2020, com o objetivo de apoiar a ação coordenada e coerente para regulação digital (CMA; ICO, 2021). Atualmente, além da CMA e do ICO, o fórum também é composto pelo *Office of Communications* (Ofcom) e a *Financial Conduct Authority* (FCA).

Dando início aos trabalhos, o DRCF publicou um plano de trabalho anual, no qual estabeleceu o formato em que se daria a cooperação entre os membros participantes. Para tanto, o fórum identificou três medidas principais para permitir a cooperação entre os reguladores

digitais: (i) apoiar o apropriado compartilhamento de informações; (ii) incorporar coerência e cooperação no quadro estatutário dos serviços digitais; (iii) garantir transparência e *accountability* (DRFC, 2021).

Desde então, diversos estudos foram publicados no âmbito do fórum; memorandos de entendimento bilaterais e multilaterais entre as entidades participantes foram firmados e atualizados; e as investigações passaram a contar com a cooperação e o compartilhamento de informações entre as autoridades.

Com efeito, o próprio CADE pontuou, em material de *benchmarking* internacional, as relações construídas entre as instituições de proteção de dados e concorrência do Reino Unido, ressaltando as principais medidas tomadas por elas, a saber (i) o desenvolvimento de novo regime regulatório pela CMA como resposta ao poder de mercado de gigantes da tecnologia; (ii) a criação, no âmbito da CMA, da unidade de mercados digitais, visando a defender a concorrência com o aumento de poder dos consumidores sobre seus dados pessoais; (iii) a cooperação em áreas de importância mútua para a CMA e o ICO; (iv) a publicação de estudos sobre proteção de dados com inter-relação com defesa da concorrência (CADE, 2021).

Comparando a experiência do Reino Unido e a do Brasil, principalmente em relação às ações listadas acima, verifica-se que, de modo geral, as medidas estipuladas no Acordo de Cooperação Técnica nº 5/2021 parecem seguir a mesma linha daquelas observadas na jurisdição britânica, isto é, obrigações gerais sobre o compartilhamento de informações e a realização de estudos.

Diferem, porém, em relação ao amadurecimento do tema, apesar de o Acordo de Cooperação Técnica nº 5/2021 e a declaração conjunta da CMA e ICO terem sido publicados no mesmo ano. Não obstante, as discussões parecem ter avançado mais no Reino Unido, principalmente considerando que a autoridade concorrencial britânica já vem enfrentando o tema através do julgamento de casos práticos há mais tempo que a brasileira. Tal fato permite às autoridades britânicas chegarem a conclusões mais precisas frente aos desafios e propor medidas mais concretas para o seu enfrentamento.

Veja-se que, para além de prever a realização de estudos gerais, a CMA propôs a elaboração de um novo regime regulatório que prevê, entre outros: (i) a criação de códigos de conduta, para aumentar a transparência, permitir a aplicação de sanções e evitar práticas de exploração ou exclusão; (ii) impor ao Google a abertura de dados, para que os concorrentes

possam aprimorar seus algoritmos e criar uma efetiva competição do mercado, observando a privacidade dos usuários; (iii) aumento da interoperabilidade do Facebook com outras mídias sociais, garantindo o consentimento do usuário; (iv) permitir e facilitar a escolha do usuário (*fairness-by-design*); (v) separar plataformas, quando necessário para a competição (CMA, 2020; GOV.UK, 2020).

Fica claro, portanto, que a cooperação no âmbito nacional parte de um objetivo mais inicial, diga-se criar bases teóricas para apenas depois aventar em propostas concretas acerca da necessidade ou não de alteração da política concorrencial e do regime regulatório aplicável às plataformas digitais.

Considerações Finais

Ao longo deste artigo, foram debatidas algumas das principais questões que envolvem mercados digitais, mais especificamente aquelas que decorrem da utilização de dados pessoais como um ativo econômico no modelo de negócios das empresas. É nesse contexto que se pode aventar uma interação entre proteção de dados e defesa econômica.

Como visto, embora nem sempre os objetivos dos dois campos estejam em convergência, diversos benefícios podem derivar de um alinhamento de políticas e abordagens regulatórias. Um exemplo de alinhamento é justamente o Acordo de Cooperação Técnica nº 5/2021, cuja análise foi objeto deste trabalho. Verificou-se que a iniciativa do CADE e da ANPD busca responder a uma dificuldade enfrentada pelo Direito Concorrencial na regulação dos mercados digitais, por meio do estabelecimento de um canal de diálogo contínuo entre as duas autoridades.

Embora as medidas do Acordo estejam alinhadas com a prática internacional, como se viu no Reino Unido, ele ainda carece de um plano de ação mais prático e objetivo que efetivamente implemente as medidas estipuladas. Por exemplo, a ausência de estipulação de prazos estruturados para a elaboração e a apresentação dos estudos sobre mercado relevante, infrações à ordem econômica e outros mencionados no Acordo pode ser aventada como uma das razões pelas quais estes ainda não foram publicados pelas autoridades.

No mesmo sentido, ainda que o acordo frise a importância do compartilhamento de informações e atuação conjunta em defesa da ordem econômica e da proteção de dados, poucos foram os casos em que essa parceria efetivamente ocorreu. Um dos poucos casos que podem

ser citados é o do WhatsApp, no qual foi emitida nota conjunta do CADE, ANPD, Ministério Público Federal (MPF) e Secretaria Nacional do Consumidor (Senacon) para adiar a alteração das políticas de privacidade do aplicativo de mensagens (BRASIL, 2021).

Cabe apontar também a importância da educação dos titulares a respeito do valor de seus dados para que eventuais medidas tomadas pelas autoridades possam efetivamente gerar resultados positivos, afinal, não adianta falar de consentimento ou privacidade, se seu titular não tem consciência do valor de seus próprios dados ou das maneiras que estes são utilizados.

A lógica de mercado das empresas da era digital tem como principal insumo o seu consumidor, passando uma imagem de produto a preço-zero que não se alinha à prática das empresas. Nesse contexto – e retomando o título deste artigo – é importante que o usuário entenda que se ele não paga monetariamente pelo produto, esse "pagamento" muitas vezes virá em forma do tratamento e exploração de seus dados, com consequências como a perda de privacidade e segurança.

O debate sobre educação midiática, inclusive, já entrou em pauta no Congresso Nacional por meio do PL 2630/2020 que visa instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Sem entrar no mérito desse controverso Projeto de Lei, cumpre evidenciar a introdução do fomento à educação para o uso seguro, consciente e responsável da internet como um dos objetivos da regulação das plataformas digitais. Embora a educação dos usuários tenha sido ressaltada em projetos posteriores, ela não foi abordada no acordo de cooperação entre CADE e ANPD, cabendo uma ênfase maior do tema.

Conclui-se então que, embora o arcabouço legal aplicável esteja alinhado, e apesar de o Acordo de Cooperação Técnica nº 5/2021 dispor de medidas necessárias para articular a cooperação entre os dois órgãos, falta ao arranjo um desenho prático de como essas medidas serão implementadas, saindo do contexto abstrato e genérico idealizado no Acordo para um objetivo e concreto que se materialize na elaboração de um plano de ação e na estipulação de prazos.

Referências bibliográficas

BAGNOLI, Vicente. *The Big Data Relevant Market*. In. DI PORTO, FABIANA. Concorrenza e Mercato: Antitrust, Regulation, Consumer Welfare, Intelectual Property. Vol. 23. Giuffrè Editore, S.p.A. Milano – 2016

BRASIL. Cade, MPF, ANPD e Senacon recomendam que Whatsapp adie entrada em

vigor da nova política de privacidade. Autoridade Nacional de Dados, Notícias. Publicado em 07.05.2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade. Acesso em 06.03.2022

BUNDESKARTELLAMT. *Preliminary Assessment in Facebook Proceeding*: Facebook's Collection and Use of Data from Third-Party Sources Is Abusive. Press Release. Publicado em 19.12.2017. Disponível em: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html. Acesso em 05.03.2023

COMPETITION & MARKETS AUTHORITY (CMA); INFORMATION COMMISSIONER'S OFFICE (ICO). Competition and data protection in digital markets: a joint statement between the CMA and the ICO. Publicado em 19 mai. 2021. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf. Acesso em 05.03.2023

CMA, Competition Markets and Authority. *A new pro-competition regime for digital markets*. Publicado em julho de 2020. Disponível em < https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice_-- .pdf>. Acesso em 26 mai. 2023

CADE, Conselho Administrativo de Defesa Econômica. *Documento de Trabalho nº 002/2021*. Benchmarking internacional sobre as instituições de defesa da concorrência e proteção de dados. Departamento de Estudos Econômicos (DEE), Jacqueline Salmen Raffoul. Publicado em junho de 2021.

DRFC, Digital Regulation Cooperation Forum. *Embedding coherence and cooperation in the fabric of digital regulators*: A summary of ideas to address barriers to cooperation and measures to strengthen digital regulatory cooperation in future. Publicado em 04.05.2021. Disponível em: https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-embedding-coherence-and-cooperation-in-the-fabric-of-digital-regulators. Acesso em 06.03.2023

ECONOMIDES, Nicholas; LIANOS, Ioannis. *Data networks and plataforms*: What effects on economic development. Antitruste and restrictions on privacy in the digital economy. Conference for Antitrust and developing and emerging economies. Concurrences n°2, 2020.

GOV.UK. *New regime needed to take on tech giants*. Publicado em jul. 2020. Disponível em < https://www.gov.uk/government/news/new-regime-needed-to-take-on-tech-giants>. Acesso em 26 mai. 2023.

MJSP, Ministério da Justiça e Segurança Pública; CADE, Conselho Administrativo de Defesa Econômica; ANPD, Autoridade Nacional de Proteção de Dados. *Acordo de Cooperação Técnica nº 5/2021* - Acordo de Cooperação Técnica entre Conselho de Defesa.

Econômica e a Autoridade Nacional de Proteção de Dados, para o aperfeiçoamento das ações voltadas à defesa, fomento e disseminação da concorrência no âmbito dos serviços de proteção de dados. Publicado em 02.06.2021. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf. Acesso em 04.03.2023.

OCDE, Organização para a Cooperação e Desenvolvimento Econômico. *Data-Driven Innovation: Big Data for Growth and Well-Being*. OCDE, Publishing, Paris. Publicado em 2015. Disponível em:

http://dx.doi.org/10.1787/9789264229358-en. Acesso em 05.03.2023

STUCKE, Maurice E. *Should We Be Concerned About Data-Opolies?* Publicado em 2018. p. 285-286. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144045. Acesso em 05.03.2023.

COMO AS MEDIDAS DE PROTEÇÃO DA COMISSÃO DE VALORES MOBILIÁRIOS FORAM IMPACTADAS PELA PORTARIA CVM/PTE/Nº 188

Luís Fernando Oliveira de Souza Costa[1]

Resumo: O presente artigo faz um estudo comparativo entre o parecer elaborado pelo Tribunal de Contas da União (TCU) no ano de 2021, que apontou a necessidade de melhorias dentro da Comissão de Valores Mobiliários (CVM) no tocante a proteção de dados dos usuários, e a Portaria CVM/PTE/N° 188, que versa sobre as competências gerais relativas à proteção de dados pessoais na Comissão de Valores Mobiliários – CVM. O estudo adotou o método explorativo bibliográfico e métodos comparativos. Além de utilizar-se de artigos, monografias e de textos legais para atingir suas conclusões, também fez o cotejo entre as falhas apontadas pelo parecer do TCU e a Portaria da CVM para verificar se as questões aventadas pelo primeiro foram tratadas pelo segundo. Ainda, avaliou se essas medidas foram efetivas.

Palavras-chave: CVM; TCU; Proteção de Dados; LGPD.

***Abstract**: This article does a comparative study between the opinion prepared by Union Court of Auditors (TCU) in 2021, which pointed out the need for improvements within the Securities and Exchange Commission (CVM) regarding the protection of the data subjects, and the impact that the CVM ordinance CVM/PTE/N°188 had in improving that question. The study used exploratory bibliographic and comparative methods. addition to using articles, thesis and legal texts to reach its conclusions, it also made a comparison between the flaws pointed out by the opinion of TCU and the CVM ordinance, in order to verify whether the issues raised by the first were addressed by the second. Furthermore, it also verified whether these measures were effective.*

***Keywords**: CVM; TCU; Data Protection; LGPD.*

[1] Pesquisador do Observatório

Introdução

A presente pesquisa visa a averiguar se a Portaria da CVM/PTE/N° 118, sobre a proteção de dados no meio da CVM, foi capaz de propiciar melhorias no seu âmbito de atuação dentro da Comissão de Valores Mobiliários (CVM). De modo a investigar isso, o presente estudo realizou uma comparação entre o parecer do Tribunal de Contas da União (TCU), que enquadrou a CVM no nível de adequação intermediário, e as previsões da Portaria citada.

O estudo do TCU utilizou o mecanismo de pesquisa Control Self-Assessment (CSA). Através dele, os gestores receberam um questionário e o responderam com base no nível de adequação que eles julgavam da sua organização no momento. A pesquisa identificou três pontos que poderiam propiciar um aumento no nível de proteção dos dados dos usuários dos serviços da CVM. A referida Portaria foi publicada em seguida e reestruturou a organização interna da CVM no que tange a proteção de dados. Desse modo, faz-se pertinente verificar se as normas ali editadas constituem mecanismos aptos a satisfazer esses gargalos apontados no parecer.

Para além disso, a presente pesquisa também terá como pontos de referência artigos, monografias e o próprio texto da Lei Geral de Proteção de Dados (LGPD, 13.709/2018). Isso se dá, especialmente, para explicar e explicitar os conceitos que nortearam o parecer do TCU, de modo a demonstrar a relevância das perguntas realizadas no questionário e o porquê de a CVM buscar sanar a questão de maneira célere.

A relevância do estudo também reside no fato de a Comissão ser capaz de aplicar sanções às entidades/empresas que estão submetidas as suas regulações. Além de ela servir de espelho para entidades públicas e para organizações privadas, tornando especialmente relevante o processo de adequação da CVM.

Por fim, o fato dos desafios por ela apresentados no processo de adequação corresponderem ao de diversas outras organizações realça a importância das questões que serão abordadas. Nessa senda, o estudo auxilia a identificar a efetividade ou não das práticas aventadas pela CVM.

1. CVM e a Portaria nº 188

A Comissão de Valores Mobiliários é uma entidade autárquica em regime especial vinculada ao Ministério da Fazenda. Foi fundada no ano de 1976 pela Lei n° 6385/76 e sua missão, conforme descrito no site do Governo Federal, é:

> Desenvolver, regular e fiscalizar o Mercado de Valores Mobiliários, como instrumento de captação de recursos para as empresas, protegendo o interesse dos investidores e assegurando ampla divulgação das informações sobre os emissores e seus valores mobiliários. (BRASIL, 2014)

Percebe-se da leitura que a informação cumpre um papel central na realização da missão da CVM, sendo, inclusive, listada de forma explícita. Para além disso, também se verifica que tal autarquia tem, enquanto um de seus valores, a "atuação pautada na proteção do investidor, na exigência de ampla divulgação de informação, no monitoramento dos riscos de mercado e na estabilidade financeira, inclusive com o apoio da autorregulação" (CVM, 2020). Ou seja, os dados detêm grande relevância no âmbito de atuação da CVM e é mais que natural que, diante de tamanha relevância, busque-se protegê-los.

Esse ímpeto de proteger as informações dos investidores, bem como de promover um ambiente de competitividade justa dentro do mercado de capitais, tem pautado a CVM há muito tempo. Isso pode se verificar, por exemplo, no período de promulgação do Marco Civil da Internet (Lei 12.965/2014, MCI), que trouxe mudanças sensíveis no ordenamento jurídico quanto a temática de proteção de dados, o que inclui, por óbvio, a necessidade de adequação das empresas presentes no mercado de capitais à nova lei. Sobretudo, em função da relevância que as atividades bancárias realizadas de modo online têm tomado dia após dia, bem como, as mudanças do mundo do trabalho propiciadas pela inclusão cada vez maior do mundo digital nos ambientes de trabalho.

Por consequência, um rearranjo da fiscalização da CVM para assegurar que tais critérios sejam atendidos por esses agentes de mercado também foi crucial.

Outro evento de fulcral importância para o mercado de capitais no âmbito da proteção de dados foi a entrada em vigor do RGPD (Regulamento Geral de Proteção de Dados) em 2018. Isso ocorre, pois, tal regramento tem implicações extraterritoriais nos casos em que entidades não sediadas na Europa operem dados pessoais de titulares residentes na Europa. Em um

contexto de crescente globalização, resta evidente que diversas empresas sediadas em território brasileiro se enquadram dentro desse requisito de extraterritorialidade (MAGRANI, 2018).

Não obstante, o diploma normativo também resguardava que a transferência internacional de dados só poderia ocorrer entre países que detinham um adequado nível de proteção de dados ou atendendo outros critérios normativos. O Brasil não estava incluído nesse cenário de nível adequado de proteção, pois até aquele momento só existiam legislações nacionais esparsas regulando a matéria (OLIVEIRA; LOPES, 2019).

Este evento mostrou a necessidade de o Brasil ter sua própria Lei Geral de Proteção de Dados, de modo a adequar-se ao padrão de proteção de dados previsto pelo RGPD. Portanto, a ascensão da LGPD provocou mudanças profundas em todo o cenário empresarial. o que acarretou numa atuação ainda mais firme da CVM dentro da seara do mercado de capitais para suprir as novas necessidades tanto do cenário internacional quanto do nacional.

Dessarte, a CVM passou por diversas adequações à LGPD, sobretudo, no seu âmbito interno. Assim sendo, foi promulgada a Portaria CVM/PTE/Nº 188, de 20 de outubro de 2021, e, através dela, distribuíram-se competências para a atuação da CVM entre quatro "operadores": (i) Comitê de Governança de Tecnologia da Informação e Transformação Digital (CGTI); (ii) encarregado de dados pessoais; (iii) titulares de componentes organizacionais (TCOs); e (iv) servidores e colaboradores.

As responsabilidades de atuação da CVM foram, portanto, pulverizadas entre esses agentes, de modo a conferir a maior eficiência possível para a atuação de cada um. Os CGTI ficaram responsáveis por:

> I – promover a conformidade normativa, a cultura institucional e o desenvolvimento profissional atinentes à proteção de dados pessoais;
> II – aprovar propostas de políticas e os procedimentos e padrões gerais sobre a coleta, a retenção, o tratamento, o compartilhamento e a eliminação de dados pessoais;
> III – aprovar os eventos de riscos de proteção de dados pessoais, bem como as medidas de segurança necessárias à redução dos níveis de exposição;
> IV – monitorar o progresso de projetos e atividades instituídos para aprimorar aspectos estruturais da proteção de dados pessoais na autarquia. (CVM, 2021)

Já ao encarregado de dados pessoais, compete:

I – colher, avaliar e responder às solicitações de titulares de dados de conformidade com as leis, normas, procedimentos e padrões aplicáveis;

II – diligenciar para que solicitações, recomendações e diretrizes sobre dados pessoais, oriundas de autoridade competente, sejam atendidas na forma e no prazo requeridos;

III – orientar servidores, contratados e parceiros sobre as políticas e procedimentos relativos ao tratamento de dados vigentes na autarquia na CVM;

IV – coordenar o planejamento, a comunicação e o acompanhamento das ações de melhoria da proteção de dados pessoais;

V – coordenar a gestão de riscos relativos à proteção de dados pessoais de acordo com o disposto na Resolução CVM nº 53, de 15 de outubro de 2021; e

VI – sistematizar registros, documentos e métricas com o fim de promover prestação de contas coesa, adequada e transparente. (CVM, 2021)

Quanto aos titulares de componentes organizacionais, ficaram reservadas as funções de:

I – promover a implementação de controles internos que, até o limite técnico, assegurem a autenticidade, a integridade, a confidencialidade e a disponibilidade dos dados pessoais;

II – organizar os processos de trabalho de modo que a proteção de dados pessoais seja exercida com constância de propósito e competência técnica;

III – conduzir a identificação, a classificação, a avaliação e o tratamento de riscos relativos à proteção de dados pessoais de acordo com a Resolução CVM nº 53, de 2021;

IV – engajar servidores, colaboradores e parceiros para o tratamento responsável, ético e qualificado dos dados pessoais;

V – alocar recursos orçamentários, técnicos e humanos para viabilizar, de forma tempestiva e qualificada, as medidas relativas à melhoria do tratamento de dados pessoais;

VI – promover o controle de acesso aos ativos de informação que retenham dados pessoais, conferindo especial zelo aos dados pessoais sensíveis; e

VII – informar ao encarregado de dados pessoais o progresso de ações e a exposição a riscos relativos à proteção de dados pessoais. (CVM, 2021)

Por fim, aos servidores, compete:

I – aplicar as definições, os princípios, os valores e as recomendações atinentes à proteção de dados pessoais;

II – assegurar que dados pessoais sejam coletados em virtude de interesse público ou por consentimento formal, específico e inequívoco do titular;

III – informar aos TCOs riscos e problemas operacionais que resultem em não conformidade aos princípios, valores e regras da proteção de dados pessoais; e

> IV – buscar, de forma ativa e continuada, os meios de capacitação para o correto emprego dos conhecimentos, habilidades e atitudes necessários à proteção de dados pessoais. (CVM, 2021)

2.1. Estudo do TCU e a importância do registro dos dados pessoais

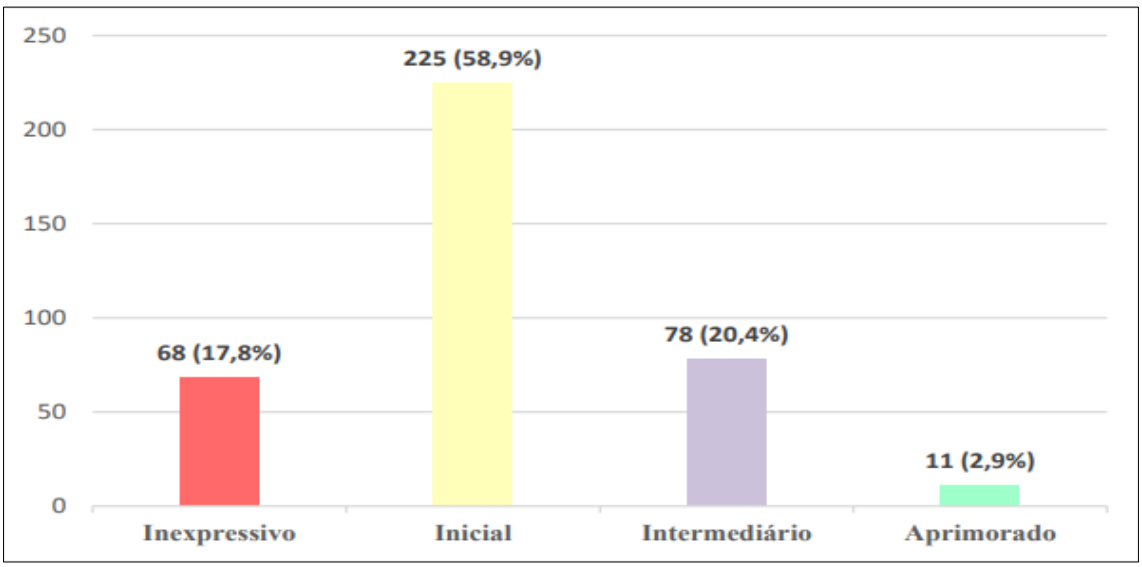
O que se extrai desse vasto rol de competências e de distribuição de tarefas é que tem sido feito um grande esforço por parte da CVM para atingir um alto padrão no que diz respeito à proteção de dados. Esse esforço foi feito com base em um relatório elaborado pelo TCU (2021) com dados coletados entre novembro de 2020 e maio de 2021. Nele, verificou-se que a CVM possuía um nível de adequação intermediário, já que ela obteve uma pontuação de 0,74 no indicador de adequação, existindo ainda um grande caminho a ser feito até que ela atingisse o nível aprimorado (0,80).

O estudo realizado pelo TCU utilizou a metodologia CSA (*Control Self-Assessment),* que consiste, essencialmente, em uma autoavaliação de controles. Nessa metodologia os gestores recebiam um questionário e o preenchiam com as respostas que melhor traduziam os controles relativos à LGPD nas suas organizações. A pesquisa levou em consideração, além da CVM, outras 382 organizações, que possuem atuação nos mais diversos segmentos. Portanto, verifica-se que foi levado em conta um universo amostral bastante abrangente para a análise.

Para além desse universo amostral, o TCU elencou diversos critérios para conseguir aferir o grau de adequação, como: “Preparação”, “Contexto Organizacional”, “Liderança”, “Capacitação”, “Conformidade do Tratamento”, “Direitos do Titular”, “Compartilhamento de Dados Pessoais”, “Violação de Dados Pessoais” e “Medidas de Proteção”.

Com base nesses critérios, o TCU distribuiu as 382 organizações em quatro níveis distintos de avanço na adequação à LGPD: Inexpressivo, com 68 das organizações; Inicial, com 225 organizações; Intermediário, com 78, por fim 11 das 382 organizações figuravam no nível aprimorado, conforme é possível depreender do quadro abaixo.

Figura 1 – Distribuição das organizações por nível de adequação à LGPD (TCU, 2021)



Fonte: elaborador pelo autor (2023)

Dentre os critérios elencados pelo estudo, o que teve maior peso negativo para a classificação da CVM foi o critério “Medidas de Proteção”, dentro dele, a CVM figurou com apenas 0,40 pontos numa escala que vai de 0 a 1. Muito embora ela esteja acima da média das organizações empregadas no estudo (0,32), percebeu-se que há uma necessidade de melhoria relevante desse aspecto.

É possível perceber, por exemplo, que a CVM não fazia o registro dos eventos das atividades de tratamento de dados pessoais, que foram definidas pelo TCU como:

> Registro dos eventos (logs) das atividades de tratamento de dados pessoais de forma que seja possível identificar por quem, quando e quais dados pessoais foram acessados. Nos casos em que ocorrem mudanças nos dados, também deve ser registrada a ação realizada (e.g.: inclusão, alteração ou exclusão) (TCU, 2021)

Visando sanar isso, a posterior normativa da CVM que disciplina a matéria determina que esse registro deve ser feito pelo controlador, nos mesmos moldes do art. 37[2] da LGPD (BRASIL, 2018).

Ou seja, a CVM agora conta com previsão normativa para cumprir esse critério. No entanto, causa uma certa estranheza que isso não tenha sido executado pela CVM à época da realização do estudo, já que isso é um requisito imposto pela LGPD. Logo, não poderia ter sido negligenciado no processo de adequação vivenciado pela CVM, pois independentemente da relevância do registro para as atividades do órgão, tratava-se de uma atividade essencial a ser desempenhada pelo controlador de dados.

A motivação para esse registro ter sido elencado na Lei é que o registro das atividades de tratamento de dados é a base para qualquer programa de adequação de dados. Tendo em vista que caso não seja feito isso não há como mensurar as próximas medidas a serem tomadas: "sem essa fotografia em série é impossível compreender o fluxo da informação, esboçar o que precisa ser modificado e o que pode ser mantido para estar em conformidade com a legislação de proteção de dados." (BIONI, 2019).

Inclusive, a CVM considerou esse ponto tão importante que na resolução CVM 35 (2021)[3], posterior a análise do TCU, foi feita uma seção específica atinente ao sistema de controle e informações que respeitavam aos empréstimos. Para além disso, no decorrer de todo o dispositivo se verificam menções esparsas a necessidade de registro e de ciência do fluxo informacional, quaisquer que fossem essas informações.

Dessa maneira, fica claro o modo como esse critério pesou negativamente na avaliação por parte do TCU acerca do nível de adequação da CVM. Também restam hialinas às motivações que levaram à CVM a mudar sua postura com relação a esse critério de modo tão célere.

[2] Art. 37 da LGPD: O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

[3] Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.

2.2. Criptografia como mecanismo de proteção dos dados

A segunda pergunta que foi utilizada no critério Medidas de Proteção e que a CVM não pontuou foi: "10.4 A organização utiliza criptografia para proteger os dados pessoais? "

A relevância da pergunta advém de o fato da criptografia cumprir um papel central na proteção de dados. Dados que não contam com essa proteção podem ser facilmente lidos e rastreados, o que pode acabar por implicar na exposição do usuário final do serviço, configurando, portanto, um cenário de vazamento de dados.

Noutras palavras: "usar criptografia aumenta a segurança do sistema e das comunicações em rede" (TEIXEIRA, 2019, p. 21). E isso se dá na medida em que permitem que apenas o destinatário da comunicação ou aos portadores da chave criptográfica acessem o conteúdo veiculado pelo usuário. Ou seja, é uma medida que é altamente eficaz em evitar que os fenômenos de vazamento de dados ocorram (MACHADO; DONEDA, 2020).

A adoção de criptografia está diretamente correlacionada com medidas eficazes para a promoção da proteção dos dados pessoais. Nessa senda, parece que o posicionamento da CVM foi adequado ao vincular a adoção da prática de criptografia ou da ausência dela às funções do CGTI, mais precisamente a de: "aprovar os eventos de riscos de proteção de dados pessoais, bem como as medidas de segurança necessárias à redução dos níveis de exposição"[4]. Ademais, parece também recair sobre os TCO o ônus de decidir sobre a adoção, ou não, da criptografia, conforme a sua competência de: "I – promover a implementação de controles internos que, até o limite técnico, assegurem a autenticidade, a integridade, a confidencialidade e a disponibilidade dos dados pessoais; ".

Verifica-se, portanto, que dentro do âmbito desta Portaria da CVM, instituiu-se elementos normativos suficientes para a adoção de criptografia, muito embora, não tenha se referido a esse aspecto de modo explícito na redação do diploma.

O cenário de que a CVM não faz uso de criptografia no tratamento de dados pessoais já não existe mais, pois, ao adentrar em seu site é possível visualizar que agora o site adotou o emprego de criptografia para tratar os dados pessoais. Em anúncio do próprio sítio eletrônico explica-se que "[o] site utiliza criptografia para que os dados sejam transmitidos de forma

[4] CVM. CVM/PTE/Nº 188, DE 20 DE OUTUBRO DE 2021. Dispõe sobre as competências gerais relativas à proteção de dados pessoais na Comissão de Valores Mobiliários –CVM. Brasília, DF, outubro de 2021. Disponível em: < portaria_cvm_pte_188_2021_protecao_dados_pessoais.pdf (www.gov.br)>. Acesso em: 18 de fev. 2023.

segura e confidencial, de maneira que a transmissão dos dados entre o servidor e o usuário, e em retroalimentação, ocorra de maneira totalmente cifrada ou criptografada. ” (CVM, 2022).

A correção desse fator apontado pelo TCU foi vital para fornecer maior proteção aos usuários do site da Comissão. Mas não só isso, também serviu de incentivo para que as empresas reguladas ou não pela CVM enxergassem nessa prática um mecanismo efetivo de evitar um cenário de vazamento de dados, já que esse tipo de incidente é relevante e sempre continuará sendo.

A título exemplificativo, percebe-se que cerca de 12% das decisões analisadas em estudo recente de jurimetria (OPICEBLUM, 2022) tinham como palco um incidente de dados e em 2020 houve cerca de 870 mil incidentes de cibersegurança no Brasil (LEMOS, 2020). O ideal é que a adequação à LGPD das empresas e entidades do setor público aumente para que esse número não cresça, com a adoção da prática da criptografia sendo um importante passo nessa direção.

2.3. *Privacy by design* e *Privacy by Default*

Por fim, há que se falar ainda na última questão formulada pelo estudo do TCU quanto ao requisito de Proteção de Dados: “10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*Privacy by Design* e *Privacy by Default*)?” (TCU, 2021).

Privacy by design pode ser entendida enquanto o meio de garantir a privacidade e proteção de direitos e liberdades dos indivíduos usuários de determinado sistema. Impõe, pois, a necessidade de que o sistema seja arquitetado tendo em mente os princípios e as previsões legais da Lei Geral de Proteção de Dados (OPICEBLUM, 2021).

Para além disso, o termo “*Privacy by Design*” é guiado por outros sete princípios, que foram criados e consolidados na doutrina por Ann Cavoukian em 2009. Na legislação os

princípios constam de forma explícita no art. 25 da RGPD[5] e no art. 46 §2º[6] da LGPD (OPICE BLUM, 2021, p. 16,17). Os 7 princípios são:

> I - empresas devem adotar abordagem proativa e não reativa;
> II - sistemas, serviços e produtos devem proteger os dados pessoais de titulares;
> III - design deve ser incorporado às medidas adotadas para a proteção de dados de titulares;
> IV - empresas não devem coletar mais dados do que o necessário;
> V - deve ser adotada segurança de ponta a ponta;
> VI - práticas empresariais devem ser dotadas de visibilidade e transparência; e
> VII - deve ser respeitada a privacidade do usuário. (OPICEBLUM, 2021)

Dessa maneira, fica evidente que o conceito de "*Privacy by Design*" é de grande relevância para a seara da proteção de dados. Ele abriga uma série de boas práticas que auxiliam, de maneira bastante efetiva, a assegurar a proteção dos dados do usuário anteriormente ao início de qualquer tratamento de dados.

O conceito de "*Privacy by Default*" por sua vez, tem como intento asseverar que sempre que um serviço/produto for divulgado ou lançado ao público, ele conterá as configurações mais atualizadas e seguras de proteção de dados por padrão. Isso quer dizer que não há necessidade de qualquer tipo de gerência por parte do usuário final para garantir um nível adequado de proteção (PRIVACY TECH, 2019).

Fica fácil perceber que ambos os conceitos estão intimamente relacionados e que ambos servem para assegurar a proteção máxima dos usuários antes da realização de qualquer

[5] Art 25 da LGPD: I- Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
II - O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

[6] Art. 46 §2º da LGPD: 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.

tratamento de dados. Portanto, não é estranho o fato de ambos os termos integrarem as legislações que os adotam no mesmo trecho.

Consoante afirmado alhures, a interpretação do art. 25 da RGPD, bem como do art. 46, § 2°, da LGPD, deve nos levar ao seguinte entendimento:

> Os agentes devem aplicar, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, medidas técnicas e organizacionais adequadas, assegurando, por padrão, que somente sejam tratados dados pessoais essenciais para cada finalidade específica de tratamento e, em especial, que dados pessoais não sejam disponibilizados, sem intervenção humana, a um número indeterminado de pessoas. (GUARIENTO E MARTINS, 2021)

A LGPD, por sua vez, importou o instituto em seu art. 46[7], com a ressalva prevista em seu §2° de que as medidas: "deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

Verifica-se que a estruturação da Portaria 188 cumpriu um papel fundamental para suprir esses requisitos, haja vista que foram definidas diretrizes nesse sentido de modo bastante amplo para todos os operadores listados. Isso é visto, especialmente, pelo modo com que a norma a todo momento se refere, de maneira tácita, a necessidade em planejar os novos sistemas para que eles já contem com adequação à LGPD desde o seu início.

No entanto, não é despiciendo relembrar que "esses princípios, no entanto, foram pensados para garantir a privacidade em sistemas de organizações em construção, nas quais os processos de engenharia de produção ainda não foram desenvolvidos, estando, pois, livres de práticas e vícios anteriores" (GUARIENTO E MARTINS, 2021).

Para o caso da CVM, contudo, verifica-se que muitas das práticas e dos padrões ali empregados já fazem parte da rotina da organização e dificilmente poderiam ser inteiramente derrubados para a reconstrução de novos. Aí é que se faz necessária a utilização do conceito de *privacy by redesign* (GUARIENTO E MARTINS, 2021). Esse conceito consiste,

[7] 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.

essencialmente, na reestruturação dos sistemas já definidos pela organização para que eles passem a entrar em conformidade com a LGPD.

Esses dispositivos afiguram-se como relevantes não só para a CVM internamente, mas também no seu objeto de regulação externo, qual seja, o âmbito do mercado de capitais. Isso se dá na medida em que o conceito de *Privacy By Design* atua enquanto salvaguarda do princípio da Responsabilidade Social Empresarial[8], mais especificamente, no que tange ao tratamento de dados do consumidor. (ROLIM, 2022).

A CVM detém competência de regular e estimular medidas autorregulatórias, bem como de assegurar que as práticas voluntárias adotadas pelas organizações observem padrões mínimos de qualidade e de objetividade. Nessa senda, é natural que a preocupação de estar em conformidade com essas práticas também seja muito presente dentro da autarquia. (ROLIM, 2022; ATHAYDE e FRAZÃO, 2018).

As referências presentes na Portaria 188 (CVM, 2021) permitem concluir com uma grande margem de segurança, que a legislação da CVM evoluiu de modo a permitir com que esses três conceitos integrassem a cultura organizacional da entidade. Assim sendo, verifica-se que a Portaria auxiliou na melhoria da proteção de dados dentro da entidade autárquica no âmbito prático. Como é sabido, o objetivo da LGPD é, justamente, promover uma cultura duradoura de proteção de dados, objetivo que foi atingido, sobremaneira, pelos mecanismos da Portaria.

> A LGPD pretende uma mudança de pensamento duradoura, prezando por estabelecer uma cultura de proteção de dados no cenário brasileiro, o que tem sido ignorado, tendo em vista que o receio de sofrer sanções foi o principal motivo que levou as empresas a se adaptarem, e não o verdadeiro intuito da Lei, que é o de garantir a segurança dos dados e proteção de seus titulares a longo prazo. (LUGATI, ALMEIDA, 2022, p. 3).

Considerações finais

Foi possível perceber que a nova Portaria da CVM forneceu diversas ferramentas para solucionar os problemas relativos à proteção de dados apontados no parecer anterior feito pelo

[8] Trata-se da responsabilidade empresarial em prestar de forma transparente, informações de relevante interesse para aquelas pessoas que são atingidas por suas atividades, o Estado, o mercado e a sociedade de uma forma geral.

TCU. E se todas as medidas que a LGPD determina foram tomadas, o nível de proteção de dados da CVM pode subir a ponto de permitir com que a Autarquia figure num estudo posterior como nível de adequação aprimorado.

As medidas adotadas pela CVM para incrementar a sua proteção de dados também podem servir de norte para outras entidades públicas seguirem por esse mesmo caminho. Sobretudo, no que se refere às práticas de "*privacy by design* e *privacy by default*", que são muito importantes para evitar com que incidentes de dados ocorram, bem como outras falhas atinentes à segurança de informação.

Vale ressaltar que inclusive entes privados podem ser beneficiados pelas práticas empregadas pela CVM, já que nada impede que eles venham a fazer uso das mesmas técnicas preconizadas pela CVM para as suas próprias empresas. Uma vez que os desafios inerentes à proteção de dados são novos, a prática de espelhar boas condutas de outros agentes pode ser muito benéfica quando não se tem o *know-how* necessário para aplicar isso de ofício.

Ademais, a CVM também pode utilizar como parâmetro para realização de futuras legislações atinentes à temática da proteção de dados os resultados obtidos tanto dessa legislação, quanto de outras. Pode, inclusive, propor boas práticas para as entidades vinculadas ao mercado de capitais, com base na sua própria experiência de adequação, propiciando, assim, um aumento geral no nível de adequação de dados.

Entretanto, ainda é possível avançar dentro dessa temática através de pesquisas mais aprofundadas que façam uso de outros instrumentos metodológicos, como, por exemplo, coleta de dados referentes à proteção de dados dentro da CVM. Isso levaria a uma pesquisa de maior profundidade que permita esgotar as outras temáticas levantadas no estudo, já que, como dito anteriormente, o presente artigo tratou única e exclusivamente da questão da proteção de dados em si. No entanto, dentro do próprio estudo do TCU são apontados diversos outros critérios que poderiam ser objeto de melhora por parte da CVM e poderiam ser explorados em futuras pesquisas.

Resta dizer que o intuito principal das modificações propostas pela CVM, e que são de grande relevância para qualquer projeto de adequação à LGPD, é mudar a visão da organização no que respeita à LGPD, fornecendo um novo paradigma para a atuação da organização. Tal paradigma inclui, mas não se limita a revisar as práticas correntes da organização, realizar novas práticas já com foco na LGPD e, especialmente, em promover a

constante capacitação e importância da temática da proteção de dados aos colaboradores. Conforme previsto na própria Portaria objeto do presente estudo, cabe aos servidores: "buscar, de forma ativa e continuada, os meios de capacitação para o correto emprego dos conhecimentos, habilidades e atitudes necessários à proteção de dados pessoais. " E caso isso não ocorra, todo esforço empregado na adequação pode vir a se perder, resta torcer para que o incentivo da CVM para evitar isso superem as intempéries do tempo.

Referências bibliográficas

ATHAYDE, Amanda; FRAZÃO, Ana. Leniência, compliance e o paradoxo do ovo ou da galinha: do compliance como instrumento de autorregulação empresarial. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord). Compliance: perspectivas e desafios dos programas de integridade. Belo Horizonte: Fórum, 2018.

BIONI, Bruno Ricardo. A obrigação de registro das atividades de tratamento de dados. Brasil, 2019. Disponível em: A obrigação de registro das atividades de tratamento de dados | Jusbrasil. Acesso em: 14 maio 2023.

BRASIL. CVM e o Mercado de Capitais. Brasil, 2014. Disponível em: <Microsoft Word - CVM E O MVM (www.gov.br)>. Acesso em: 16 de fev. de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF, agosto de 2018. Disponível em: < L13709 (planalto.gov.br)>. Acesso em: 10 de fev. 2023.

CVM. RESOLUÇÃO CVM N° 35, DE 26 DE MAIO DE 2021. Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020. Disponível em: < RESOLUÇÃO CVM Nº 35, DE 26 DE MAIO DE 2021 - RESOLUÇÃO CVM Nº 35, DE 26 DE MAIO DE 2021 - DOU - Imprensa Nacional (in.gov.br)>. Acesso em: 15 de fev. de 2023.

CVM. CVM/PTE/Nº 188, DE 20 DE OUTUBRO DE 2021. Dispõe sobre as competências gerais relativas à proteção de dados pessoais na Comissão de Valores Mobiliários –CVM. Brasília, DF, outubro de 2021. Disponível em: < portaria_cvm_pte_188_2021_protecao_dados_pessoais.pdf (www.gov.br)>. Acesso em: 18 de fev. 2023.

CVM. Termos de Uso. Brasil, 2022. Disponível em: < CVMWEB-TU-v20220810.pdf>. Acesso em: 20 de fev, 2023.

CVM. Valores. Brasil, 2020. Disponível em: <Valores (cvm.gov.br)>. Acesso em: 18 de fev, 2023.

LEMOS, Ronaldo. Privacy By Design: conceito, fundamentos e aplicabilidade na LGPD. In: BIONI, Bruno et al. Tratado de proteção de Dados pessoais. Brasília, Curitiba, Porto Alegre, São Paulo: Forense, 2020. Edição do Kindle. E-book.

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. Revista de Direito, *[S. l.]*, v. 14, n. 01, p. 01–20, 2022. DOI: 10.32361/2022140113764. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 26 fev. 2023.

MACHADO, Diego; DONEDA, Danilo. DIREITO AO ANONIMATO NA INTERNET: FUNDAMENTOS E CONTORNOS DOGMÁTICOS DE SUA PROTEÇÃO NO DIREITO BRASILEIRO. Brasil, Revista de Direito Civil Contemporâneo, v. 23, ano 7, p. 95-140, 2020. Disponível em:<Microsoft Word - Direito ao anonimato na Internet - Fundamentos e contornos dogmáticos de sua proteção no direito brasileiro. Draft..docx (ssrn.com)>. Acesso em: 14 de fev. de 2023.

MAGRANI, Eduardo. Seis pontos para entender o Regulamento Geral de Proteção de Dados da UE. 2018. Disponível em: < http://eduardomagrani.com/seis-pontos-para-entender-o-regulamento-geral-de-protecao-de-dados-da-ue/>. Acesso em: 18 de fev. 2023.

MARTINS, Ricardo Maffeis; GUARIENTO, Daniel Bittencourt. Privacy by Design, by default e by redesign. Brasil: Migalhas, 2021. Disponível em: <Privacy by design, by default e by redesign - Migalhas>. Acesso em: 20 de fev. de 2023.

NEVES, Douglas Ramos Inacio. A segurança de dados em um ambiente corporativo. Trabalho de conclusão de curso (Curso de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2015. Disponível em: <Repositório Institucional do Conhecimento do Centro Paula Souza: A segurança de dados em um ambiente corporativo (cps.sp.gov.br)>. Acesso em: 26 de fev. de 2023>

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

OPICE BLUM. LGPD_LOOKOUT, RELATÓRIO ANUAL DE JURIMETRIA 2022. Brasil, 2022. Disponível em: <09-relatorio-jurimetria-2022.pdf (opiceblum.com.br)>. Acesso em: 26 de fev. de 2023.

OPICE BLUM. O QUE É PRIVACY BY DESIGN E COMO ESTÁ INSERIDO NA LGPD? Brasil, 2021. Disponível em: <O que é Privacy by Design? | Opice Blum>. Acesso em: 14 de fev. de 2023.

PRIVACY TECH. Privacy by Design e by Default: entenda a diferença. Brasil, 2019. Disponível em: <Privacy by Design e by Default: entenda a diferença - Privacy Tech - Portal sobre privacidade e proteção de dados>. Acesso em: 24 de fev. de 2023.

ROLIM, Maria da Conceição Lima Melo. A SEGURANÇA DOS DADOS EM UM AMBIENTE CORPORATIVO. Orientador: Sandro Mansur Gilban. 2022. Monografia (Programa de Pós-Graduação em Direito Empresarial e Cidadania) - UNICURITIBA, [S. l.], 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/25101. Acesso em: 14 fev. 2023.

TEIXEIRA, Pedro Henrique da Silva. AUTENTICAÇÃO DE USUÁRIO: GARANTINDO A INTEGRIDADE DOS DADOS ATRAVÉS DE CRIPTOGRAFIA. Brasil, p. 21, 2019. Disponível em: http://raam.alcidesmaya.com.br/index.php/projetos/article/download/61/59. Acesso em: 14 maio 2023.

TCU. (Acórdão 1.384/2022-TCU-Plenário, Relatoria Min. Augusto Nardes). Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. Disponível em: <09-1638734_anexo_ao_oficio0146_2022_tcu_sefti.pdf (www.gov.br)> Acesso em: 26 de fev. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO AUTARQUIA ESPECIAL

Wanessa Larissa Silva de Araújo[1]

Resumo: A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia da administração pública federal responsável por garantir a proteção de dados pessoais no Brasil. Este artigo visa apresentar que a transformação da natureza jurídica da ANPD em autarquia especial consolidou a sua independência e autonomia técnica, decisória, administrativa e orçamentária. Para tanto, fez-se necessário realizar uma pesquisa de abordagem qualitativa de caráter exploratório bibliográfico e documental, o que permitiu apresentar uma visão geral dos marcos cronológicos que resultaram na ANPD como autarquia especial, o que repercutiu positivamente para a proteção dos dados pessoais nas relações nacionais e internacionais.

Palavras-chave: ANPD; LGPD; Autarquia Especial; Direito Administrativo.

Abstract: *The National Data Protection Authority (ANPD) is the federal public administration autarchy responsible for the enforcement of the protection of personal data in Brazil. This article aims to present that the transformation of the legal nature of the ANPD into a special autarchy consolidated its independence and technical, decision-making, administrative and budget autonomy. Therefore, it was necessary to carry out qualitative research with an exploratory bibliographical and documentary approach, which allowed presenting an overview of the chronological milestones that resulted in the ANPD as a special autarchy, which had a positive impact on the protection of personal data at the national and in international relations.*

Keywords**:** *ANPD; LGPD; Special Autarchy; Administrative Law.*

[1] Pesquisadora vinculada ao Observatório da LGPD. Graduada em Direito pela Universidade de Brasília.

Introdução

Este artigo, mediante análise dos arcabouços legais de proteção de dados pessoais brasileiros, parte de uma investigação bibliográfica e documental acerca da **Autoridade Nacional de Proteção de Dados (ANPD) como Autarquia Especial**. Nesse sentido, o objetivo da pesquisa é evidenciar a transformação da natureza jurídica da Autoridade como forma da consolidação da sua devida independência e autonomia institucional.

A Lei Geral de Proteção de Dados (LGPD) – Lei n° 13.709 foi sancionada em 2018; porém, durante a fase de sanção, foi vetada a criação da ANPD pelo Presidente da República. O veto presidencial foi realizado sob alegação de inconstitucionalidade do processo legislativo por vício de iniciativa, já que a criação da Autoridade deveria ser de iniciativa do Poder Executivo Federal.[1]

Por outro lado, o então presidente Michel Temer expressou concordância em relação à criação da Autoridade. Diante disso, em dezembro de 2018, foi publicada a Medida Provisória nº 869/2018 que posteriormente foi convertida na Lei nº 13.853/2019 com algumas modificações em relação ao texto apresentado no Projeto de Lei. Assim, vale destacar que a Autoridade foi criada como um órgão da administração pública federal, integrante da Presidência da República (DONEDA, 2020, p. 466).

A necessidade de proporcionar maior nível de independência e transformar a natureza jurídica da ANPD foi expressa na própria Lei nº 13.853/2019. O art. 55-A, §§1º e 2º, demonstravam a natureza "transitória" da ANPD, uma vez que estabelecia o prazo de dois anos, a partir da entrada em vigor da estrutura regimental, para que houvesse uma avaliação da possibilidade de converter a natureza da Autoridade, tendo em vista seu caráter transitório legalmente estabelecido pela hipótese de que poderia "*ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República*" (art. 55-A, §1º).

[1] BRASIL, SENADO. Sancionada com vetos a Lei Geral de Proteção de Dados Pessoais. Brasília, 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais?utm_campaign=Artigos&utm_content=Sancionada+com+vetos+lei+geral+de+prote%C3%A7%C3%A3o+de+dados+pessoais+%E2%80%94+Senado+Not%C3%ADcias+%281%29&utm_medium=email&utm_source=EmailMarketing&utm_term=Artigo:+Aprovada+MP+869/2018+que+cria+a+Autoridade+Nacional+de+Prote%C3%A7%C3%A3o+de+Dados+Brasileira>. Acesso em: 26 fev. 2023.

Conforme as referências internacionais e parâmetros do Estado Democrático, os órgãos administrativos independentes podem ser caracterizados pela sua autonomia organizacional, financeira e contábil. Vale citar que, em 2000, a Carta de Direitos Fundamentais da União Europeia inaugurou a concepção de que a autoridade de garantia constitui o ponto essencial do próprio direito fundamental à proteção de dados pessoais. Isso repercutiu no Regulamento Geral de Proteção de Dados (GDPR), bem como nos países que possuem legislação de proteção de dados, inclusive o Brasil (DONEDA, 2020, p. 468).

Diante disso, considera-se que a **proteção de dados pessoais é fortalecida por meio do estabelecimento de uma Autoridade de Proteção independente e autônoma**. Sendo assim, diante do ordenamento jurídico brasileiro e da demanda regulatória, fez-se necessário consolidar a independência e autonomia da ANPD por meio da transformação da natureza jurídica da instituição.

A transformação da ANPD em autarquia especial e, por conseguinte, a consolidação da sua independência e autonomia são produtos de diversos marcos cronológicos da história da proteção de dados pessoais do Brasil. Nesse sentido, o presente artigo apresenta o objeto de pesquisa, conforme os três seguintes tópicos: **(i) Definição e Cronologia dos Marcos Importantes da ANPD; (ii) ANPD como Autarquia Especial; e (iii) A importância da Transformação da Natureza Jurídica da ANPD.**

1. Definição e Cronologia dos Marcos Importantes da ANPD

Faz-se necessário destacar a ANPD nos termos da LGPD. A LGPD define a autoridade nacional como "*órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional"* (art. 5º, XIX, LGPD). Tal definição é detalhada pela Seção I do Capítulo IX da LPGD, o que abrange os artigos 55-A ao 55-M.

Diante disso, torna-se conveniente reproduzir a cronologia dos marcos importantes da Autoridade, conforme demonstrado na Tabela 1.[1]

[1] BRASIL, ANPD. ANPD torna-se autarquia de natureza especial. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>.

Tabela 1 – Cronologia dos Marcos Importantes da ANPD

Mês e Ano	Marco Cronológico
Ag/2018	Publicada a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, com veto sobre a criação da ANPD.
Dez/2018	Medida Provisória (MPV) nº 869 dispunha sobre a proteção de dados pessoais e a criação da Autoridade Nacional de Proteção de Dados.
Jul/2019	Conversão da MPV nº 869 na Lei nº 13.853, de 08 de julho de 2019, que cria a Autoridade Nacional de Proteção de Dados.
Ago/2020	Definida e aprovada a estrutura regimental e o quadro de cargos da ANPD pelo Decreto nº 10.474, de 26 de agosto de 2020, posteriormente, alterada pelo Decreto nº 10.975, de 22 de fevereiro de 2022.
Nov/2020	Nomeação do primeiro Diretor-Presidente da Autoridade Nacional de Proteção de Dados, Waldemar Gonçalves Ortunho Júnior, em 06 de novembro de 2020, bem como dos 4 Diretores do Conselho Diretor da Autoridade: Arthur Pereira Sabbat, Joacil Basílio Rael, Nairane Farias Rabelo Leitão e Miriam Wimmer.
Mar/2021	Publicação do Regimento Interno da Autoridade, pela Portaria nº 1, de 8 de março de 2021.
Fev/2022	Promulgação da Emenda Constitucional nº 115/2022, em 10 de fevereiro de 2022, que insere o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais do art. 5º da Constituição Federal, além de fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.
	Em fevereiro, a Autoridade teve sua composição organizacional fortalecida pela publicação do Decreto nº 10.975/2022, que modificou a estrutura da ANPD acrescentando novos cargos, remanejando e transformando cargos em comissão e funções de confiança, além da criação da Coordenação-Geral de Tecnologia da Informação (CGTI).[1]
Jun/2022	Publicação da Medida Provisória nº 1.124, de 13 de junho de 2022, que transforma a natureza jurídica da Autoridade Nacional de Proteção de Dados em autarquia de natureza especial.
Out/2022	Conversão da MPV nº 1.124 na Lei nº 14.460, de 25 de outubro de 2020, que cria a Autoridade Nacional de Proteção de Dados.
	Publicação do Decreto nº 11.348, de 1º de janeiro de 2023, que estabeleceu a nova estrutura do Ministério da Justiça, contemplando a ANPD como órgão vinculado à Pasta.[2]
Jan/2023	
	Publicação da Medida Provisória nº 1.154, de 1º de janeiro de 2023, que estabeleceu o apoio administrativo à ANPD pelo Ministério da Justiça e da Segurança Pública.
	Publicação da Portaria Conjunta MJSP/ANPD nº 5/2023, de 09 de fevereiro de 2023, que estabeleceu a colaboração temporária em atividades administrativas a serem prestadas pelo Ministério da Justiça e da Segurança Pública (MJSP).[3]

Fonte: Adaptado da ANPD

A cronologia dos marcos importantes da ANPD demonstra o caminho gradativo para o estabelecimento de uma autoridade de garantia da proteção de dados pessoais, cuja competência é importante para a efetivação da tutela desse direito fundamental. Danilo Doneda (2020, p. 302) propõe uma definição às autoridades de proteção como

> entes ou órgãos públicos dotados de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; da falta de controle e sujeição ao poder Executivo, dotadas de garantias de autonomia através da nomeação de seus membros, dos requisitos para esta nomeação e da duração de seus mandatos; e tendo função de tutela de interesses constitucionais em campos socialmente relevantes.

Conforme Danilo Doneda (2021), a independência e autonomia são atributos fundamentais para autoridades de proteção de dados. Doneda destaca que a independência pode ser garantida por meio do isolamento da atuação da autoridade em relação à influência dos poderes estatais constituídos na administração pública direta.

Nesse sentido, ressalta-se que há características que demonstram a independência da Autoridade. Conforme Doneda (2021), tais características são: (i) gerência sobre o próprio orçamento e estrutura; (ii) limitação na escolha dos membros como exigência de especialização da formação profissional; (iii) incompatibilidade de atuação dos membros com outras atividades; e (iv) ausência de ingerência governamental sobre atos da autoridade; ou seja, desvinculação hierárquica em relação ao governo.

Tal independência convive com o paradoxo de essas autoridades não serem diretamente legitimadas pelo voto popular. Diante disso, Doneda (2021) destaca a importância do equilíbrio entre a sua independência e os fundamentos da sua legitimidade, o que pode envolver mecanismos de controle por meio de atribuição e delimitação de competências por lei, referências constitucionais e objetivos específicos.

Diante disso, convém destacar que leis e outros atos normativos brasileiros demonstram esforços para garantir a independência e autonomia da ANPD. Isso é demonstrado no tópico seguinte que apresenta a Autoridade como autarquia especial.

2. ANPD como Autarquia Especial

O processo legislativo da LGPD abrange debates do início de 2010 com a primeira versão do Anteprojeto, bem como com a segunda versão em 2015. O Anteprojeto de Lei de Proteção de Dados foi elaborado sob a coordenação do Ministério da Justiça e seu texto inicial não incluía a criação de uma autoridade para supervisionar a lei; porém, havia menções implícitas sobre a centralidade de um "*órgão competente*".

A consulta pública ministerial teve algumas contribuições da sociedade civil em relação ao "*órgão competente*" voltadas a definirem questões sobre nomenclatura, finalidades e competência.[1] O texto inicial foi encaminhado à Casa Civil da Presidência da República que posteriormente o enviou para a Câmara dos Deputados, o que resultou no Projeto de Lei nº 5.276, no dia 13 de maio de 2016 (DONEDA, 2021).

A Comissão especial da Câmara dos Deputados criada para analisar o PL nº 5.276/2016 incluiu explicitamente a criação da autoridade sob o formato de uma autarquia federal em regime especial. Conforme Maria Di Pietro (2023), a autarquia é pessoa jurídica de direito público que compõe a Administração indireta, mas possui as mesmas prerrogativas e sujeições da Administração Direta. A autora também enfatiza que a doutrina apresenta cinco características comuns das autarquias: (i) criação por lei; (ii) personalidade jurídica própria; (iii) capacidade de autoadministração; (iv) especialização dos fins ou atividades; e (v) sujeição a controle ou tutela.

Com base na doutrina italiana, Márcio Iório Aranha (2018) compreende que o conceito de autarquia consiste na personalidade jurídica dotada de autoadministração e autossuficiência. Segundo Di Pietro (2023), o regime especial corresponde (i) à maior autonomia em relação à Administração Direta; (ii) estabilidade do mandato fixo dos seus dirigentes; e (iii) ao caráter final das suas decisões, que não são sujeitas à apreciação por outros órgãos ou entidades da Administração Pública.

Sobretudo, o texto que criava a ANPD como autarquia em regime especial foi aprovado pelo plenário da Câmara dos Deputados e do Senado Federal para seguir sanção presidencial; porém, a ANPD como autarquia especial foi vetada pela Presidência da República, sob o argumento que tal previsão ultrapassava o limite da competência do Poder Legislativo, uma vez

[1] BRASIL. Ministério da Justiça. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 26 fev. 2023.

que estabelecia matéria de competência restrita do Presidente, pois envolvia aumento de despesas em projeto de lei (DONEDA, 2021).

A Lei Geral de Proteção de Dados Pessoais foi sancionada em 14 de agosto de 2018 (BRASIL, 2018, art. 5º, XIX); porém, a criação da Autoridade Nacional foi vetada sob alegação de vício de iniciativa por parte do Poder Legislativo. Assim, no dia 27 de dezembro de 2018, foi publicada a Medida Provisória nº 869/2018, a qual criou a Autoridade Nacional de Proteção de Dados e modificou outros pontos da Lei (DONEDA, 2021).

A Medida Provisória 869/2018 retirou o termo "indireta" associado à administração e estabeleceu a ANPD como órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei (BRASIL, 2018b, art. 5º, XIX). Após modificações pela Comissão Mista no Congresso Nacional, a MPV 869/2018 foi convertida na Lei 13.853, no dia 08 de julho de 2019, que modificou a LGPD e estabeleceu o caráter transitório da natureza jurídica da Autoridade, nos termos do art. 55-A com a seguinte previsão:

> Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)
> § 1º **A natureza jurídica da ANPD é transitória e poderá ser transformada** pelo Poder Executivo em entidade da administração pública federal indireta, **submetida a regime autárquico especial** e vinculada à Presidência da República.
> § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo **deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.**
> § 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias *(grifos nossos)*.

O art. 55-A revela a importância do caráter transitório da ANPD em relação ao regime e estrutura administrativa. Isso decorre da possibilidade de o Poder Público transformar a Autoridade em entidade pública federal indireta, submetida ao regime autárquico especial vinculada à Presidência da República, cuja avaliação e transformação deveria ser realizada em até 2 anos da sua estruturação.

Diante disso, destaca-se a definição da estrutura organizacional da ANPD estabelecida pelo Decreto 10.474, de 26 de agosto de 2020. Fez-se determinações importantes para os

parâmetros necessários à instalação do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD). Nesse sentido, ressalta-se a importância da publicação do Regimento Interno da Autoridade, pela Portaria nº 1, de 8 de março de 2021. Sobretudo, em 2022 foi publicado o Decreto nº 10.975, de fevereiro de 2022, que modificou a estrutura da ANPD e criou a Coordenação-Geral de Tecnologia da Informação, com vista a fortalecer a autonomia técnica e decisória da Autoridade.

Finalmente, em 13 de junho de 2022 a Presidência da República assinou a Medida Provisória nº 1.124 que transformou a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial.[1] Em agosto de 2022, o CNPD manifestou apoio à conversão da MPV 1.124/2022 em lei. O órgão consultivo destacou que o estatuto jurídico preconizado pela Medida Provisória apresenta condição adequada para que a ANPD seja autônoma e independente em aspectos orçamentários, funcionais, técnicos e administrativos.[2]

Vale ressaltar que a manifestação do CNPD destacou a importância de a MPV 1.124/2022 tratar exclusivamente sobre a conversão da ANPD em autarquia de natureza especial e questões correlatas à independência da Autoridade.[3] Por outro lado, o parecer do Relator, Senador Jorge Kajuru, demonstra que a MPV envolveu a apresentação de 29 emendas perante a Comissão Mista que abordava matérias diversas do objetivo da MPV.

As 29 emendas foram analisadas conforme 9 objetivos sobre (i) alocação de servidores e criação de carreira; (ii) inclusão de termos específicos, criação da Procuradoria da ANPD e critérios de escolha dos membros do Conselho Diretor; (iii) fixação do mandato dos membros do Conselho Diretor; (iv) garantia da prevalência do direito ao acesso à informação, nos termos da Lei de Acesso à Informação (LAI); (v) fixação do número e qualidade dos membros do Conselho Nacional de Proteção de Dados Pessoais e de Privacidade (CNPD); (vi) destinação do produto da arrecadação das multas ao Fundo de Defesa de Direitos Difusos; (vii) mudanças relativas ao tratamento de dados pessoais de crianças e adolescentes; (viii) alteração da LAI para instituir o teste de dano e interesse público; (ix) inclusão de crime relativo à inviolabilidade

[1] BRASIL, ANPD. Disponível em: ANPD torna-se autarquia de natureza especial. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>. Acesso em: 26 fev. 2023.
[2] BRASIL, ANPD. Nota de Apoio à Conversão da MPV nº 1.124/2022. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/cnpd-2/nota-de-apoio-a-conversao-da-mpv-1-124-2022>. Acesso em: 26 fev. 2023.
[3] *Ibidem.*

dos segredos no Código Penal.[1] O parecer concluiu que as emendas não apresentaram relevância à Lei Geral de Proteção de Dados Pessoais, assim as duas Casas Legislativas aprovaram a conversão da MPV 1.124/2022, sem emendas, na Lei nº 14.460, de 25 de outubro de 2022.[2] Vale ressaltar que a Lei nº 14.460 revogou os §§ 1º, 2º e 3º do art. 55-A e estabeleceu a seguinte previsão: "*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*" (BRASIL, 2022, art. 55-A).

Convém ressaltar que em setembro de 2022, foi inaugurada a sede da autarquia na capital federal. Conforme o Diretor-Presidente, Waldemar Gonçalves, as novas instalações permitem que as funções da ANPD sejam desempenhadas com maior eficiência, o que representa um passo importante para o fortalecimento da instituição, especialmente após a conversão em autarquia de natureza especial.[3]

Segundo manifestação do Poder Executivo, a Lei visa evitar a descontinuidade administrativa da ANPD. Além disso, destaca-se o objetivo de trazer mais confiabilidade ao sistema regulatório relativo à proteção de dados, tendo em vista que a natureza especial é compatível com outros regimes regulatórios internacionais.[4]

Torna-se inequívoco que a proteção de dados pessoais no Brasil foi fortalecida com a promulgação da Lei nº 14.460/2022. A natureza especial da Autoridade preserva a autonomia técnica e decisória em relação à administração pública direta, bem como garante que a gestão administrativa e financeira seja descentralizada, assim como as demais autarquias. Além disso, a Lei é importante também por (i) atribuir determinações sobre o corpo técnico da ANPD; (ii) converter o cargo do Diretor-Presidente em Cargo de Natureza Especial sem aumento de

[1] BRASIL, Senado Federal. Parecer nº 309 de 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9205606&ts=1667313945386&disposition=inline>. Acesso em: 26 fev. 2023.
[2] BRASIL, ANPD. ANPD comemora aniversário de dois anos. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-comemora-aniversario-de-dois-anos>. Acesso em: 26 fev. 2023.
[3] BRASIL, ANPD. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade visita nova sede da ANPD. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/cnpd-2/nota-de-apoio-a-conversao-da-mpv-1-124-2022>. Acesso em: 26 fev. 2023.
[4] BRASIL, Câmara dos Deputados. Promulgada lei que transforma Autoridade Nacional de Proteção de Dados em autarquia. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9205606&ts=1667313945386&disposition=inline>. Acesso em: 26 fev. 2023.

despesa; (iii) alocar servidores; e (iv) mudar a estrutura para viabilizar o funcionamento institucional.[1]

Nesse sentido, revela-se que a mudança da natureza jurídica da ANPD complementa a autonomia técnica e decisória com a plena autonomia administrativa e orçamentária. Sendo assim, revela-se a importância da positivação da ANPD como autarquia especial, tendo em vista que tal condição proporciona uma autonomia para o pleno exercício das suas respectivas funções e competências legais. Diante disso, a análise da importância de tal mudança é endereçada no próximo tópico.[2]

3. A Importância da Transformação da Natureza Jurídica da ANPD

A Autoridade Nacional de Proteção de Dados como autarquia especial indica a consolidação de uma Autoridade com a devida independência e autonomia. Trata-se de condição necessária para priorizar ações que podem melhorar resultados para a sociedade da informação com maior segurança jurídica aos titulares e agentes de tratamento de dados pessoais, principalmente, por estar vinculada ao Ministério da Justiça e Segurança Pública (MJSP) que possui coordenadoria específica para Direitos Digitais.[3]

Stéfano Rodotá considera que a necessidade da autoridade administrativa independente é confirmada pela experiência dos países que não a previram, onde a proteção confiada ao judiciário é insuficiente.[4] Em relação à União Europeia, a importância de uma autoridade independente é evidenciada desde 2001, após o protocolo adicional relativo à Convenção de

---

[1] BRASIL, ANPD. Congresso Nacional promulga a Lei nº 14.460 que transforma a ANPD em autarquia de natureza especial. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/congresso-nacional-promulga-a-lei-no-14-460-que-transforma-a-anpd-em-autarquia-de-natureza-especial#:~:text=Com%20a%20promulga%C3%A7%C3%A3o%2C%20a%20Autoridade,de%20dados%20pessoais%20no%20Pa%C3%ADs.>.

[2] BRASIL, ANPD. ANPD torna-se autarquia de natureza especial. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>. Acesso em: 26 fev. 2023.

[3] BRASIL, ANPD. O MJSP estuda mudanças normativas para o ambiente digital no Brasil. Brasília, 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-estuda-mudancas-normativas-para-ambiente-digital-no-brasil>. Acesso em: 26 fev. 2023.

[4] *"[...] un'autorità amministrativa indipendente, eventualmente dotata di poteri regolamentari di adattamento dei principi contenuti nelle clausole generali a situazioni nuove o particolari; l'esigenza di questa autorità è confermata dall'esperienza di quei paesi che non l'hanno prevista, dove si è dimostrata insufficiente la protezione affidata solo alla magistratura."* RODOTÀ, Stefano. Privacy e costruzione della sfera privata. Ipotesi e prospettive. In: Rivista Politica del Diritto, anno XXII, numero 4, pp. 521 – 546. Bolonha: Il Mulino, dezembro 1991. p. 543.

Estrasburgo de 1981, que estabeleceu a necessidade de criar autoridade independente (*Supervisory Authorities*) para efetivar a proteção de dados pessoais, tendo em vista que a Lei por si só não seria suficientemente eficaz.[1]

Nesse sentido, destaca-se que esse modelo foi adotado na Diretiva 95/46/CE como Autoridade de Controle ou *Data Protection Authorities* (DPA). Tal órgão foi mantido no Regulamento Geral de Proteção de Dados ou *General Data Protection Regulation* (GDPR), nos termos do capítulo VI, no qual dispõe sobre sua competência e poderes, bem como a necessária independência no exercício de suas funções.[2]

Conforme Doneda (2020), o contexto brasileiro apresenta que órgãos administrativos independentes foram inseridos sistematicamente na estrutura institucional do país para atender demandas regulatórias baseada em contextos relacionados com (i) setores em que o Estado operava em caráter de monopólio; (ii) a busca de maior eficiência; (iii) definição de normas técnicas. De forma respectiva, convém citar os seguintes exemplos: Agência Nacional de Telecomunicações (ANATEL); (ii) Conselho Administrativo de Defesa Econômica (CADE); (iii) Agência Nacional de Vigilância Sanitária (Anvisa).

Nesse sentido, ressalta-se que no Brasil as agências reguladoras são entes da administração pública indireta, constituída na modalidade de autarquia de regime especial. Tratam-se de órgãos independentes, mesmo sendo vinculados ao Ministério competente para tratar da respectiva atividade.[3]

Diante disso, revela-se que a ANPD se equipara às agências reguladoras, tendo em vista que tais órgãos possuem plena autonomia político-administrativa e econômico-financeira. Por outro lado, Fabrício Alves ressalta que a Lei das Agências Reguladoras (LAR) não se aplica à ANPD, uma vez que a Autoridade não assume qualidade de agência, ainda que seja autarquia em regime especial.[4]

Nesse sentido, convém citar que a MP nº 1.124 de 2022 expressa a intenção da Presidência em não submeter a ANPD ao regime jurídico da LAR. Isso é evidente, pois

[1] LIMA, Cíntia Rosa Pereira de. Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados. (Coleção teses de doutoramento). Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584936397. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 24 jan. 2023.
[2] *Ibidem.*
[3] *Ibidem.*
[4] ALVES, Fabrício M. ANPD como autarquia federal: o que muda para a proteção de dados no Brasil? Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/anpd-como-autarquia-federal-o-que-muda-para-a-protecao-de-dados-no-brasil-14062022>. Acesso em: 26 fev. 2023.

identificam-se alguns pontos de diferenças: (i) para a ANPD, o prazo de mandato dos diretores permanece sendo 4 anos, permitida recondução, enquanto para Agências é de 5 anos, não permitida a recondução; (ii) mais requisitos para indicação de nomes para cargos pela LAR do que pela LGPD; e (iii) entre as estruturas e os funcionamentos das ouvidorias previstas na LGPD e na LAR. Sendo assim, diante da ausência de denominar a ANPD como agência e do estabelecimento de tais critérios distintos, conclui-se a inequívoca intenção executiva em torná-la em autarquia especial (ALVES; VALADÃO, 2022).

Conforme Márcio Iorio Aranha (2018), instituições de regulação surgiram como mecanismos reguladores normativos. O autor ressalta que tal contexto faz parte do processo descentralizador da Administração Pública, o que evidencia a independência como características dos entes reguladores. Nesse sentido, Lucas Rocha Furtado (2016) considera que mecanismos de descentralização administrativa possibilitam ao poder público buscar novas formas para que as novas demandas do Estado sejam atendidas. Conforme João Pedro Carvalho (2020), a dissociação do poder público e a função regulatória originou a estruturação de agências reguladoras como autarquias em regime especial com personalidade jurídica própria.

Evidencia-se que não é novidade ao ordenamento brasileiro a criação de órgão independente da estrutura administrativa tradicional. Conforme Doneda (2020), a necessidade de tais órgãos se refere à atividade marcada pela especificidade e caráter técnico do setor; além disso, destaca-se que uma crescente complexidade das relações sociais e da organização do Estado demandam por órgãos que respondam às necessidades de forma direta e dinâmica, o que é relevante como autoridade de garantia na defesa e promoção dos direitos do cidadão.

Diante disso, revela-se que a independência dessas autoridades é importante, pois a sua competência envolve fiscalizar agentes de tratamento públicos ou privados. Destaca-se que a independência da ANPD reflete (i) na tutela do cidadão; (ii) na estruturação do sistema normativo de proteção de dados; (iii) na segurança jurídica por meio da uniformização da interpretação e aplicação da lei; (iv) no equilíbrio concorrencial para evitar vantagens competitivas em relação às empresas que eventualmente não cumprem a LGPD; (v) nas medidas regulatórias que envolve fomento de boas práticas e regime sancionatório próprio; e (vi) na publicação de opiniões e decisões que diminui a assimetria entre os cidadãos e os agentes de tratamento (DONEDA, 2021).

Sobretudo, destaca-se que o reconhecimento da necessária independência da Autoridade está alinhado com políticas e programas governamentais que visam (i) estabelecer

facilidades do comércio internacional; (ii) fomentar a competitividade; e (iii) impactar a sociedade e empresas.[1] Tais objetivos são enfatizados no texto da Exposição de Motivos Interministerial (EMI) nº 00141/2022 ME CC, de 7 de junho de 2022, que acompanhou a MPV nº 1.124/2022.

A exposição de motivos subscrita pelos Ministros de Estado da Economia e da Casa Civil ressalta a necessidade de redimensionar e fortalecer a ANPD em relação à sua estrutura, quadro pessoal, processos e orçamento. Assim, fez-se necessário alterar o nível da autonomia da Autoridade de forma coerente, satisfatória e adequada, diante do crescente nível de exigência da sociedade nacional e internacional referente à proteção de dados pessoais.[2]

Nesse sentido, revela-se que a criação de uma autarquia assegura a autonomia administrativa. Isso é evidenciado pelos destaques listados na exposição de motivos interministerial, uma vez que tal transformação proporciona

> (i) maior confiabilidade no sistema regulatório brasileiro de proteção de dados; (ii) maior compatibilidade frente a outros regimes regulatórios semelhantes; (iii) harmonização internacional, com benefícios potenciais para a economia de dados brasileira, bem como para garantir maior segurança e soberania nacional dos dados pessoais dos cidadãos brasileiros; (iv) maior possibilidade de ingresso em blocos econômicos e organismos internacionais de relevância; e (v) maior protagonismo brasileiro na economia digital e em proteção de dados em âmbito nacional e internacional (BRASIL, 2022).

A exposição de motivos interministerial também destacou que a autonomia da ANPD aumenta com a transformação da sua natureza jurídica. Isso é relevante, tendo em vista o protagonismo brasileiro na economia digital e na proteção de dados em âmbito nacional e internacional. Sobretudo, reconhece-se que o maior grau de independência da Autoridade é fundamental para que a legislação brasileira cumpra o papel de viabilizar o ambiente aberto ao recebimento e envio de dados pessoais para além das fronteiras.[3]

---

[1] BRASIL. ANPD. ANPD torna-se autarquia de natureza especial. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>.
[2] BRASIL. Ministério da Economia; Casa Civil. Exposição de Motivos Interministerial (EMI) nº 00141/2022 ME CC, de 7 de junho de 2022. Brasília, 2022. Disponível: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Exm/Exm-Mpv-1124-22.pdf>.
[3] *Ibidem.*

Os impactos decorrentes da independência e autonomia da ANPD são positivos ao ecossistema caracterizado pelo intenso fluxo de dados pessoais. Assim, destaca-se que tais impactos podem proporcionar (i) compatibilidade com regimes regulatórios internacionais; (ii) alinhamento com boas práticas; (iii) aprimoramento da condição do Brasil para o ingresso em organismos e blocos internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE).[1]

Conforme destacado na exposição de motivos interministerial, a transformação da ANPD permite o emprego de maiores ferramentas para a inserção das empresas brasileiras na economia digital internacional. Além disso, torna-se possível que o Brasil ocupe papel relevante nas discussões internacionais da América Latina, bem como do norte global.[2]

Certamente, a transformação da natureza jurídica da ANPD eleva a reputação e a credibilidade internacional do Brasil. Conforme Danilo Doneda (2021), a independência da ANPD é fundamental para que o país obtenha vantagens econômicas e políticas derivadas da LGPD, o que abrange "*a obtenção da adequação europeia, que garantiria o livre fluxo de dados pessoais entre o Brasil e os países do bloco, depende inexoravelmente do estabelecimento de uma autoridade independente*" (DONEDA, 2021, p. 473).

Nesse sentido, Doneda (2021) alerta que o comércio internacional apresenta requisitos concretos relativos à proteção de dados pessoais. Dentre tais requisitos, destaca-se a independência da autoridade nacional de proteção de dados, o que facilita que empresas ou órgãos brasileiros possam participar do fluxo internacional de dados. Exemplo disso é a previsão do Regulamento Geral de Proteção de Dados que inclui a Autoridade Nacional independente como uma das condições para autorizar a transferência internacional de dados pessoais (LEONARDI, 2021).

O autor exemplifica tal facilidade com o acordo entre a União Europeia e o Japão. A partir do estabelecimento de uma autoridade independente pelo Japão, as empresas japonesas tiveram acesso a um mercado de mais de quinhentos milhões de consumidores, o que evidencia a consolidação da "*maior área de livre fluxo de dados do mundo*" (DONEDA, 2021, p. 473).

---

[1] BRASIL. ANPD. ANPD torna-se autarquia de natureza especial. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>.

[2] BRASIL. Ministério da Economia; Casa Civil. Exposição de Motivos Interministerial (EMI) nº 00141/2022 ME CC, de 7 de junho de 2022. Brasília, 2022. Disponível: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Exm/Exm-Mpv-1124-22.pdf>.

Na América do Sul, Argentina e Uruguai possuem o reconhecimento da adequação em relação à proteção de dados pessoais, nos termos do Regulamento Geral de Proteção de Dados da União Europeia. No caso do Brasil, destaca-se que o nível de adequação do arcabouço normativo será avaliado pela Comissão da União Europeia conforme os seguintes critérios em relação à ANPD: (i) independência estrutural e organizacional; e (ii) exercício, atribuições e poderes da Autoridade sem intervenções indevidas, desde que seja capaz de monitorar atividades de entes estatais e privados (TEFFÉ; MAGRANI; VIOLA, 2018).

Diante disso, ressalta-se que um dos critérios de avaliação do nível adequado de proteção de dados pessoais é a presença de uma autoridade independente. Essa avaliação envolve comumente contextos de critérios que permitem a transferência internacional de dados, por isso as Autoridades devem ter poderes de investigação e intervenção relativas às regras de proteção de dados pessoais e às atividades realizadas pelos agentes de tratamento (MARQUES; AQUINO, 2021).

Ademais, Fabrício Alves destaca a importância da transformação da ANPD como órgão independente da Presidência da República que outrora era pertencente à administração pública direta. O autor ressalta que a manutenção da Autoridade na antiga condição poderia submetê-la a constantes questionamentos jurídicos, bem como ter suas punições administrativas anuladas em processos no âmbito da Justiça Federal em que os entes públicos se apresentassem na qualidade de sancionados.[1]

Evidencia-se, portanto, que a independência consolidada pela transformação da natureza jurídica da ANPD é fundamental para o exercício de suas respectivas funções e competências. Além disso, é um marco importante para efetivar a proteção de dados pessoais, tendo em vista que a nova autarquia possui condição jurídica e administrativa para instituir unidades regionais no território brasileiro, o que é possível ampliar atuação regulatória, contenciosa administrativa ou judicial de forma expressiva e independente em relação aos entes privados ou públicos.

[1] ALVES, Fabrício M. ANPD como autarquia federal: o que muda para a proteção de dados no Brasil? Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/anpd-como-autarquia-federal-o-que-muda-para-a-protecao-de-dados-no-brasil-14062022>. Acesso em: 26 jul.. 2023.

Considerações Finais

Diante do exposto e do ordenamento brasileiro, evidencia-se que a independência da Autoridade Nacional de Proteção de Dados (ANPD) é assegurada pelo regime autárquico especial, uma vez que a natureza jurídica das autarquias é caracterizada pela autonomia administrativa. Nesse sentido, a transformação da natureza jurídica da ANPD foi importante para garantir a independência da Autoridade, bem como as demais repercussões positivas do crescente grau de autonomia.

Evidenciou-se que a consideração sobre a necessidade da independência e autonomia da ANPD esteve presente desde os debates iniciais do Anteprojeto da Lei de Proteção de Dados Pessoais no Brasil. Porém, os principais impasses para tal consolidação se referem a questões orçamentárias, o que abrange competência restrita ao Presidente da República, isso resultou no veto da criação da ANPD, diante do cenário em que a LGPD ainda não era vigente. Posteriormente, a Autoridade foi criada com vínculo à Presidência da República por meio da MP nº 869, o qual apresentou modificações na redação da redação vetada, o que manteve certa insegurança jurídica que se estendia desde o veto.

Diante disso, foi oportuno demonstrar os marcos cronológicos da ANPD, o que permitiu identificar atos normativos que empregaram um caminho gradativo para a consolidação de uma Autoridade independente conforme regime autárquico especial. Nesse sentido, foi possível enfatizar a importância da Lei nº 13.853/2019 que abriu o caminho para a MPV nº 1.124/2022 e proporcionou a transformação da ANPD em autarquia especial, por meio da Lei nº 14.460/2022.

Por fim, ressalta-se que a importância da transformação da ANPD em autarquia especial consiste justamente na consolidação de uma instituição independente para exercer suas competências legais e regulatórias. Nesse contexto, a importância de tal natureza é elevada pelos impactos positivos que a Autoridade independente proporciona, dos quais podem se destacar (i) o fortalecimento da proteção de dados pessoais; (ii) a melhora da credibilidade e reputação aos entes internacionais; (iii) o fomento à cooperação internacional; (iv) o protagonismo na economia digital aberta com fluxo transfronteiriço de dados pessoais; e (v) a independência funcional, orçamentária e administrativa para estabelecer suas próprias prioridades e fiscalizar os agentes de tratamento, inclusive o Poder Público.

Referências bibliográficas

ALVES, Fabrício M. ANPD como autarquia federal: o que muda para a proteção de dados no Brasil? Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/anpd-como-autarquia-federal-o-que-muda-para-a-protecao-de-dados-no-brasil-14062022>.

ARANHA, M. I. Manual de Direito Regulatório: Fundamentos de Direito Regulatório. 4. ed. rev. ampl. London: Laccademia Publishing, 2018.

ALVES, Fabrício da Mota; VALADÃO, Rodrigo Borges. ANPD: Agência reguladora ou autoridade reguladora independente? Disponível em: <https://www.migalhas.com.br/coluna/dados-publicos/369257/anpd-agencia-reguladora-ou-autoridade-reguladora-independente>. Acesso em: 26 jul. 2023.

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

BRASIL. Lei 13.853, no dia 08 de julho de 2019. *Diário Oficial da União.* Brasília, DF, 08, Jul. de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

BRASIL. Lei nº 14.460, de 25 de outubro de 2022. *Diário Oficial da União.* Brasília, DF, 25, Out. de 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

BRASIL. Portaria nº 11, de 27 de Janeiro de 2021. *Diário Oficial da União.* Brasília, DF, 28, Jan. de 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>.

BRASIL, ANPD. O MJSP estuda mudanças normativas para o ambiente digital no Brasil. Brasília, 2022. Disponível em:

https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-estuda-mudancas-normativas-para-ambiente-digital-no-brasil>.

BRASIL, ANPD. ANPD torna-se autarquia de natureza especial. Brasília, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial>.

BRASIL, ANPD. ANPD comemora aniversário de dois anos. Brasília, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-comemora-aniversario-de-dois-anos>.

BRASIL, ANPD. ANPD publica Agenda Regulatória 2023-2024. Brasília, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024>.

BRASIL, ANPD. Nota de Apoio à Conversão da MPV nº 1.124/2022. Brasília, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/cnpd-2/nota-de-apoio-a-conversao-da-mpv-1-124-2022>.

BRASIL, ANPD. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade visita nova sede da ANPD. Brasília, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/cnpd-2/nota-de-apoio-a-conversao-da-mpv-1-124-2022>.

BRASIL, ANPD. Congresso Nacional promulga a Lei nº 14.460 que transforma a

ANPD em autarquia de natureza especial. Brasília, 2022. Disponível em:

<https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/congresso-nacional-promulga-a-lei-no-14-460-que-transforma-a-anpd-em-autarquia-de-natureza-especial#:~:text=Com%20a%20promulga%C3%A7%C3%A3o%2C%20a%20Autoridade,de%20dados%20pessoais%20no%20Pa%C3%ADs.>.

BRASIL, ANPD. ANPD e Ministério da Justiça e Segurança Pública editam portaria conjunta. Brasília, 2023. Disponível em:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ministerio-da-justica-e-seguranca-publica-editam-portaria-conjunta>.

BRASIL, Câmara dos Deputados. Promulgada lei que transforma Autoridade Nacional de Proteção de Dados em autarquia. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9205606&ts=1667313945386&disposition=inline>.

BRASIL. Ministério da Economia; Casa Civil. Exposição de Motivos Interministerial (EMI) nº 00141/2022 ME CC, de 7 de junho de 2022. Brasília, 2022. Disponível: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Exm/Exm-Mpv-1124-22.pdf>.

BRASIL, Senado Federal. Parecer nº 309 de 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9205606&ts=1667313945386&disposition=inline>.

CARVALHO, J. P. A. L. da F. A natureza jurídica da Autoridade Nacional de Proteção de Dados à luz da Teoria do Estado Regulador. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, nº 2, p. 118-132, outubro de 2020.

FURTADO, L. R. Curso de Direito Administrativo. 5ª ed., rev. e atual. Belo Horizonte: Fórum, 2016.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In:* BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Grupo GEN, 2021. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais [livro eletrônico] : elementos da formação da Lei Geral de Proteção de Dados / Danilo Cesar Maganhoto Doneda. -- 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020.

LEONARDI, Marcel. Transferência Internacional de Dados Pessoais. In: BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Grupo GEN, 2021. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/.

LIMA, Cíntia Rosa Pereira de. Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados. (Coleção teses de doutoramento). Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584936397. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 24 fev. 2023.

APLICAÇÃO DA LGPD AO USO DE COOKIES E O GUIA ORIENTATIVO PARA COOKIES E PROTEÇÃO DE DADOS DA ANPD

Paulo Ricardo da Silva Santana[1]

Resumo: Este artigo tem o objetivo de analisar a aplicação da LGPD ao uso de *cookies*, abordando o Guia Orientativo para *Cookies* e Proteção de Dados publicado pela ANPD. O ponto de partida foi uma revisão bibliográfica sobre *cookies* para *Web*, rastreamento e proteção de dados. Em seguida, foi realizada uma análise do Guia Orientativo para *Cookies* e Proteção de Dados da ANPD e de disposições da LGPD, em perspectiva comparada com normas de proteção de dados internacionais, em especial do sistema europeu. Diante de um cenário em que *banners* de *cookies* passaram a dominar os sites eletrônicos após a difusão de normas de proteção de dados, muitas vezes sem a observação de determinações legais, observou-se que o Guia representa um importante passo para contribuir com a proteção dos direitos e a privacidade de titulares de dados pessoais.

Palavras-chave: *cookies*; *Web*; consentimento; rastreamento; privacidade; LGPD

Abstract: *This paper aims to analyze the application of the LGPD to the use of cookies by addressing the Guidance for Cookies and Data Protection published by the ANPD. The starting point was a literature review on web cookies, tracking and data protection. Then, an analysis of the Guidelines for Cookies published by the ANPD and provisions of the LGPD in comparison with international data protection standards, in particular the European system. In a scenario in which cookie banners have dominated electronic sites after the dissemination of data protection rules, often without complying with legal determinations, one could note that the Guide represents an important step towards the protection of human rights and the privacy of the data subjects.*

[1] Paulo Ricardo da Silva Santana é graduado em Sistemas de Informação pelo Centro Universitário do Distrito Federal (UDF) e em Direito pela Universidade de Brasília (Unb). Coordenador de Pesquisa do Observatório da LGPD/Unb. Membro da comissão de Privacidade e Proteção de Dados da OAB/DF. Advogado e Consultor em Proteção de Dados em FdS Advogados.

Keywords*: *cookies; Web; consent; tracking; privacy; LGPD

Introdução

Durante os anos 2000, a Internet se transformou em uma plataforma provedora de serviços digitais, a Web 2.0.[2] Motores de otimização de busca, serviços de música, serviços de compra e venda e redes sociais tornaram a Internet um terreno rico em matéria-prima gratuita para a tradução da experiência humana em dados comportamentais,[3] originando o que Shoshana Zuboff denomina de superávit comportamental humano.[4]

Esse processo começou ainda nos primeiros anos da *Web*, em meados dos anos 90, quando *cookies* para internet foram inventadas por Lou Montulli, com o propósito de resolver um problema essencial: as páginas da *Web* não tinham a capacidade de lembrar do usuário após o fim de uma interação. Ao solucionarem o problema de "memória" dos protocolos de comunicação da *Web*, os c*ookies* acabaram possibilitando a ampliação do fluxo informacional e do processo de tradução da experiência humana do mundo real para o virtual, iniciando a produção de uma vastidão de dados, vistos como petróleo pelas agências de publicidade da época.

Nos primeiros anos, nenhum usuário comum que navegasse pelas páginas da *Web* teria como saber que os *cookies* estavam lá no seu dispositivo coletando seus dados pessoais. Quando foram notados em 1996, o desafio inicial foi entender seu funcionamento e os riscos envolvidos para os titulares de dados. Em que pese tenham ajudado a melhorar a experiência do usuário na *Web*, os *cookies* também viabilizaram formas de rastreamento do usuário desenfreadas e até ilegais com sérias consequências para os titulares de dados pessoais.

A expansão relativamente recente das normas de proteção de dados impôs aos agentes de tratamento o dever de adequação de suas aplicações digitais. O resultado foi uma enxurrada de *banners* informativos sobre c*ookies*. Na prática, foi possível verificar que as adequações nem sempre foram empenhadas de forma legítima ou efetiva à salvaguarda dos direitos dos titulares.

---

[2] O'REILLY, Tim. *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. O 'Reilly, 30 de set. 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1. Acesso em: 24 de jan. 2023

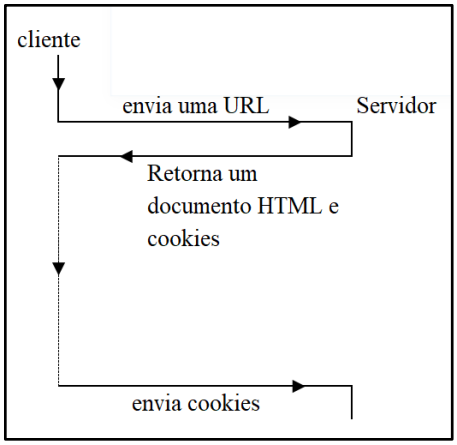
[3] ZUBBOF, Shoshana. A Era do Capitalismo de Vigilância. 1 ed. Editora Intrínseca, 2021. p.18

[4] Ibid. p.114

Nesse recorte, este artigo tem o objetivo de analisar as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD) aplicáveis aos *cookies*, abordando o Guia Orientativo para *Cookies* e Proteção de Dados publicado pela ANPD em 2022. Considerando o tema exposto, a principal pergunta de pesquisa deste trabalho é: Qual é o impacto do referido guia? Para responder à questão principal, será realizada uma breve reflexão sobre a relevância dos *cookies* na *Web* e como eles se relacionam com a privacidade e a proteção de dados.

1. Sobre os cookies

Quem sabe se os *cookies* tivessem sido inventados por um programador brasileiro eles não se chamassem cafezinho? A lógica do *cookie* é a mesma do cafezinho: algo que se oferece quando alguém faz uma visita.[5] De maneira bem resumida, o internauta, ao visitar um *site* eletrônico, recebe um pequeno pedaço de código que armazena algumas de suas informações que podem ser posteriormente enviadas de volta ao servidor onde o site está hospedado.



Fonte: Autor, adaptado de MONTULLI (2007)

[5] Em 2002, Andrew Stuart, do portal Domino Power, publicou um artigo investigando o porquê dos *cookies* se chamarem assim. Após enviar um e-mail a Lou Montulli, ele recebeu a resposta de que os cookies foram nomeados em homenagem a um termo típico da Ciência da Computação: "*magic cookies*". Veja mais em: STUART, Andrew. *Where cookie comes from*. Domino Power, 1 de jul. 2002. Disponível em: http://dominopower.com/article/where-cookie-comes-from. Acesso em: 24 de fev. 2023; STEVEN, Johnson. *The Magic Cookie: How Lou Montulli Cured The Web's Amnesia*. The Hidden Heroes. Disponível em: https://hiddenheroes.netguru.com/lou-montulli. Acesso em: 08 de fev. 2023.

As informações compartilhadas entre a origem e o destino são denominadas "informações de estado",[6] o que pode incluir dados diversos, como nomes de usuários, *login*, produtos selecionados em uma loja virtual, páginas visitadas anteriormente e outros relacionados à interação que ocorre entre o internauta e o *site* visitado.

No mundo real, se um cliente for ao supermercado e por qualquer motivo precisar largar tudo e sair, os produtos ficarão no carrinho de compras e serão posteriormente devolvidos às prateleiras. Ocasionalmente, quando tiver que fazer compras, o cliente terá que procurar pelos produtos novamente. Nesse quesito, não era tão diferente fazer compras na *Internet* antes da existência dos *cookies*. Se tivesse que interromper rapidamente a sessão ou enfrentasse qualquer falha na conexão, o internauta teria que reiniciar o processo. Quando idealizou os *cookies*, Lou Montulli pensou em uma forma de contornar problemas como esse.

Embora possa parecer que a *Web* não se importasse com compradores digitais, a verdade é que naquela época a falta de armazenamento de dados dos internautas era uma característica comum. Os navegadores "não possuíam memória" e isso gerava diversos problemas. Por exemplo, um usuário que escolhesse o idioma em uma página multilíngue perderia suas preferências ao clicar em um novo *link*. Além disso, sem informações sobre os usuários, era impossível contar a quantidade de visitantes de uma página.[7]

Entretanto, havia outras implicações de grande relevância: segurança e privacidade. A *Web* teve suas primeiras versões desenvolvidas no renomado CERN, *European Organization for Nuclear Research* (Organização Europeia para Pesquisa Nuclear),[8] visando a possibilitar o compartilhamento de informações entre cientistas por universidades e institutos em todo o mundo.[9] Seu projeto inicial descrevia um "projeto de hipertexto" chamado "WorldWideWeb" no qual uma "teia" de "documentos de hipertexto" poderia ser visualizada por "navegadores".[10]

---

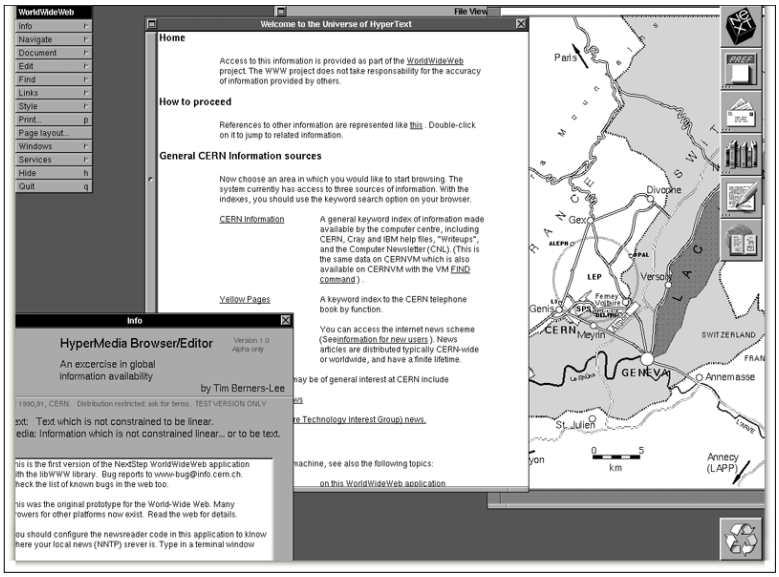
[6] Conforme detalhado na patente dos cookies, "*estado de cliente persistente em um sistema cliente-servidor baseado em protocolo de transferência de hipertexto, de n.º US 20070185978A1: "Um método e aparelho para transferir informações de estado entre um sistema de computador servidor e um sistema de computador cliente*." Ver mais em: MONTULLI, Lou. *Persistent Client State In A Hypertext Transfer Protocol Based Client-Server System*. US 20070185978A1. 9 de ago. 2007. United States Patent and Trademark Office. Palo Alto: USPTO, 2007. p. 1.

[7] Um departamento com uma estação de acesso com um identificador único, como o IP (*Internet Protocol*), poderia ter vários usuários acessando um determinado conteúdo em um servidor *Web*. A identificação por IP não resolveria o problema.

[8] *European Organization for Nuclear Research* (Organização Europeia para Pesquisa Nuclear).

[9] CERN. *A short history of the Web*. Disponível em: https://home.cern/science/computing/birth-web/short-history-web. Acesso em: 21 de fev. 2023.

[10] Ibid. n.p.



Fonte: CERN (1993)[11]

No entanto, como os navegadores não guardavam informações sobre os visitantes das páginas eletrônicas, era como alguém entrando em sua casa sem que fosse possível ter qualquer ideia de quem estava fazendo a visita. Sob essas condições, ainda era perfeitamente possível o acesso a informações privilegiadas por um visitante sem permissão.

Para garantir a segurança da conexão entre o visitante e o servidor, é fundamental que haja uma conexão segura e que informações mínimas sobre a origem e o destino da conexão sejam compartilhadas. Em seu documento de patente sobre os *cookies*, Montulli propôs um método de chamada no qual o computador cliente transmitia informações somente por meio de um canal seguro de comunicação ao servidor de destino. Dessa forma, a segurança da conexão seria preservada e o risco de interceptação de dados sensíveis seria reduzido.[12]

Mais de vinte anos após sua invenção vir ao mundo em entrevista ao portal *The Hidden Heroes*, Montulli esclareceu que um dos objetivos dos *cookies* era dar mais segurança e privacidade ao usuário.[13] Em outra entrevista, Montulli explicou que havia uma desconfiança

[11] Captura de tela registrada em 1993 da página *Web* do CERN em que os cientistas utilizavam para consultar informações úteis. Ver mais em: CERN. *Tim Berners-Lee's original World Wide Web browser*. Disponível em: http://info.cern.ch/NextBrowser.html. Acesso em: 21 de fev. 2023.

[12] Item 25 do parágrafo [0120]. "*The method of claim 13, wherein a state object specifies if it is a secure state object, and wherein if a state object is secure, then said client computer system only transmits said secure state object over a secure communication channel to said server*." Ver mais em: MONTULLI, Lou. Op. Cit.,2007. p. 17.

[13] "*That information would be accessible only to you and the specific web server you were interacting with. The cookie served to you by the Yahoo web server would only be visible to Yahoo. If you went to another site - say Wired.com- they could create their own cookie to give you a persistent identity on their site, but they'd have no*

do Governo na época. Então, para solucionar alguns problemas da *Web*, era preciso desenvolver um mecanismo que permitisse que o internauta pudesse **ser lembrado sem ser rastreado**.[14]

Embora os objetivos de dar mais segurança e privacidade ao usuário não tenham sido declarados na submissão da patente dos *cookies*,[15] nos anos seguintes ao da invenção, Montulli seguiu trabalhando nessa questão ao propor *Request For Comment 2119*[16] de 1997 (RFC 2119/97), em que foi submetida uma proposta de *Protocolo de rastreamento de padrões da Internet*.[17]

Dentre as várias diretrizes propostas, a RFC 2119/97 estabelecia tópicos direcionados para o aumento da privacidade do usuário de *Internet*, como regras de comunicação entre o computador do internauta e o servidor; recomendações sobre segurança; e privacidade. A RFC 2119 também propôs direitos para os usuários de *Internet*, como o de aceitar ou rejeitar *cookies*.[18]

Se, de fato, a intenção jamais tivesse sido rastrear os usuários, isto só ficou claro com a RFC 2119/97. Contudo, esta RFC já surgiu após um cenário de desconfiança sobre o que os *cookies* poderiam fazer e em um contexto em que as discussões sobre privacidade *online* já tomavam forma. Os *cookies* estavam em pleno funcionamento e praticamente despercebidos pelos usuários, quando o jornalista Tim Jackson publicou uma matéria sobre o que de fato eram os *cookies* e para que serviam, despertando o debate a respeito de questões relacionadas à privacidade dos usuários de *Internet* em razão dos *cookies*.[19]

---

way of detecting the existence of the Yahoo cookie.". Ver mais em: STEVEN, Johnson. *The Magic Cookie: How Lou Montulli Cured The Web's Amnesia*. The Hidden Heroes, Disponível em: https://hiddenheroes.netguru.com/lou-montulli. Acesso em: 08 de fev. 2023.

[14] KIHN, MARTIN. Lou Montulli: *The Man Who Invented the Cookie*. Martin Kihn, 21 de out. 2019. Disponível em: https://martinkihn.com/2019/10/21/lou-montulli-the-man-who-invented-the-browser-cookie. Acesso em: 23 de fev. 2023

[15] Nos parágrafos [010] a [015] Montulli resume as possibilidades de aplicação da sua invenção. Nada é mencionado sobre privacidade. O termo privacidade sequer aparece nos 20 parágrafos descritivos da invenção.

[16] As RFC's, *Requests For Comments* (Solicitações de Comentários) são uma forma de fomentar discussão e de obter sugestões de melhorias em determinadas tecnologias. São documentos técnicos. De peso relevante, elas costumam ser adotadas como normas de padronização. A RFC 2119/97 se tornou obsoleta por RFC's posteriores: RFC's 2965/2000 e 6265/2011.

[17] MONTULLI, Lou. KRISTOL, David. *HTTP State Management Mechanism*. RFC 2109. Standards Track, fev. de 1997. Disponível em: https://www.rfc-editor.org/rfc/rfc2109. Acesso em: 22 fev. 2023.

[18] Em relação ao direito do internauta de rejeitar os *cookies* no seu computador, o servidor não deveria armazenar as informações. É o disposto no item 4.3.2 da RFC 2119/97: *To prevent possible security or privacy violations, a user agent rejects a cookie (shall not store its information)* […]; Ibid. n.p.

[19] JACKSON, *Tim. This bug in your PC is a smart cookie*. Financial Times, London, Week n. 7, n. 32.906, 12 de fev. 1996. *Companies & Markets*, p. 15.

Pouco tempo após a publicação de Tim Jackson, a *Federal Trade Commission – FTC*, agência americana de defesa da concorrência e proteção do consumidor, que já vinha desde 1995 promovendo encontros para discutir a privacidade *online*,[20] no *workshop* "*Consumer Privacy on the Global Information Infrastructure"*, tratou de temas como práticas de *sites* relacionados à coleta, uso e transferência de informações pessoais, esforços auto regulatórios e desenvolvimento tecnológico para aumentar a privacidade dos consumidores; esforços educacionais para consumidores e empresas; o papel do governo na proteção da privacidade das informações *online*; e questões especiais levantadas pela coleta *online* e uso de informações sobre crianças.[21]

A preocupação geral da FTC era com a publicidade direcionada para crianças, e um tipo particular de *cookies* que veremos adiante, os *cookies* de terceiros, chamaram atenção nos debates que se seguiram[22] e que culminaram na elaboração do *Children's Online Privacy Protection Act – COPPA*.[23]

Tim Jackson terminou assim o seu artigo no *Financial Times*: *"o único consolo é que é improvável que as violações de privacidade usando essa tecnologia tenham consequências de vida ou morte. Afinal, a pior coisa que a maioria das empresas fará é tentar vender algo para você"*.[24] Certo que, naquela época, talvez fosse difícil prever o impacto que os *cookies* gerariam na *Internet* e no mundo real, ajudando a inaugurar uma nova era para a sociedade, fortemente marcada pela vigilância, hábil em converter a experiência humana em matéria prima gratuita para práticas comerciais dissimuladas de extração, previsão e venda.[25]

A tecnologia que foi supostamente concebida com a promessa de dar mais segurança e privacidade ao usuário foi a mesma que possibilitou, às gigantes da tecnologia, o rastreamento

---

[20] FEDERAL Trade Commission. *Privacy Online: A Report to Congress*. FTC, jun. 1998. p.1.

[21] FEDERAL Trade Commission. *Prepared statement of the Federal Commission on Internet Privacy before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary United States House of Representatives*. FTC, 26 de mar. 1998. Disponível em: https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-internet-privacy/privacy.pdf. Acesso em: 26 de fev. 2023. n.p.

[22] FEDERAL Trade Commission. *Privacy online: Fair Information practices in the electronic marketplace*. FTC, mai. 2000. p.21

[23] A *Children's Online Privacy Protection* Act é uma lei federal americana de 1998 que impõe certos requisitos aos operadores de *sites* ou serviços *online* direcionados a crianças menores de 13 anos de idade e aos operadores de outros *sites* ou serviços *online* que tenham conhecimento real de que estão coletando informações pessoais *online* de uma criança menor de 13 anos. Ver mais em: COPPA. 15 U.S.C. §§ 6501-6506. *Children's Online Privacy Protection Act*. 21 de abr. de 2000. Disponível em: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. Acesso em: 26 de fev. 2023.

[24] JACKSON, Tim. Op. Cit., 1996. p. 15.

[25] ZUBBOF, Shoshana. *A Era do Capitalismo de Vigilância*. 1 ed. Editora Intrínseca, 2021. p.7.

massivo do comportamento dos usuários, visando aos aumentos dos ganhos de capital por meio da violação sistemática de sua privacidade, confirmando a afirmação de Stefano Rodotà de que a *Internet* se apresenta cada vez mais claramente como uma trama de possibilidades ainda não resolvidas, como um conjunto de promessas contraditórias: no caso dos *cookies*, coleta e compartilhamento de informações pessoais oferecendo mais segurança e privacidade.[26]

1.1. Rastreamento

Os *cookies* nasceram para facilitar (**i**) o gerenciamento de sessão – classificados como necessários – e para (**ii**) a personalização da experiência do usuário durante a navegação, classificados como não necessários. Todavia, as empresas de publicidade foram rápidas em utilizar essa tecnologia para captar o comportamento dos usuários de *Internet* e utilizar essas informações para aumentar os ganhos de capital por meio da definição e análise de perfis comportamentais. Assim, surgiram *cookies* com a finalidade de (**iii**) rastreamento. Esses são basicamente os tipos de *cookies* existentes, que podem ainda ser classificados quanto à origem: (**1**) *cookies* primários ou; (**2**) de terceiros.[27] Enquanto os primários se reportam ao servidor de origem, os de terceiros enviam informações para servidores diferentes da página acessada. Exatamente por isso, são muito utilizados para publicidade.

Há ainda uma classificação relevante que diz respeito ao seu tempo de duração: os *cookies* de (**a**) sessão ou (**b**) persistentes.[28] Os de sessão duram enquanto a interação do usuário com a página acessada durar. Os persistentes, por sua vez, só são eliminados após a data prevista para expirar, ou seja, persistem por um tempo determinado.

Compreender essas diferenças nos permite direcionar mais adequadamente as reflexões atinentes à problemática em torno dessas tecnologias. Grande parte dessa problemática gravita em torno dos *cookies* de terceiros, do tipo persistente, usados com a finalidade de rastreamento dos usuários. Aliás, foram *cookies* dessa natureza, com uma perigosa adaptação, que foram

---

[26] RODOTÀ, Stefano. *A vida na sociedade da vigilância - A privacidade hoje* / Stefano Rodotà – Organização, seleção e apresentação de Maria Celina Bodin de Moraes. – Rio de Janeiro: Renovar, 2008. p. 169;
[27]MOZILLA. Cookies HTTP. https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Cookies#rastreamento_e_privacidade. Acesso em: 08 de Mar. 2023.
[28] MOZILLA. Cookies HTTP. https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Cookies. Acesso em: 08 de Mar. 2023.

largamente utilizados pela gigante das telecomunicações americana, a Verizon, em um escândalo de rastreamento de milhões de pessoas, reportando por Robert McMillan em 2014.[29]

Desenvolvidos pela Turn Inc,[30] os *cookies* utilizados pela Verizon ficaram conhecidos como "*cookies zumbis*", "*perma-cookie*" ou ainda "*supercookies*", em razão de serem um tipo de *cookie* que "volta a vida", mesmo após ter expirado ou ter sido apagado do computador do usuário. A finalidade era, de forma oculta, rastrear o usuário. A questão chegou à FTC,[31] que entendeu o caso como violação do *Federal Trade Commission Act* e, dentre várias terminações, impôs à Turn Inc o dever de informar os usuários sobre os dados coletados e de fornecer mecanismo para que os usuários pudessem rejeitar a coleta de dados (*opt-out*).[32]

"*Hoje, a tecnologia criou balas de prata que permitem às empresas atingir as pessoas individualmente. A longo prazo, isso é bom, pois adaptará a publicidade mais de acordo com o que o consumidor deseja.* " Embora não pudesse entender completamente na época os riscos em torno do rastreamento por *cookies*, Jackson de alguma forma anunciava o que estava por vir: o uso massificado dessa tecnologia por empresas de publicidade.

Para entender como chegamos a esse ponto, é preciso também entender que, grosso modo, uma página *Web* é como uma teia de vários *links* atrelados a alguma outra página ou serviço.[33] Esses *links* podem conter referências a imagens e arquivos de *sites* em outros servidores.[34] Por essa razão, é ainda muito comum acessar uma página qualquer da *Web* e visualizar *banners* com propagandas que direcionam para outros provedores. E foi com base nessa característica essencial da *Web*, que os *cookies* de terceiros surgiram.

---

[29] MCMILLAN, Robert. *Verizon's 'Perma-Cookie' Is a Privacy-Killing Machine*. WIRED, 27 de out. 2014. Disponível em: https://www.wired.com/2014/10/verizons-perma-cookie. Acesso em: 08 de mar. 2023.

[30] Depois do escândalo, a empresa mudou de nome, tendo sido incorporada por outra – *Cardinal Group*. Em um perfil remanescente na Bloomberg está descrito que a empresa "*offers data and media management platform technologies. The Company provides platforms which allows centralized management of multiple inventory sources, target custom audiences at scale, and optimize performance*." Ver mais em: BLOOMBERG. *Turn Inc.* Disponível em: https://www.bloomberg.com/profile/company/4528628Z:US. Acesso em: 08 de mar. 2023

[31] FEDERAL Trade Commission. *Complaint. Docket nº 1523099*. FTC. Disponível em: https://www.ftc.gov/system/files/documents/cases/turn_inc_final_complaint.pdf. Acesso em: 08 de mar. 2023.

[32] FEDERAL Trade Commission. *Decision and Order Docket nº 1523099*. FTC. Disponível em: https://www.ftc.gov/system/files/documents/cases/turn_decision_and_order.pdf . Acesso em: 08 de mar. 2023.

[33] Essas páginas são elaboradas por meio de linguagem de marcação de texto, o *HTML - Hypertext Markup Language*. O *HTML* é a estrutura básica das páginas *Web* e de aplicações *Web*. Veja mais em: W3C. HTML & CSS. W3C. Disponível em: https://www.w3.org/standards/webdesign/htmlcss. Acesso em: 07 de mar. 2023.

[34] ROBBINS, Jennifer Niederst. *Learning Web Design: A Beginner's Guide to HTML, CSS, JavaScript, and Web Graphics*. 5ª ed. O'Reilly Media, 2018. p. 27-32

Após os *cookies* virem ao mundo, as agências de publicidade logo perceberam ser possível não só enviar imagens e textos de seus servidores, como também fornecer um mecanismo para receber de volta informações do usuário. A rodovia dos dados digitais se tornara assim de "mão dupla", não só entre os usuários e os *sites* por eles visitados, para as finalidades já explanadas acima, como também entre os usuários e terceiros, para fins publicitários.

Ainda nos anos 90, a agência de publicidade *DoubleClick* foi pioneira nas atividades de rastreamento dos internautas, tendo sido adquirida em pouco tempo por ninguém menos que a gigante Google, que incorporou suas soluções no produto Google *AdWords*.[35] Um fato muito curioso já que a empresa que praticamente moldou uma nova forma de capitalismo por meio da utilização massificada de rastreamento de usuários da *Web* é a mesma que está sendo responsável por uma iniciativa de acabar com os *cookies* de terceiros.[36]

Muitos são os questionamentos que surgem em torno da iniciativa de pôr fim aos *cookies* de terceiros, especialmente com relação ao impacto que isso poderá gerar nos mercados digitais e no setor publicitário. Embora essa iniciativa venha com uma promessa de promover mais privacidade aos internautas, convém destacar que ainda estamos, em certa medida, tentando desenvolver mecanismos para lidar adequadamente com todos os riscos que essa tecnologia impõe. Já vimos que a tecnologia não é muito boa em cumprir suas promessas. Diante disso, surge uma questão: o que, de fato, virá depois dos *cookies*?

Na era do Capitalismo de Vigilância, os usuários de *Internet* sempre estarão sujeitos a algum tipo de rastreamento. No decorrer deste trabalho, pudemos verificar usos úteis para o rastreamento, de modo que não se pode afirmar que todo rastreamento *online* é ruim. O que precisa ser observado é se a implementação e uso dessas tecnologias respeitam minimamente

---

[35] Definido pela própria Google, o Google Ads (que era conhecido como Google AdWords e Google AdWords Express) é uma solução de publicidade on-line que as empresas usam para promover os seus produtos e serviços na Pesquisa Google, no YouTube e em outros sites na Web.

[36] Em 2022 a Google anunciou o projeto *Privacy Sandbox,* uma iniciativa para o desenvolvimento de ferramentas alternativas aos *cookies* de terceiros. A ideia central é promover a privacidade dos usuários e, ao mesmo tempo, garantir a publicidade direcionada. *Cookies*, de alguma maneira integram a arquitetura da *Web* atual. A iniciativa da Google é voltada para os usuários do seu navegador da *Web*, o Google Chrome. Contudo, sendo de longe o navegador mais utilizado no mundo, não é exagero afirmar que esta iniciativa tem o potencial de pôr fim à era dos *cookies* – de terceiros. Ver mais em: CHAVEZ, Anthony. *Expanding testing for the Privacy Sandbox for the Web.* Google, 27 de jul. 2022. https://blog.google/products/chrome/update-testing-privacy-sandbox-web.. Acesso em: 08 de mar. 2023; MEREWOOD, Rowan. *No spooky cookies: Cookies are best fresh, so what are the latest recipes to ensure you can still enjoy spooky season without any stale cookies?.* Google, 24 de out. 2023. Disponível em: https://developer.chrome.com/blog/no-spooky-cookies/. Acesso em: 08 de mar. 2023.

as garantias e liberdades individuais, não só resguardando, mas promovendo a privacidade e o livre desenvolvimento da personalidade dos usuários.

1.2. Informação e Consentimento

Com as normativas de proteção de dados ganhando cada vez mais destaque nos espaços de debate, os provedores de serviços digitais se lançaram para tentar adaptar seus serviços e páginas *web* às novas regulamentações. Isso provocou uma inundação de *banners* irritantes sobre políticas de privacidade e *cookies*, inclusive afetando a experiência do usuário. Em março de 2021, o NOYB – *European Center for Digital Rights* – fez uma investigação sobre *cookies* ilegais e apresentou mais de 700 reclamações em toda a Europa.[37]

Entre 2021 e 2022, as reclamações relacionadas ao tema registradas junto à Autoridade Nacional de Proteção de Dados (ANPD) foram 100 vezes menores (informações fornecidas pela própria ANPD via Lei de Acesso à Informação).[38] Claro que é preciso considerar uma série de outros fatores para uma comparação precisa, mas o índice revela que o Brasil tem um longo caminho pela frente para conscientizar os titulares sobre seus direitos.

Na Europa, há duas regulamentações importantes aplicáveis aos *cookies*: *General Data Protection Regulation* (GDPR) e *ePrivacy Directive*. Para o GPDR, os *cookies* são vistos como dados pessoais e, por isso, atraem as disposições das normativas de proteção de dados. Em termos práticos, isso implica dizer que, para processar esses dados, as empresas precisam do consentimento do usuário ou justificar com base no legítimo interesse.[39]

A *ePrivacy Directive*, dentre outras disposições, estabelece que "*é, de suma importância que sejam prestadas informações claras e exaustivas aos utilizadores, sempre que haja atividades que possam resultar nesse tipo de armazenamento ou de possibilidade de acesso*."[40]

---

[37] NOYB. *Where did all the "reject" buttons come from?!*. NOYB, 27 de out. 2023. Disponível em: https://noyb.eu/en/where-did-all-reject-buttons-come. Acesso em: 09 de mar. 2023.

[38] Em solicitação via Lei de Acesso à Informação à ANPD sobre reclamações relacionadas a (i) cookies e (ii) rastreamento de dados pessoais sem consentimento do titular, o órgão informou que foram recebidos, até o momento da resposta conclusiva (13/02/2023), 4 requerimentos que relatavam problemas na Política de *Cookies* de Agentes de Tratamento. Outros 3 requerimentos foram recebidos que versavam sobre algum tipo de rastreamento de dados pessoais sem consentimento.

[39] GDPR.EU. *Cookies, the GDPR, and the ePrivacy Directive*. Ver mais em: https://gdpr.eu/cookies. Acesso em: 09 de mar. 2023.

[40] EUR.LEX. Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de novembro de 2009. EUR.LEX. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0136. Acesso em: 02 de mai. 2023. p. 20.

Como se pode depreender, a informação ao titular é um elemento essencial para um consentimento legal. Aliás, nesse sentido, são os preceitos do GDPR e da LGPD, nos quais o consentimento é uma manifestação livre, informada e inequívoca.[41]

Ainda nessa seara, o Guia Orientativo sobre *cookies* da ANPD (o qual será analisado detalhadamente mais adiante), explica que os *banners* de *cookies* contribuem para o processo de tomada de decisão consciente pelo titular, além de fortalecer o controle sobre seus dados pessoais e o respeito às suas legítimas expectativas[42] e ainda que a utilização de *cookies* sem as devidas salvaguardas técnicas e jurídicas pode gerar impactos negativos sobre os direitos e a privacidade de titulares de dados pessoais.[43]

Contudo, tem sido prática comum que páginas *web* apresentem *cookies* com informações confusas e *layouts* que dificultam a informação do titular sobre a coleta dos seus dados,[44] o que vai contra as disposições da própria *ePrivacy Directive* na qual "*as formas de prestação de dar informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão simples quanto possível*." [45]

Além de *layouts* pouco intuitivos, dificultando a compreensão dos usuários, há outros problemas: linguagem pouco clara; opções pré-marcadas; ausência de opção de rejeição, o que dificulta o gerenciamento dos *cookies* e traz consequências para além do direito do titular de participar do processo de decisão sobre o tratamento de dados pessoais.

O cenário fica ainda mais preocupante quando se reflete sobre a possibilidade de que, ainda que a decisão seja dada de forma livre, informada e inequívoca, as empresas possam adotar práticas como as da Verizon no escândalo de 2014, na qual a decisão do titular sobre o rastreamento de seus dados era absolutamente ignorada.

---

[41] Ver: considerando 32 do GDPR; Art. 5º, XII da LGPD.

[42] AUTORIDADE Nacional de Proteção de Dados. *Guia Orientativo: Cookies e proteção de dados pessoais*. ANPD, out. 2022. p. 30.

[43] Ibid. p. 5.

[44] NOYB. *Noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints*. NOYB, 31 de mai. 2021. Disponível em: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints. Acesso em: 09 de mar. 2023; NOYB. *226 complaints lodged against deceptive cookie banners*. NOYB, 09 de ago. 2022. Disponível em: https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners. Acesso em: 09 de mar. 2023

[45] EUR.LEX. Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de novembro de 2009. EUR.LEX. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0136. Acesso em: 02 de mai. 2023. p. 20.

2. Guia Orientativo sobre *Cookies* e Proteção de Dados Pessoais da ANPD

A relação entre *cookies* e a Lei Geral de Proteção de Dados Pessoais (LGPD) se dá na mesma sistemática do modelo europeu. Embora não mencione uma vez sequer o termo *cookies*, fica evidente, pela leitura de seus dispositivos, que eles representam uma forma de operação de tratamento de dados pessoais[46] e, portanto, sua utilização deve observar os preceitos estabelecidos na LGPD.

A ANPD publicou, em outubro de 2022, o Guia Orientativo sobre *Cookies* e Proteção de Dados Pessoais com o objetivo de explicar a temática, educar titulares de dados pessoais sobre seus direitos e orientar os agentes de tratamento sobre boas práticas na área, abordando desde questões mais conceituais, como a classificação dos *cookies* de acordo com diversos parâmetros, até pontos mais técnicos, como boas práticas a serem observadas na utilização de *cookies* em *sites* eletrônicos.[47]

O Guia segue tendência de outras autoridades de proteção de dados estrangeiras como o *Guía sobre el uso de las cookies* da *Agencia Española Protección Datos* (AEPD), que foi publicado em junho de 2022,[48] o *Guidance on the use of cookies and similar technologies,*[49] da *Information Comissioner's Office* (ICO), *e o Questions-réponses sur les lignes directrices modificatives et la recommandation «cookies et autres traceurs»,*[50] da *Commission Nationale de l'Informatique et des Libertés* (CNIL).

Em comparação com os guias de autoridades de proteção de dados estrangeiras, alguma discussão pode ser levantada sobre a estrutura adotada pelo guia da ANPD. O guia da CNIL, por exemplo, adota estrutura de perguntas e respostas, o que pode facilitar ainda mais o

---

[46] Art. 5º, X – tratamento: 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;

[47] AUTORIDADE Nacional de Proteção de Dados. ANPD lança guia orientativo "Cookies e Proteção de Dados Pessoais". GOV.br, 18 de out. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/anpd-lanca-guia-orientativo-201ccookies-e-protecao-de-dados-pessoais201d. Acesso em: 08 de mar. 2023.

[48] AEPD. *Guía sobre el uso de las cookies*. AEPD. Jun. de 2022. Disponível em: https://www.aepd.es/es/documento/guia-cookies.pdf. Acesso em: 09 de mai. 2023.

[49] ICO. *Guidance on the use of cookies and similar technologies*. ICO. Disponível em: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies. Acesso em: 09 de mai. 2023.

[50] CNIL. *Questions-réponses sur les lignes directrices modificatives et la recommandation «cookies et autres traceurs». CNIL.* https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ. Acesso em: 09 de mai. 2023.

esclarecimento de dúvidas dos titulares e controladores. Embora o guia da ANPD mencione tecnologias similares de rastreamento, esse ponto não é pormenorizado como ocorre no guia da CNIL e da ICO. À parte disso, o Guia da ANPD é sistematizado de forma similar tanto na estrutura quanto no conteúdo.

O Guia é dividido em quatro partes: (I) Conceitos e Classificações; (II) *Cookies* e a LGPD; (III) Política de *Cookies* e; (IV) *Banners* de *Cookies*. A primeira e a segunda parte são mais gerais, sendo a primeira destinada para uma explanação ampla sobre as categorias e classificações dos diversos tipos de *cookies* existentes. Já na segunda, *Cookies* e a LGPD, o guia traz significativas elucidações, destacando o diálogo da temática com o Marco Civil da Internet (Lei n.º 12.965/2014 ou MCI) e como a LGPD serviu para ampliar suas disposições protetivas. Adiante, enfatizou a necessidade de observância dos preceitos da LGPD, em especial: princípios da finalidade, necessidade e adequação (art. 6º, I, II e III); princípios do livre acesso e da transparência (art. 6º, IV e VI); direitos do titular; término do tratamento e eliminação dos dados pessoais; e hipóteses legais.[51]

Sobre o término do tratamento, mister destacar que o Guia orienta que o período de retenção de *cookies* deve ser compatível com as finalidades do tratamento, limitando-se ao estritamente necessário para se alcançar essa finalidade.[52]

O Guia também aborda de maneira destacada a problemática discutida no tópico 1.2. deste artigo. Em item destacado do Guia, recomenda-se que o consentimento seja informado, exigindo-se, para tanto, que sejam apresentadas ao titular todas as informações necessárias para uma avaliação e uma tomada de decisão consciente a respeito da autorização ou recusa para utilização de *cookies*. Esclarece ainda que deve ser assegurada ao titular a possibilidade efetiva de aceitar ou recusar a utilização de *cookies*, sem consequências negativas ou de intervenções do controlador que possam viciar ou prejudicar sua manifestação de vontade.[53]

2.1. Políticas de *Cookies*

As políticas de *cookies* são iniciativas respeitáveis ao passo que proporcionam ao titular uma oportunidade para compreender o que ocorre com os dados pessoais coletados, para qual

[51] AUTORIDADE Nacional de Proteção de Dados. Guia Orientativo: Cookies e proteção de dados pessoais. ANPD, out. 2022. p. 13-17.
[52] Ibid. p. 17.
[53] Ibid. p. 18.

finalidade, o término do tratamento, direitos dos titulares, entre outros. Isso claro em um cenário no qual as políticas estejam completamente aderentes às disposições legais.

A terceira parte do Guia da ANPD aborda as Políticas de *cookies*[54], indicando que os agentes de tratamento devem se preocupar em disponibilizar informações aos titulares. A medida, é claro, põe os agentes em conformidade com os princípios do livre acesso e da transparência (art. 6º, IV e VI da LGPD). Ainda de acordo com o Guia, os agentes devem apresentar informações sobre as finalidades específicas que justificam a coleta de dados pessoais por meio de *cookies*, o período de retenção e se há compartilhamento com terceiros, entre outros aspectos indicados no art. 9º da LGPD.

Não há uma determinação legal ou uma prática de mercado que determine uma forma específica para prestação das informações (*banners*, políticas ou outro documento). Nesse aspecto, o Guia acerta ao exemplificar que as informações possam ser fornecidas (**i**) com uma seção específica no Aviso de Privacidade; (**ii**) em um local específico e separado; ou (**iii**) no próprio *banner* de *cookies*, sendo determinante apenas que as informações essenciais sejam apresentadas ao titular.

2.2. *Banners* de *Cookies*

Banner de *cookies* são definidos pelo Guia como um recurso visual usado no *design* de aplicativos ou *sites* na *Internet*, que utiliza barras de leitura destacadas para informar ao titular de dados, de forma resumida, simples e direta, sobre a utilização de *cookies* naquele ambiente. Nesse aspecto, são mecanismos indispensáveis para informar o titular e dar-lhe maior controle sobre o tratamento de seus dados, promovendo transparência e aderência aos princípios de proteção de dados pessoais.[55]

O destaque nesta quarta parte do Guia fica para os tópicos de recomendações de elaboração de *banners* em que os agentes poderão se orientar para elaboração de *banner* de *cookies*. Resumidamente, os agentes devem fornecer informações claras e objetivas, de fácil acesso, além, é claro, de mecanismos que oportunizem ao titular desabilitar os *cookies* não necessários.

[54] Ibid. p. 28-29.
[55] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Op. Cit.,2022. p.30.

Por fim, há um rol não exaustivo de práticas a serem evitados durante a elaboração de *banner* de *cookies* em *sites* eletrônicos, dos quais destaca-se (**i**) dificultar a visualização e compreensão dos botões de rejeitar *cookies* ou de configurar *cookies*, e conferir maior destaque apenas ao botão de aceite; (**ii**) impossibilitar ou dificultar a rejeição de todos os *cookies* não necessários e; (**iii**) dificultar o gerenciamento de *cookies* (por exemplo, não disponibilizar opções específicas de gerenciamento para *cookies* que possuem finalidades distintas).

Considerações Finais

Durante este trabalho, pudemos verificar que os *cookies* são uma realidade do mundo virtual que não pode ser ignorada. Embora exerçam um papel essencial no funcionamento da *Web* e até mesmo de aplicativos móveis, seu uso de forma indiscriminada e apartado das normas de proteção de dados podem trazer consequências catastróficas para os titulares.

A LGPD representou um marco significativo para a proteção de direitos individuais e este processo se consolidou com a proteção de dados sendo alçada à categoria de direitos fundamentais pela emenda constitucional n.º 115 de 2022.[56]

Em uma visão reducionista, a LGPD seja uma versão enxuta do GDPR, seja por sua extensão, seja por não pormenorizar algumas questões atinentes à privacidade. No entanto, sob essa ótica, é possível verificar um cenário para que a regulação se dê de forma mais adequada e atual. Embora seja somente um guia orientativo, o Guia da ANPD para *cookies* tem potencial para movimentar o mercado e impactar diretamente os titulares de dados.

Por fim, tendo os *cookies* um papel tão relevante e, ao mesmo tempo, tão cercado de riscos aos titulares, será que não cabe à ANPD um papel mais ativo na fiscalização dos *cookies* e *banners* de *cookies*? De qualquer forma, para ampliar essa reflexão, o guia orientativo para os cookies é certamente um bom ponto de partida.

[56] A EC nº 115 não incluiu a proteção de dados no rol de direitos fundamentais na Constituição Federal, como também fixou competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Ver mais em: BRASIL, Emenda Constitucional nº 115. Presidência da República, 10 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 10 de mar. 2023.

Referências bibliográficas

AUTORIDADE Nacional de Proteção de Dados. Guia Orientativo: *Cookies e proteção de dados pessoais*. ANPD, 18 de out. 2022.

AUTORIDADE Nacional de Proteção de Dados. *ANPD lança guia orientativo "Cookies e Proteção de Dados Pessoais"*. GOV.BR, 18 de out. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/anpd-lanca-guia-orientativo-201ccookies-e-protecao-de-dados-pessoais201d. Acesso em: 08 de mar. 2023.

BLOOMBERG. Turn Inc. Disponível em: https://www.bloomberg.com/profile/company/4528628Z:US. Acesso em: 08 de mar. 2023

BRASIL, Emenda Constitucional nº 115. Presidência da República, 10 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 10 de mar. 2023.

CERN. *A short history of the Web*. Disponível em: https://home.cern/science/computing/birth-web/short-history-web. Acesso em: 21 de fev. 2023.

CERN. *Tim Berners-Lee's original World Wide Web browser*. Disponível em: http://info.cern.ch/NextBrowser.html. Acesso em: 21 de fev. 2023.

CHAVEZ, Anthony. *Expanding testing for the Privacy Sandbox for the Web*. Google. 27 de jul. 2022. https://blog.google/products/chrome/update-testing-privacy-sandbox-web.. Acesso em: 08 de mar. 2023

COPPA. 15 U.S.C. §§ 6501-6506. *Children's Online Privacy Protection Act*. 21 de abr. 2000. Disponível em: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. Acesso em: 26 de fev. 2023.

EUR.LEX. DIRETIVA 2009/136/CE DO PARLAMENTO EUROPEU E DO CONSELHO

de 25 de novembro de 2009. EUR.LEX. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0136. Acesso em: 02 de mai. 2023. p. 20.

FEDERAL Trade Commission. *Privacy Online: A Report to Congress*. FTC. Federal Trade Commission, jun. 1998. p.1.

FEDERAL Trade Commission. *Prepared statement of the Federal Commission on Internet Privacy before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary United States House of Representatives*. FTC, 26 de mar. 1998. Disponível em: https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-internet-privacy/privacy.pdf. Acesso em: 26 de fev. 2023. n.p.

FEDERAL Trade Commission. *Complaint. Docket nº 1523099*. FTC. Disponível em: https://www.ftc.gov/system/files/documents/cases/turn_inc_final_complaint.pdf. Acesso em: 08 de mar. 2023.

FEDERAL Trade Commission. *Decision and Order Docket nº 1523099*. FTC. Disponível em: https://www.ftc.gov/system/files/documents/cases/turn_decision_and_order.pdf . Acesso em: 08 de mar. 2023.

GDPR.EU. *Cookies, the GDPR, and the ePrivacy Directive*. Ver mais em: https://gdpr.eu/cookies. Acesso em: 09 de mar. 2023

JACKSON, *Tim. This bug in your PC is a smart cookie*. Financial Times, London,

Week n. 7, n. 32.906, 12 de fev. 1996. *Companies & Markets*, p. 15.

MEREWOOD, Rowan. *No spooky cookies: Cookies are best fresh, so what are the latest recipes to ensure you can still enjoy spooky season without any stale cookies?*. Google. 24 de out. 2023. Disponível em: https://developer.chrome.com/blog/no-spooky-cookies/. Acesso em: 08 de mar. 2023.

MCMILLAN, Robert. *Verizon's 'Perma-Cookie' Is a Privacy-Killing Machine*. 27 de out. 2014. WIRED. Disponível em: https://www.wired.com/2014/10/verizons-perma-cookie. Acesso em: 08 de mar. 2023.

MONTULLI, Lou. *Persistent Client State In A Hypertext Transfer Protocol Based Client-Server System*. US 20070185978A1, 9 ago. 2007. United States Patent and Trademark Office. Palo Alto: USPTO, 2007.

MONTULLI, Lou. KRISTOL, David. *HTTP State Management Mechanism. RFC 2109. Standards Track*, fev. de 1997. Disponível em: https://www.rfc-editor.org/rfc/rfc2109. Acesso em: 22 fev. 2023.

NOYB. *Where did all the "reject" buttons come from?!*. NOYB, 27 de out. 2023. Disponível em: https://noyb.eu/en/where-did-all-reject-buttons-come. Acesso em: 09 de mar. 2023.

NOYB. *Noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints*. NOYB, 31 de mai. 2021. https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints. Acesso em: 09 de mar. 2023

NOYB. *226 complaints lodged against deceptive cookie banners*. NOYB, 09 de ago. 2022. https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners. Acesso em: 09 de mar. 2023.

KIHN, MARTIN. *Lou Montulli: The Man Who Invented the Cookie*. Martin Kihn, 21 de out. 2019. Disponível em: https://martinkihn.com/2019/10/21/lou-montulli-the-man-who-invented-the-browser-cookie. Acesso em: 23 de fev. 2023

MOZILLA. *Cookies HTTP*. https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Cookies. Acesso em: 08 de Mar. 2023.

MOZILLA. *Cookies HTTP: rastreamento e privacidade*. https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Cookies#rastreamento_e_privacidade. Acesso em: 08 de mar. 2023.

O'REILLY, Tim. *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. O 'Reilly, 30 de set. 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1. Acesso em: 24 jan. 2023

ROBBINS, Jennifer Niederst. *Learning Web Design: A Beginner's Guide to HTML, CSS, JavaScript, and Web Graphics*. 5ª ed. O'Reilly Media, 2018. p. 27-32

RODOTÀ, Stefano. *A vida na sociedade da vigilância - A privacidade hoje* / Stefano Rodotà – Organização, seleção e apresentação de Maria Celina Bodin de Moraes. – Rio de Janeiro: Renovar, 2008. p. 169;

STEVEN, Johnson. *The Magic Cookie: How Lou Montulli Cured The Web's Amnesia*. Disponível em: <https://hiddenheroes.netguru.com/lou-montulli>. Acesso em: 08 de fev. 2023. n.p.

STUART, Andrew. *Where cookie comes from*. Domino Power, 1º de jul. 2002. Disponível em: http://dominopower.com/article/where-cookie-comes-from. Acesso em: 24 de fev. 2023.

W3C. *HTML & CSS*. Disponível em: https://www.w3.org/standards/webdesign/htmlcss. Acesso em: 07 de mar. 2023.

ZUBBOF, Shoshana. *A Era do Capitalismo de Vigilância*. 1ª ed. Editora Intrínseca, 2021. p.18

ADESÃO DO BRASIL À CONVENÇÃO 108: DESAFIOS E PERSPECTIVAS PARA A PROTEÇÃO DE DADOS PESSOAIS

Thobias Prado Moura[1]

Resumo: A proteção de dados pessoais é um tema cada vez mais relevante em todo o mundo. No Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2020 e a Autoridade Nacional de Proteção de Dados (ANPD) foi criada em 2019 para fiscalizar e regulamentar a aplicação da lei. Nesse contexto, um dos diplomas legislativos mais importantes se trata da Convenção de Strasbourg nº 108 do Conselho Europeu de 1981, que foi o primeiro documento a regulamentar a proteção de dados pessoais na Europa. A Convenção estabeleceu princípios fundamentais, objetivos e finalidades para garantir o respeito pelos direitos e liberdades fundamentais dos cidadãos europeus, em relação ao tratamento automatizado de dados pessoais. Em 2018, foi adotada a Convenção 108+, uma versão modernizada que reflete os desafios colocados pela evolução tecnológica na proteção de dados pessoais. Este artigo tem como objetivo analisar os desafios e perspectivas para a adesão do Brasil à Convenção 108 e à Convenção 108+, bem como seus impactos na proteção de dados pessoais no país. Para tanto, abordar-se-á a importância da proteção de dados pessoais no cenário global e nacional à luz do Constitucionalismo Digital; a Convenção 108 e sua relevância como instrumento internacional de proteção de dados e; a posição do Brasil em relação à adesão e à proteção de dados pessoais e os desafios a serem superados.

Palavras-chave: Lei Geral de Proteção de Dados; Convenção 108; Constitucionalismo Digital.

Abstract: *The protection of personal data is an increasingly relevant topic worldwide. In Brazil, the General Data Protection Law (LGPD) came into effect in 2020 and the National Data*

[1] Doutorando em Direito pela Universidade Nova de Lisboa, Pesquisador em Governança da Internet no Laboratório de Direitos Humanos (LabDH) e no *WhatNext.Law*.

Protection Authority (ANPD) was created in 2019 to supervise and regulate the application of the law. In this context, one of the most important legislative documents is the Council of Europe's Strasbourg Convention No. 108 of 1981, which was the first document to regulate personal data protection in Europe. The convention established fundamental principles, objectives, and purposes to ensure respect for the fundamental rights and freedoms of European citizens in relation to the automated processing of personal data. In 2018, Convention 108+, a modernized version that reflects the challenges posed by technological evolution in personal data protection, was adopted. This article aims to analyze the challenges and prospects for Brazil's accession to Convention 108 and Convention 108+, as well as their impacts on personal data protection in the country. To this end, it will discuss the importance of personal data protection in the global and national scenario in the light of digital constitutionalism; Convention 108 and its relevance as an international instrument of data protection; Brazil's position in relation to accession and personal data protection and the challenges to be overcome.

Keywords: *protection of personal data; General Data Protection Law; Convention 108; digital constitutionalism.*

Introdução

A proteção de dados pessoais é um tema cada vez mais relevante em todo o mundo, especialmente no contexto da crescente digitalização da sociedade.[2] No Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2020 e estabeleceu um marco regulatório para a proteção de dados pessoais no país.[3] Para efetivar, fiscalizar e regulamentar a aplicação da lei a Autoridade Nacional de Proteção de Dados (ANPD) foi criada em 2019.[4]

No entanto, o Brasil ainda enfrenta desafios para garantir uma proteção efetiva dos dados pessoais, como a falta de uma "LGPD Penal" e o fato da ANPD ainda estar em processo

[2] WE ARE SOCIAL. Digital 2021: global overview report. global overview report. 2021. Disponível em: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/. Acesso em: 27 nov. 2022.
[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Online, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 dez. 2022.
[4] BRASIL. Lei Nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Online, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

de estruturação e definição de seu escopo de atuação.[56] Isso significa que a ANPD ainda está se preparando para enfrentar os desafios que virão com a aplicação da LGPD e pode levar algum tempo para que esteja plenamente operacional.[7]

Em adição a isso, a proteção de dados pessoais é um tema de grande importância para a privacidade e segurança das pessoas em todo o mundo, e a União Europeia tem sido uma grande influência nesse sentido.[8] Em 1981, o Conselho da Europa adotou a Convenção 108, tornando-se o primeiro instrumento internacional juridicamente vinculativo no domínio da proteção de dados. Esta Convenção é especialmente relevante para o Brasil, que enfrenta desafios na proteção efetiva dos dados pessoais e está buscando fortalecer seu marco regulatório neste aspecto.[9]

A Convenção foi criada para garantir que o processamento de dados pessoais fosse realizado de forma justa e legal, e que as pessoas tivessem o direito de saber quais informações estão sendo coletadas e como estão sendo utilizadas.[10]

Nesse contexto, este artigo tem como objetivo discutir a importância da adesão do Brasil à Convenção 108 da Europa. Além disso, serão apresentados os desafios enfrentados pelo Brasil em relação à proteção de dados pessoais e como a adesão à Convenção 108 pode contribuir para o fortalecimento da proteção de dados no país, trazendo mais segurança e confiança para os usuários e empresas que lidam com informações pessoais, especialmente considerando a Convenção como parte do chamado "Constitucionalismo Digital".

---

[5] ALMEIDA, Eloísa Machado de; ESTELLITA, Heloisa (org.). Dados, privacidade e persecução penal: cinco estudos. São Paulo: Data Privacy Research, 2021. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31784/Dados%2C%20privacidade%20e%20persecu%C3%A7%C3%A3o%20penal.pdf?isAllowed=y&sequence=1. Acesso em: 05 jan. 2023.

[6] SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A Autoridade Nacional de Proteção de Dados (ANPD) e os desafios tecnológicos: alternativas para uma estruturação responsiva na era da governança digital. Revista Direitos Fundamentais & Democracia, (S.I), v. 27, n. 3, p. 217-253, dez. 2022.

[7] GROSSMANN, Luís Osvaldo. ANPD começa a aplicar multas por infrações à LGPD a partir de fevereiro. 2023. Disponível em: https://www.convergenciadigital.com.br/Governo/Legislacao/ANPD-comeca-a-aplicar-multas-por-infracoes-a-LGPD-a-partir-de-fevereiro-62379.html. Acesso em: 10 fev. 2023.

[8] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 9.

[9] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.

[10] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.

Nesse sentido, violações transnacionais de dados pessoais têm se tornado cada vez mais proeminentes com o avanço da globalização e da digitalização da sociedade. Essas violações não apenas podem ocorrer dentro das fronteiras de um país, mas também podem se estender além das fronteiras nacionais, levando a danos potencialmente severos para os indivíduos afetados.

No cerne da Convenção 108, está a intenção de promover a cooperação internacional e a assistência mútua no cumprimento das leis de proteção de dados. Destarte, caso o Brasil se junte à Convenção, poderá contribuir junto a outros países no combate a violações de dados transnacionais. Esta cooperação oferece uma camada adicional de segurança aos cidadãos brasileiros, pois garante que suas informações pessoais estejam protegidas tanto internamente, como globalmente.

No entanto, a adesão também envolve desafios a serem superados, como a necessidade de ajustar as leis e regulamentos nacionais para se adequar aos princípios da Convenção. Esses desafios exigem uma abordagem holística que não se detenha somente no aparato legal do Estado brasileiro, mas sobretudo utilize de ferramentas que podem contribuir para sua superação, sobretudo considerando que o Brasil ainda não ratificou a Convenção, atuando apenas como Estado Observador do Comitê da Convenção Internacional de Proteção de Dados Pessoais do Conselho da Europa.[11]

Ao analisar a Convenção sob a perspectiva do Constitucionalismo Digital, é possível compreender como os princípios e as normas da Convenção se relacionam com outras iniciativas de proteção de direitos digitais, como o Marco Civil da Internet, a LGPD e o GDPR. Além disso, é possível identificar lacunas e desafios na implementação da Convenção no contexto do mundo digital, como a dificuldade de garantir a proteção de dados em um ambiente global e o uso cada vez mais intenso de algoritmos e inteligência artificial na tomada de decisões.

A adesão do Brasil à Convenção 108 é um passo importante na direção de enfrentar esses desafios e fortalecer a proteção de dados pessoais no país. No entanto, a implementação efetiva da Convenção e a superação dos desafios associados requerem uma compreensão

[11] COUNCIL OF EUROPE. Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers! 2018. Disponível em: https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers-. Acesso em: 20 dez. 2022.

abrangente dos direitos digitais e da forma como a proteção de dados se encaixa no contexto mais amplo do Constitucionalismo Digital.

O Constitucionalismo Digital é um conceito que se refere ao estudo das implicações e desafios que a era digital apresenta ao Direito Constitucional e à proteção dos direitos fundamentais. Ele se concentra na necessidade de adaptação dos princípios fundamentais do Direito Constitucional às novas realidades tecnológicas, e na garantia da proteção dos direitos humanos em um contexto em que as tecnologias digitais desempenham um papel cada vez mais importante na vida cotidiana.

Nele se inclui temas como a privacidade e a proteção de dados pessoais, a liberdade de expressão e informação na Internet, a regulação da tecnologia de vigilância e os direitos dos consumidores no ambiente digital[12]. Além disso, o Constitucionalismo Digital também se preocupa com a governança da Internet e com a participação democrática no processo de tomada de decisões sobre questões relacionadas à tecnologia.[13]

A análise da Convenção 108 sob a perspectiva do Constitucionalismo Digital é fundamental para entender como a proteção de dados pessoais se encaixa na governança digital e quais são as implicações para os direitos fundamentais no mundo digital.

Isso implica a necessidade de ampliar a compreensão dos desafios e oportunidades relacionados à proteção de dados no contexto da governança digital, a fim de aprimorar as iniciativas em prol da proteção de direitos fundamentais no mundo virtual.

Desse modo, o tema mostra-se extremamente relevante em um contexto em que é necessário a consolidação de políticas públicas e de regimes regulatórios que atuem para garantir a confiança e a credibilidade do uso de serviços digitais, especialmente a partir da proteção da privacidade, da segurança dos dados pessoais e do princípio da autodeterminação informativa, recentemente reconhecido judicialmente e legislativamente como princípio constitucional da nação brasileira.

[12] CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. International Review Of Law, Computers & Technology, [S.I.], v. 33, n. 1, 2 jan. 2019. p. 5-6

[13] GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism? mapping attempts to craft an internet bill of rights. Berkman Klein Center For Internet & Society Research Publication, Cambridge, v. 15, nov. 2015. p. 10-13. Disponível em: https://dash.harvard.edu/handle/1/28552582. Acesso em: 27 dez. 2022.

1. A Convenção 108 e sua relevância como instrumento internacional de proteção de dados

Conforme exposto no tópico anterior, a Convenção 108 do Conselho da Europa, também conhecida como Convenção para a Proteção das Pessoas em Relação ao Tratamento Automatizado de Dados Pessoais, foi um marco importante na proteção dos direitos fundamentais relacionados à privacidade e proteção de dados pessoais.[14]

Ela se baseia em princípios fundamentais que visam garantir a proteção da privacidade e dos direitos humanos no tratamento de dados pessoais, independentemente do meio ou tecnologia utilizados. Para tanto, ela é composta por três partes: a primeira define os objetivos, finalidades e princípios fundamentais; a segunda aborda o fluxo transfronteiriço de dados pessoais; e a terceira trata do acesso e da consulta aos bancos de dados.[15]

Os princípios da Convenção incluem a proteção dos direitos e liberdades fundamentais, especialmente o direito à vida privada, diante do tratamento automatizado de dados pessoais. Isso significa que a Convenção tem como objetivo garantir que os dados pessoais sejam tratados de forma adequada e respeitando os direitos humanos.[16]

Doneda sintetiza os princípios orientadores da Convenção como:

a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
b) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam

[14] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.
[15] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.
[16] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.

feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;

c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;
e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado[17].

Embora a Convenção não seja obrigatória, sua adoção propulsionou a regulamentação da proteção de dados pessoais em muitos países da Europa, além de servir como referência importante para a elaboração de leis nacionais.[18] Estes princípios, formam uma estrutura basilar para diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, sendo o núcleo das questões com as quais o ordenamento jurídico deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais.[19]

[17] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 25 fev. 2023. p.101.

[18] FACHINETTI, Aline Fuke; CAMARGO, Guilherme. Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil. Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados. Acesso em: 20 jan. 2023.

[19] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 25 fev. 2023. p.101.

Atualmente, a Convenção tem 55 países signatários, incluindo diversos países da Europa continental, a Argentina, e México, além de oito países observadores.[20] No entanto, é de se notar que o Brasil ainda não é parte da Convenção 108, o que pode gerar dificuldades em relação às transferências internacionais de dados pessoais.[21]

Além do mais, sua natureza não obrigatória significa que os países signatários da Convenção são livres para adotar suas próprias leis e políticas de proteção de dados, inclusive com diferentes níveis de proteção. Atualmente, a Convenção 108 continua a ser uma referência importante para a proteção de dados pessoais, inclusive para a União Europeia, que adotou o Regulamento Geral de Proteção de Dados (GDPR), em 2018, que se baseia em muitos dos princípios estabelecidos na Convenção.[22] A Convenção também tem sido um modelo para a elaboração de outras leis e tratados internacionais relacionados à proteção de dados pessoais.

Recentemente uma atualização foi proposta, chamada de Convenção 108+.[23] A atualização proposta, estabelece novas regras e padrões de privacidade que visam garantir a proteção adequada dos dados pessoais em toda a Europa, levando em conta o ambiente digital em constante mudança.[24] A atualização é vista como um marco importante na proteção de dados pessoais na Europa e um passo importante para a harmonização das leis de proteção de dados pessoais em toda a Europa.[25]

A Convenção 108+ estabelece um conjunto de novas regras e padrões de privacidade que visam garantir a proteção adequada dos dados pessoais em toda a Europa. Algumas das principais mudanças e atualizações incluem:

---

[20] COUNCIL OF EUROPE. National information. 2023. Disponível em: https://www.coe.int/en/web/data-protection/national-information. Acesso em: 20 fev. 2023.

[21] BRANCHER, Paulo Marcos Rodrigues. Proteção internacional de dados pessoais. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em: 02 fev. 2023.

[22] UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). 27 abr. 2016.Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt#d1e2012-1-1>. Acesso em: 18 fev. 2023.

[23] NATARAJAN, Aishwarya. Dawn of a new era of global data protection? 2021. Disponível em: https://voelkerrechtsblog.org/dawn-of-a-new-era-of-global-data-protection/. Acesso em: 10 jan. 2023.

[24] FACHINETTI, Aline Fuke; CAMARGO, Guilherme. Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil. Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados. Acesso em: 20 jan. 2023.

[25] FACHINETTI, Aline Fuke; CAMARGO, Guilherme. Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil. Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados. Acesso em: 20 jan. 2023.

(i) a aplicação a qualquer forma de processamento de dados pessoais, incluindo processamento manual, desde que os dados estejam relacionados às atividades pessoais ou profissionais de um indivíduo;

(ii) o fortalecimento dos direitos individuais, incluindo o direito de ser informado sobre o processamento de seus dados, o direito de acesso, o direito de retificação, o direito à portabilidade dos dados e o direito ao esquecimento e;

(iii) o aumento das obrigações do controlador de dados, impondo obrigações mais rigorosas aos controladores de dados em relação à proteção de dados pessoais;

(iv) cooperação e responsabilidade transfronteiriça, reconhecendo a importância da cooperação transfronteiriça em relação à proteção de dados pessoais;

(v) Fortalecimento da supervisão e fiscalização, estabelecendo requisitos mais rigorosos para a supervisão e fiscalização da proteção de dados pessoais, incluindo a criação de autoridades nacionais de proteção de dados (DPA) independentes e a necessidade de mecanismos efetivos de recurso[26].

A atualização da Convenção é vista como um marco importante na proteção de dados pessoais na Europa e deve ajudar a manter a privacidade e garantir a segurança e a confiança no uso de serviços digitais em todo o continente.[27] Também é vista como um passo importante para a harmonização das leis de proteção de dados pessoais em toda a Europa, o que é essencial para o desenvolvimento de um mercado digital único na União Europeia, uma vez que cria uma base comum para a proteção de dados pessoais em todo o mundo e ajuda a garantir que as pessoas sejam protegidas independentemente de onde seus dados sejam processados.[28]

Os princípios orientadores da Convenção 108, que visam garantir a proteção adequada dos dados pessoais em diversas situações, representam um marco importante na proteção dos direitos fundamentais relacionados à privacidade e proteção de dados pessoais. No entanto, com a crescente digitalização das nossas vidas, surge uma nova questão: como garantir a proteção dos dados pessoais em um ambiente cada vez mais conectado e tecnológico?

[26] COUNCIL OF EUROPE. Convention 108+. 2023. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 Acesso em: 20 fev. 2023.

[27] NATARAJAN, Aishwarya. Dawn of a new era of global data protection? 2021. Disponível em: https://voelkerrechtsblog.org/dawn-of-a-new-era-of-global-data-protection/. Acesso em: 10 jan. 2023.

[28] NATARAJAN, Aishwarya. Dawn of a new era of global data protection? 2021. Disponível em: https://voelkerrechtsblog.org/dawn-of-a-new-era-of-global-data-protection/. Acesso em: 10 jan. 2023.

A resposta a essa pergunta exige uma abordagem de Constitucionalismo Digital, que leva em consideração a proteção dos direitos fundamentais no contexto da era digital, conforme veremos. Ele pode ser uma ferramenta valiosa para ajudar o Brasil e outros países a aplicar os princípios da Convenção de maneira eficaz e adaptável ao rápido avanço da tecnologia.

2. A luta contra a vigilância digital: a proteção de dados pessoais no cenário global e nacional

A complexidade da proteção de dados ganha outra dimensão quando considerado o fluxo transnacional de informações. Em uma era digital globalizada, os dados pessoais não reconhecem fronteiras nacionais. Isso significa que informações coletadas em um país podem ser facilmente processadas ou armazenadas em outro, ampliando a possibilidade de vigilância para além das fronteiras geográficas.

O crescente uso da tecnologia e das plataformas digitais na sociedade atual tem levado à coleta massiva de dados pessoais, o que tem gerado preocupação sobre a proteção dessas informações e o respeito aos direitos fundamentais dos indivíduos.[29] Nesse sentido, percebe-se a vigilância digital como um fenômeno crescentemente, seja na esfera pública ou privada, com o intuito de monitorar e controlar atividades on-line.[30] Essa onipresença da tecnologia e do monitoramento tem implicações significativas para a privacidade, autonomia e liberdade dos indivíduos.[31]

No entanto, a preocupação com a proteção de dados pessoais tem levado a iniciativas nacionais e internacionais em prol da criação de marcos normativos e legislações que protejam a privacidade e os direitos dos cidadãos na era digital. A proteção de dados pessoais no cenário global e nacional é uma questão cada vez mais relevante, dada a importância crescente da internet e das plataformas digitais em nossas vidas.

[29] LYON, David; ZUREIK, Elia. Computers, surveillance, and privacy. Minneapolis: University of Minnesota Press, 1996. p. VII.
[30] LYON, David; ZUREIK, Elia. Computers, surveillance, and privacy. Minneapolis: University of Minnesota Press, 1996. p. VII.
[31] TELES, Edson. Ação Política Híbrida e a Dissolução da Cidadania. Revista de Filosofia Moderna e Contemporânea, [S.I.], v. 8, n. 3, p. 84, 31 jan. 2021. Biblioteca Central da UNB. http://dx.doi.org/10.26512/rfmc.v8i3.34494.

A interdependência global maximiza os riscos, já que o mundo digital funciona de uma maneira descentralizada,[32] na qual diferentes atores globais, com agenda própria definem políticas e normas que orientam e definem a relação entre o uso da tecnologia com a sociedade.[33]

Para combater esse cenário, surgiram diversas iniciativas que buscam estabelecer limites à acumulação predatória de dados e proteger os direitos dos cidadãos. Uma dessas iniciativas é o chamado Constitucionalismo Digital.

Gill, Redeker e Gasser conceituam o Constitucionalismo Digital como um movimento que busca conectar diversas iniciativas que buscam articular uma gama de direitos políticos, normas de governança e definir limites ao exercício do poder no mundo digital.[34] Além disso, estabelece mecanismos de salvaguarda que asseguram que nenhuma entidade, seja ela da esfera pública ou privada, esteja acima dos direitos individuais fundamentais das pessoas que utilizam instrumentos digitais.[35]

Além disso, eles elencam uma série de princípios e direitos que devem ser garantidos no mundo virtual, são eles: Liberdades e Direitos Básicos; Limites Gerais ao Poder Estatal; Governança da Internet e Participação Civil; Direito à Privacidade e Vigilância; Acesso à Internet e Educação Digital; Abertura e Estabilidade nas Redes; e Direitos Econômicos e Responsabilidade.[36]

No campo legal, diversas leis e regulamentações surgiram – especialmente no continente europeu - buscando proteger a privacidade e os direitos dos usuários da Internet, como o Regulamento Geral sobre a Proteção de Dados (RGPD) adotado pela União Europeia,[37]

---

[32] FILGUEIRAS, Fernando; ALMEIDA, Virgílio. Governance for the Digital World: neither more state nor more market. [S.I]: Springer International Publishing, 2020.p.62-63.

[33] FILGUEIRAS, Fernando; ALMEIDA, Virgílio. Governance for the Digital World: neither more state nor more market. [S.I]: Springer International Publishing, 2020.p.3.

[34] GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism?: mapping attempts to craft an internet bill of rights. Berkman Klein Center For Internet & Society Research Publication, Cambridge, v. 15, nov. 2015. Disponível em: https://dash.harvard.edu/handle/1/28552582. Acesso em: 27 dez. 2022. p.2-3.

[35] MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo Digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, v. 16, n. 1, jan.-abr. 2020, p. 8.

[36] GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism?: mapping attempts to craft an internet bill of rights. Berkman Klein Center For Internet & Society Research Publication, Cambridge, v. 15, nov. 2015. Disponível em: https://dash.harvard.edu/handle/1/28552582. Acesso em: 27 dez. 2022. p.7-10.

[37] GUIMARÃES, João Alexandre; MACHADO, Lecio. Comentários à lei geral de proteção de dados: lei 13.709/2018 com alterações da MPV 869/2020. Rio de Janeiro: Lumen Juris, 2020, p. 5.

o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) no Brasil.[38] Nesse sentido, observa-se que esses aparatos legais se originaram principalmente a partir da Convenção 108 e da Diretiva 95/46/EC.

Conforme já descrito, a Convenção 108 visa proteger os indivíduos no que diz respeito ao processamento automatizado de dados pessoais, sendo considerada a primeira norma internacional sobre proteção de dados pessoais.[39]

Já a Diretiva 95/46/EC, também conhecida como Diretiva de Proteção de Dados da União Europeia, foi uma lei de proteção de dados que entrou em vigor em 1995 e estabelece as regras para o tratamento de dados pessoais em toda a União Europeia (UE).[40] Em maio de 2018, a Diretiva 95/46/EC foi substituída pelo Regulamento Geral de Proteção de Dados da União Europeia (RGPD), que estabelece um conjunto mais abrangente de regras e sanções para a proteção de dados pessoais na UE.[41]

Esse fenômeno busca estabelecer um novo marco regulatório para a proteção dos direitos dos cidadãos na era digital. A Convenção 108 está englobada pelo Constitucionalismo Digital na medida em que esta busca articular direitos fundamentais e normas de governança para garantir a proteção dos direitos dos usuários da internet, incluindo a proteção de dados pessoais.

Em muitos países, as normas de proteção de dados pessoais foram incorporadas à legislação nacional, muitas vezes seguindo as diretrizes da Convenção 108. O Marco Civil da

[38] MONCAU, Luiz Fernando Marrey; ARGUELHES, Diego Werneck. The Marco Civil da Internet and Digital Constitutionalism. In: FROSIO, Giancarlo. Oxford Handbook of Online Intermediary Liability. Oxford: Oxford University Press, 2020. p. 189-213.

[39] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.

[40] UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 24/10/1995. Disponível em: <https://eur-lex.europa.eu/ legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 15 feb 2023.

[41] UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). 27 abr. 2016.Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt#d1e2012-1-1>. Acesso em: 18 fev. 2023.

Internet[42] e a LGPD, no Brasil, e o RGPD,[43] na União Europeia, são exemplos de instrumentos normativos que incorporam os princípios da Convenção 108 e que se inserem no contexto do Constitucionalismo Digital.

Assim, a Convenção 108 é um importante instrumento no contexto do Constitucionalismo Digital, uma vez que estabelece diretrizes para a proteção dos direitos fundamentais dos indivíduos no que diz respeito ao processamento de dados pessoais, que são um dos principais temas de debate e regulamentação no ambiente digital atual.

Nesse sentido, a partir das suas diretrizes, o Brasil pode construir regulamentações robustas para a segurança dos dados dentro de tratamentos automatizados. As prescrições de segurança de dados do Artigo 7 que versam sobre a implementação de medidas de segurança apropriadas para a proteção contra destruição, perda, acesso, alteração ou disseminação não autorizada de dados pessoais, podem ser transformadas em normas e guias da ANPD direcionada à todas as entidades que processam dados de forma automatizada, o que garante uma abordagem uniforme e pró cidadão nesses casos.

Ainda no contexto nacional, o artigo 12º estabelece uma estrutura eficaz para o gerenciamento de transferências transfronteiriças de dados. Isso é especialmente valioso para as empresas brasileiras que operam em escala global, permitindo que naveguem com clareza nos desafios associados à transferência de dados pessoais além das fronteiras.

Tais medidas, ao serem incorporadas no ordenamento brasileiro, empoderaram os cidadãos e aumentam a confiança no processamento de dados.

Assim, a Convenção estabelece normas e princípios que incluem a garantia de que o processamento de dados pessoais seja feito de forma justa e para fins legítimos, que os dados pessoais sejam armazenados de forma segura, bem como reforçam o direito dos indivíduos saberem quem está coletando seus dados e para que fins.

[42] MONCAU, Luiz Fernando Marrey; ARGUELHES, Diego Werneck. The Marco Civil da Internet and Digital Constitutionalism. In: FROSIO, Giancarlo. Oxford Handbook of Online Intermediary Liability. Oxford: Oxford University Press, 2020. p. 189-213.

[43] REDEKER, Dennis. Towards a European Constitution for the Internet? Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational Digital Constitutionalism, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European_Constitution.pdf. Acesso em: 31 jan. 2023. p.17.

Esses princípios refletem muitas das preocupações centrais do Constitucionalismo Digital, que também visa estabelecer limites ao poder das entidades que coletam e usam dados pessoais, e garantir que os direitos fundamentais dos indivíduos sejam respeitados na era digital. Desse modo, percebe-se que a Convenção 108 serve como um exemplo de como as leis e regulamentações podem ser usadas para implementar os princípios do Constitucionalismo Digital na prática, ajudando a moldar uma Internet que seja segura e respeite os direitos e liberdades dos usuários.

3. A adesão do Brasil às Convenções 108 e 108+ e os desafios a serem superados

Tanto a informação quanto o conhecimento são recursos compartilhados na era digital, como a informação e o conhecimento, que são afetados por dilemas sociais[44]. Problemas como interrupções no funcionamento de aplicativos em todo o mundo, desinformação, vigilância, dentre outros são semelhantes aos problemas relacionados a outros bens comuns, o que gera custos que afetam toda a sociedade. O desafio é pensar em como governar esses "pontos comuns" da era digital de forma a beneficiar toda a sociedade e reduzir esses custos.[45]

Uma abordagem que promova um processo decisório coletivo e multissetorial, com a participação ativa da sociedade civil na criação de normas, pode beneficiar a comunidade em termos de expansão e difusão de conexões, conhecimentos, serviços e novas formas de comunicação.

Essa construção coletiva, aplicada em um ecossistema não somente global, mas também regional e local, seria capaz de oferecer grandes avanços na persecução de direitos dos usuários-cidadãos, respeitando práticas sociais comuns, tradições culturais e valores socialmente compartilhados.

Nesse sentido, pode-se perceber que, com adoção do GDPR e a atuação ativa da União Europeia, para estabelecer uma regulação global ao mundo digital, há um esforço para enxergar

[44] HESS, Charlotte; OSTROM, Elinor. Understanding Knowledge as a Commons: from theory to practice. Cambridge: The MIT Press, 2007.
[45] FILGUEIRAS, Fernando; ALMEIDA, Virgílio. Governance for the Digital World*:* neither more state nor more market. [S.I]: Springer International Publishing, 2020.p. 15.

os direitos humanos em perspectiva, mobilizando redes globais em favor da institucionalização do Constitucionalismo Digital.[46]

A adesão do Brasil à Convenção 108 sobre proteção de dados pessoais dialoga justamente com esta perspectiva. Sua ocorrência é um desafio complexo que exige a reflexão sobre as normas e valores que fundamentam a proteção de dados e os direitos humanos dentro do ordenamento jurídico brasileiro.

No Brasil, o processo de ratificação de um tratado internacional, que é regulado pela Constituição Federal de 1988, é complexo e envolve várias etapas.[47] Esse processo de ratificação é fundamental para garantir a conformidade do Estado brasileiro com suas obrigações internacionais e para proteger os direitos e interesses de seus cidadãos no cenário internacional.[48]

A não ratificação pelo país pode ter implicações significativas para a proteção de dados pessoais no país, impactando em sua imagem em relação ao seu compromisso com a proteção de dados, e em possíveis investimentos estrangeiros e acordos comerciais.

Outrossim, sem seguir padrões internacionais, pode haver dificuldades em garantir a segurança dos dados em transações internacionais.[49] É importante ressaltar que, apesar do Brasil ainda não ter ratificado a Convenção, o país tem tomado medidas significativas para reforçar sua agenda de proteção de dados.

---

[46] REDEKER, Dennis. Towards a European Constitution for the Internet? Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational Digital Constitutionalism, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European_Constitution.pdf. Acesso em: 31 jan. 2023. p.17.

[47] MEDEREIROS, Antônio Paulo Cachapuz de. A Constituição de 1988 e o poder de celebrar tratados. Revista de Informação Legislativa, v. 45, n. 179, p. 89-126, jul./set. 2008. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/160460/Constituicao_1988_poder.pdf?sequence=6&isAllowed=y. Acesso:em 02 fev. 2023.

[48] MEDEREIROS, Antônio Paulo Cachapuz de. A Constituição de 1988 e o poder de celebrar tratados. Revista de Informação Legislativa, v. 45, n. 179, p. 89-126, jul./set. 2008. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/160460/Constituicao_1988_poder.pdf?sequence=6&isAllowed=y. Acesso:em 02 fev. 2023.

[49] MARQUES, Fernanda Mascarenhas. Regulação do fluxo de dados pessoais entre fronteiras: os contornos e limites da decisão de adequação de países terceiros. 2020. 137 f. Dissertação (Mestrado) - Curso de Direito, Fundação Getulio Vargas, São Paulo, 2020. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29278/FMM.pdf?sequence=5&isAllowed=y. Acesso em: 15 fev. 2023.

Nesse âmbito, o país aprovou duas importantes legislações, o Marco Civil da Internet (MCI)[50] em 2014 e a LGPD em 2018. O propósito dessas legislações foi estabelecer limites à coleta de dados no território brasileiro.

Mesmo sem possuir status constitucional, o MCI atua como instrumento de regulação da Internet através de uma linguagem constitucional ao concentrar-se em princípios amplos que visam proteger os direitos e limitar o poder estatal on-line, podendo ser caracterizado como um marco normativo digital de teor constitucional.[51]

Entretanto, o MCI vem sendo questionado, principalmente no seu artigo 19º, que estabelece que provedores de aplicações de internet somente podem ser responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomarem as providências para tornar indisponível o conteúdo infrator.

Paralelamente, o Supremo Tribunal Federal (STF) passou a analisar o Tema n° 987, sobre a constitucionalidade do artigo 19 do MCI e o Tema n° 533, que discute o dever da empresa hospedeira de um site em fiscalizar e retirar do ar conteúdo publicado por usuários sem necessidade de intervenção do Judiciário.

Mais recentemente, os atos antidemocráticos de 08 de janeiro, reacenderam o debate sobre a influência descontrolada das plataformas digitais na esfera política. Evidenciou-se que a disseminação desenfreada de desinformação e conteúdos prejudiciais podem abalar a estabilidade política do país.[52]

É válido ressaltar, contudo, que o Art. 19 do MCI é um reflexo da própria estrutura e princípios que norteiam a internet, baseados na neutralidade, livre expressão e participação democrática. Nesse sentido, sua discussão e eventual modificação devem ser pautadas não somente em eventos pontuais, mas também considerando a essência desses fundamentos que guiam a rede mundial de computadores.

---

[50] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Online, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 jan. 2023.

[51] MONCAU, Luiz Fernando Marrey; ARGUELHES, Diego Werneck. The Marco Civil da Internet and Digital Constitutionalism. In: FROSIO, Giancarlo. Oxford Handbook of Online Intermediary Liability. Oxford: Oxford University Press, 2020. p. 189-213.

[52] Nesse sentido, temas relacionados à responsabilidade dos intermediários, sobretudo grandes plataformas entraram não somente na pauta do STF e de propostas de revisão do MCI, como também nas discussões envolvendo o PL 2630. Na prática, isso significa que se espera que empresas como Google, Facebook, Twitter e outras tomem medidas mais rigorosas para evitar a disseminação de desinformação e conteúdo prejudicial em suas plataformas, em vez de agir apenas quando direcionadas por ordens judiciais.

No que diz respeito à LGPD, a norma incorporou uma série de institutos, princípios e regras do GDPR. A LGPD especifica os direitos do titular da proteção de dados - arts. 17 e 18 - que devem ser aplicados em sintonia com os preceitos constitucionais, bem como com a normativa internacional.

Além disso, o Brasil reconheceu a proteção de dados como um direito fundamental, inclusive no meio digital, por meio da Emenda Constitucional nº 115/2022.[53] Nesse sentido, Sarlet entende que o Supremo Tribunal Federal (STF), por meio das Ações Diretas de Inconstitucionalidade (ADIs) 6387, 6389, 6390 e 6393, já havia reconhecido a matéria como tendo status de direito fundamental.[54]

Dessa maneira, essas normativas e decisões dialogam com a necessidade de uma resposta adequada aos desafios sociais atuais que exigem a reinterpretação de direitos e garantias fundamentais que restrinjam os abusos tanto do poder público quanto da esfera privada.[55]

O Brasil tem participado ativamente de discussões e acordos internacionais sobre proteção de dados,[56] como a Convenção de Budapeste, que prevê a criminalização de condutas relacionadas a ataques cibernéticos e a proteção de dados pessoais no contexto da investigação e repressão criminal.[57]

Apesar desses desafios, a abordagem brasileira para o enfrentamento desses problemas vem se destacando. No cenário internacional, o país tem sido um dos mais ativos na política digital global, e em diálogo com a resposta europeia, o governo brasileiro não busca se fechar em uma abordagem intraestatal, mas aumentar o diálogo internacional cooperativo.[58]

---

[53] BRASIL. Constituição (2022). 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. Online, Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 10 jan. 2023.

[54] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à proteção de dados. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 50.

[55] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à proteção de dados. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 50.

[56] KURBALIJA, Jovan. Uma introdução à Governança da Internet. São Paulo: Comitê Gestor da Internet no Brasil, 2016, p. 204.

[57] COUNCIL OF EUROPE. Convention on Cybercrime. Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/1680081561. Acesso em: 10 fev. 2023.

[58] KURBALIJA, Jovan. Uma introdução à Governança da Internet. São Paulo: Comitê Gestor da Internet no Brasil, 2016, p. 204.

A posição do Brasil em relação à adesão à Convenção 108 é um ponto importante a ser considerado na discussão sobre a proteção de dados pessoais no país. Atualmente, o Brasil é um país observador do Comitê da Convenção Internacional de Proteção de Dados Pessoais do Conselho da Europa.[59]

Uma adesão à Convenção pode trazer inúmeros benefícios para a proteção de dados no Brasil, como a possibilidade de estabelecer normas e princípios claros para a coleta, processamento e armazenamento de dados pessoais, aperfeiçoando o escopo já definido nas normativas de proteção de dados nacionais. Além disso, pode fomentar o desenvolvimento de boas práticas em relação à privacidade e proteção de dados no país.

Outro ponto a ser considerado são as implicações da adesão do Brasil à Convenção 108 para a proteção de dados pessoais no país. A Convenção estabelece uma série de normas e princípios para a proteção de dados pessoais, que podem contribuir para a criação de um ambiente mais seguro e confiável para usuários e empresas que lidam com informações pessoais.[60] A adesão também pode fortalecer a posição do Brasil no cenário global em relação à proteção de dados, o que pode ser especialmente importante em um mundo cada vez mais conectado e digitalizado.[61]

Isto estaria em consonância com seu esforço para aprimorar a governança digital, seria uma medida relevante e coerente com uma perspectiva de Constitucionalismo Digital. Internalizar a Convenção teria grande importância para fortalecer a proteção de dados pessoais no país, uma vez que os padrões internacionais estabelecidos pela Convenção 108 são referência na matéria e poderiam servir de norteador para a elaboração de políticas públicas na área.

Com relação a Convenção 108+, a mesma reflete essas mudanças tecnológicas e, portanto, oferece um quadro normativo mais atualizado e abrangente para a proteção de dados pessoais. Em um segundo momento, sua adesão seria consistente com a abordagem de

[59] COUNCIL OF EUROPE. Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers! 2018. Disponível em: https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers-. Acesso em: 20 dez. 2022.

[60] COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.

[61] BRANCHER, Paulo Marcos Rodrigues. Proteção internacional de dados pessoais. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em: 02 fev. 2023.

Constitucionalismo Digital do país, que visa proteger os direitos fundamentais dos cidadãos no ambiente digital.

Uma adoção combinada das duas convenções promoveria a proteção dos direitos à autodeterminação informativa e à proteção de dados dos cidadãos brasileiros, inclusive na era da tecnologia da inteligência artificial, que exige novas abordagens na proteção de dados pessoais.

Por fim, para que a proteção de seus cidadãos seja efetiva, é imperativo que haja uma proteção sólida dos direitos à autodeterminação informativa e à proteção de dados em outros lugares além da sua jurisdição. Portanto, a busca por soluções colaborativas é um passo importante para que o país caminhe em direção à proteção dos direitos dos usuários-cidadãos, promovendo a dignidade humana, garantindo a privacidade e a liberdade na era digital.

Considerações finais

Conforme explorado, a proteção de dados pessoais é cada vez mais importante em um momento em que a tecnologia vem se tornando cada vez mais essencial para o desenvolvimento da sociedade em todo o mundo. No Brasil, apesar a construção de marcos regulatórios para a proteção de dados pessoais e a criação da ANPD ainda há desafios a serem enfrentados.

A adesão do Brasil à Convenção 108 pode contribuir para o fortalecimento do escopo da proteção de dados pessoais no país, trazendo mais segurança e confiança para os usuários e empresas que lidam com informações pessoais, especialmente considerando a Convenção como parte do chamado "Constitucionalismo Digital".

É fundamental que o Brasil siga avançando na proteção dos dados pessoais de seus cidadãos, com medidas como a adesão à Convenção 108 e a criação de uma "LGPD Penal", para que se possa garantir a conformidade do Estado brasileiro com suas obrigações internacionais de proteção dos direitos humanos, especialmente àqueles relacionados ao mundo digital, tais como o direito à privacidade, à proteção dos dados e à autodeterminação informativa.

Com a adoção de padrões internacionais e a implementação de políticas públicas na área, haverá maior promoção de uma cultura de privacidade, da segurança e da dignidade humana na era digital, o que permite uma sociedade mais justa e equitativa para todos.

Referências bibliográficas

ALMEIDA, Eloísa Machado de; ESTELLITA, Heloisa (org.). *Dados, privacidade e persecução penal:* cinco estudos. São Paulo: Data Privacy Research, 2021. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31784/Dados%2C%20privacidade%20e%20persecu%C3%A7%C3%A3o%20penal.pdf?isAllowed=y&sequence=1. Acesso em: 05 jan. 2023.

BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em: 02 fev. 2023.

BRASIL. Constituição (2022). 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.* Online, Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 10 jan. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Online, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 dez. 2022.

BRASIL. Lei Nº 13.853, de 8 de julho de 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.* Online, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.* Online, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 jan. 2023.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. *International Review Of Law, Computers & Technology*, [S.I.], v. 33, n. 1, 2 jan. 2019. p. 5-6

COUNCIL OF EUROPE. *Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers !* 2018. Disponível em: https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers-. Acesso em: 20 dez. 2022.

COUNCIL OF EUROPE. Convention nº 108 de 28 de jan. de 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).* Strasbourg. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 23 dez. 2022.

COUNCIL OF EUROPE. *Convention on Cybercrime*. Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/1680081561. Acesso em: 10 fev. 2023.

COUNCIL OF EUROPE. *National information.* 2023. Disponível em: https://www.coe.int/en/web/data-protection/national-information. Acesso em: 20 fev. 2023.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law* [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuri

dico/article/view/1315. Acesso em: 25 fev. 2023.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno *et al*. *Tratado de Proteção de Dados Pessoais.* Rio de Janeiro: Forense, 2021.

FACHINETTI, Aline Fuke; CAMARGO, Guilherme. *Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil.* Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados. Acesso em: 20 jan. 2023.

FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the Digital World:* neither more state nor more market. [S.I]: Springer International Publishing, 2020.

GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards Digital Constitutionalism? mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. Disponível em: https://dash.harvard.edu/handle/1/28552582. Acesso em: 27 dez. 2022.

GROSSMANN, Luís Osvaldo. *ANPD começa a aplicar multas por infrações à LGPD a partir de fevereiro.* 2023. Disponível em: https://www.convergenciadigital.com.br/Governo/Legislacao/ANPD-comeca-a-aplicar-multas-por-infracoes-a-LGPD-a-partir-de-fevereiro-62379.html. Acesso em: 10 fev. 2023.

GUIMARÃES, João Alexandre; MACHADO, Lecio. *Comentários à lei geral de proteção de dados:* lei 13.709/2018 com alterações da MPV 869/2020. Rio de Janeiro: Lumen Juris, 2020.

HESS, Charlotte; OSTROM, Elinor. *Understanding Knowledge as a Commons*: from theory to practice. Cambridge: The MIT Press, 2007.

KURBALIJA, Jovan. *Uma introdução à Governança da Internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

LYON, David; ZUREIK, Elia. *Computers, surveillance, and privacy.* Minneapolis: University of Minnesota Press, 1996.

MARQUES, Fernanda Mascarenhas. *Regulação do fluxo de dados pessoais entre fronteiras: os contornos e limites da decisão de adequação de países terceiros*. 2020. 137 f. Dissertação (Mestrado) - Curso de Direito, Fundação Getulio Vargas, São Paulo, 2020. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29278/FMM.pdf?sequence=5&isAllowed=y. Acesso em: 15 fev. 2023.

MEDEREIROS, Antônio Paulo Cachapuz de. A Constituição de 1988 e o poder de celebrar tratados. *Revista de Informação Legislativa*, v. 45, n. 179, p. 89-126, jul./set. 2008. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/160460/Constituicao_1988_poder.pdf?sequence=6&isAllowed=y. Acesso:em 02 fev. 2023.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo Digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito,* v. 16, n. 1, jan.-abr. 2020.

MONCAU, Luiz Fernando Marrey; ARGUELHES, Diego Werneck. The Marco Civil da Internet and Digital Constitutionalism. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability***.** Oxford: Oxford University Press, 2020.

NATARAJAN, Aishwarya. *Dawn of a new era of global data protection?* 2021. Disponível em: https://voelkerrechtsblog.org/dawn-of-a-new-era-of-global-data-protection/. Acesso em: 10 jan. 2023.

REDEKER, Dennis. Towards a European Constitution for the Internet? *Bremen International Graduate School Of Social Sciences*: Comparative Institutionalization and Mobilization in European and Transnational Digital Constitutionalism, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European_Constitution.pdf. Acesso em: 31 jan. 2023.

SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A Autoridade Nacional de Proteção de Dados (ANPD) e os desafios tecnológicos: alternativas para uma estruturação responsiva na era da governança digital. *Revista Direitos Fundamentais & Democracia*, (S.I), v. 27, n. 3, p. 217-253, dez. 2022.
SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à proteção de dados. In: BIONI, Bruno *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

SILVA, Vanessa Junior da. *Proteção geral de dados: Comunidade Europeia x Brasil.* 2019. TCC (Graduação) - Curso de Direito, Universidade Univates, Lajeado, 2019. Disponível em: https://www.univates.br/bduserver/api/core/bitstreams/cb6348ff-35c6-4e20-aa9a-5fcfbb029b4d/content. Acesso em: 12 dez. 2022.

UNIÃO EUROPEIA. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados).* Jornal Oficial da União Europeia, Estrasburgo, 24/10/1995. Disponível em: <https://eur-lex.europa.eu/ legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 15 feb 2023.

TELES, Edson. Ação Política Híbrida e a Dissolução da Cidadania. *Revista de Filosofia Moderna e Contemporânea*, [S.I.], v. 8, n. 3, 31 jan. 2021. Biblioteca Central da UNB. http://dx.doi.org/10.26512/rfmc.v8i3.34494.

UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (RGPD)*. 27 abr. 2016.Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt#d1e2012-1-1>. Acesso em: 18 fev. 2023.

WE ARE SOCIAL. *Digital 2021:* global overview report. global overview report. 2021. Disponível em: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/. Acesso em: 27 nov. 2022.

ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

Elis Bandeira Alencar Brayner[1]

Resumo: Em 30 de novembro de 2022, o processo de adesão do Brasil à Convenção de Budapeste foi concluído, de modo a alterar o panorama nacional de repressão a crimes cibernéticos. A partir desse contexto, o presente trabalho buscou realizar revisão bibliográfica sobre a Convenção sobre Crimes Cibernéticos, compilar a legislação brasileira acerca do Direito Digital pré-existente e verificar a compatibilidade entre ambos. Adiante, foi realizada uma análise do contexto histórico no qual foi criada a Convenção de Budapeste, seu conteúdo, a posição hierárquica dos tratados internacionais no Brasil e das normas de controle de delitos no meio virtual. Observou-se que há estreita harmonia entre as normas internas e a Convenção sobre Crimes Cibernéticos e, mais que isso, a adesão do Brasil representa um avanço na responsabilização penal de agentes que praticam condutas criminosas na internet.

Palavras-chave: crimes cibernéticos; Convenção de Budapeste; Direito Digital; internet.

Abstract: *On November 30, 2022, the Brazilian adhesion process to the Budapest Convention was concluded, thus changing the national framework of repressing cybercrime. Within this scenario, this paper seeks to conduct a literature review on the Convention on Cybercrime, compile the pre-existing Brazilian legislation on Digital Law and verify the compatibility between the two. Furthermore, an analysis of the historical context in which the Budapest Convention was created, as well as its content, the hierarchical position of international treaties in Brazil and the rules of crime control in the virtual environment was performed. The study observed that there is a strong harmony between the domestic norms and the Convention on Cybercrime and, moreover, Brazil's adhesion represents an advance in the criminal liability of agents who practice criminal conducts on the internet.*

[1] Elis Bandeira Alencar Brayner é pós-graduanda em Direito Digital e Proteção de Dados do Instituto Brasiliense de Direito Público (IDP). Bacharela em Direito pela Universidade de Brasília (UnB). Pesquisadora do Privacy Lab - Centro de Direito, Internet e Sociedade (CEDIS) do IDP. Coordenadora de Comunicação do Observatório da LGPD/UnB. Estagiária da Pós-Graduação da Defensoria Pública da União no 5º Ofício Cível. Advogada.

***Keywords*:** *cybercrimes; Budapest convention; Digital Law; internet*

Introdução

Em 21 de novembro de 2001, foi aberta para assinatura, em Budapeste, a Convenção do Conselho Europeu sobre o Cibercrime, o primeiro acordo internacional que tratou explicitamente sobre essa espécie de crimes, também conhecida como Convenção de Budapeste. Este tratado entrou em vigor apenas em 2004 (COUNCIL OF EUROPE, 2017, *online)* e possui como objetivo principal:

> (...) a repressão dos crimes cibernéticos com a utilização de normas eficientes e práticas, mediante as quais a sociedade se sinta segura para se desenvolver, sem a interferência daqueles que procuram por meios escusos conseguir lucros, mesmo que causem prejuízos monetários e danos morais a terceiros. (FERNANDES, 2013, p.175)

Durante a convenção de Budapeste, o espaço cibernético foi definido como um espaço comum utilizado por aqueles que trafegam na internet a partir da conexão com os serviços de comunicação e informação (BOITEUX, 2004, p. 170). Ou seja, é nesse ambiente que os crimes cibernéticos ou cibercrimes ocorrem.

Os crimes digitais tornaram-se progressivamente mais relevantes e perigosos com a evolução da tecnologia da informação, que estão presentes na rotina de indivíduos espalhados por todo o globo. De acordo com dados de um relatório da União Internacional de Telecomunicações, em 2022, 67% da população mundial estava conectada à internet.

Dentre os casos recentes de crimes virtuais no Brasil com repercussão nacional, cita-se o ataque ocorrido em novembro de 2020 ao sistema eletrônico do Superior Tribunal de Justiça que resultou no bloqueio de acesso aos processos que tramitam na egrégia corte e aos e-mails de seus funcionários (ALVES, Paulo, 2020, n.p.). Até o presente momento, as investigações do referido crime ainda não foram concluídas pela Polícia Federal.

Nesse contexto, buscar-se-á analisar o disposto no ordenamento jurídico brasileiro acerca do Direito Digital e na Convenção de Budapeste, à qual o Brasil aderiu no final de 2022. Esse artigo dedica-se a averiguar se, de fato, houve algum benefício com a adesão ao tratado internacional.

1. A Convenção de Budapeste e a tipificação penal de crimes cibernéticos

O primeiro registro da utilização do termo "crime cibernético" ocorreu em 1997, antes mesmo da Convenção de Budapeste, em 1997, durante um encontro dos líderes do G-8, grupo formado pelos países considerados mais desenvolvidos econômica e industrialmente, responsável pela adoção dos Dez Princípios do Combate ao Cibercrime (ANTUNES, 2022, p. 25). Esse termo continua sendo atual e utilizado pela literatura dedicada ao tema e, de acordo com as lições de NASCIMENTO (2021, n.p.), pode ser definido como:

> (...) todas as condutas típicas, antijurídicas e culpáveis praticadas no âmbito digital ou que estejam envolvidas com a informação digital através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares, smartphones e tablets. Estes crimes se propagam através da internet, em razão das diversificadas maneiras de interação entre indivíduos que surgiram ao longo do tempo.

O texto Convenção de Budapeste é formado por 48 artigos, que se organizam em quatro capítulos, quais sejam: *I) Terminologia*; *II) Medidas a Tomar a Nível Nacional*; *III) Cooperação Internacional;* e *IV) Disposições Finais*, respectivamente. Nele, o cibercrime foi tipificado como infrações contra sistemas e dados de tecnologias da informação (Capítulo II, Título I), infrações relacionadas com computadores (Capítulo II, Título II), infrações relacionadas com o conteúdo, como a pornografia infantil (Capítulo II, Título III) e infrações relacionadas com a violação de direitos autorais (Capítulo II, Título IV), cujas proposituras estão adentradas em Direito Penal Material (CONVENÇÃO DE BUDAPESTE, 2001).

Hoje, o Tratado possui 68 países signatários do Tratado, que também é utilizado por outros 156 países como fonte de orientação em suas legislações nacionais (COUNCIL OF EUROPE, 2017, *online)*. A seguir, serão detalhados o contexto histórico no qual surgiu esse documento, seu conteúdo e a posição hierárquica dos tratados internacionais no ordenamento jurídico brasileiro.

1.1. Contexto histórico

A primeira tentativa de harmonizar as leis sobre crimes cibernéticos ocorreu na Europa em 1989, por meio da publicação de diretrizes para os legisladores dos Países-membros do Conselho Europeu, denominada Recomendação R(89)9.

Essas orientações consistem numa lista de oito infrações específicas relativas a computadores, sendo elas: fraude informática, falsificação informática, danos a dados ou programas de computador, sabotagem informática, acesso não autorizado, interceptação não autorizada, reprodução não autorizada de uma topografia. A referida lista era composta ainda por quatro delitos facultativos: alteração de dados ou programas de computador, espionagem de computador, uso não autorizado de um computador, uso não autorizado de um programa de computador protegido (GROTTO, 2010, p. 4).

Não obstante, em 1997, a União Europeia constatou em relatório que as diretrizes da Recomendação R(89)9 não haviam alcançado a compatibilização visada. Isto é, a despeito da recomendação, as Nações-membros do Conselho Europeu continuavam com discrepâncias expressivas quanto às suas legislações sobre crimes virtuais, de modo a se fazer imprescindível a criação um tratado que permitisse uma cooperação internacional efetiva e harmônica (GROTTO, 2010, p. 5), nas palavras de um dos membros do Conselho Europeu, Dr. Henrik Kaspersen (KASPERSEN, 1997, p. 104 a 106):

> (...) há Estados-membros que não implementaram (a Recomendação) de modo algum, enquanto outros apenas implementaram um certo número de diretrizes ou não seguiram determinada diretriz pertinente ao caso.

No ponto, insta destacar que a harmonia de leis acerca de crimes cibernéticos é essencial, haja vista que a falta de dupla criminalidade, por exemplo, impede que as investigações que envolvem vários países tenham sucesso (GARCIA, 2004, PICOTTI, 2005, n.p.). Sendo assim, em novembro de 1996, o Comitê Europeu para Problemas Criminais reuniu um conjunto de especialistas para que um tratado internacional fosse instituído de forma a solucionar a questão dos crimes digitais (CSONKA, 2004, p. 247).

O resultado desse encontro de especialistas é precisamente a Convenção de Budapeste, que foi assinada de imediato por 26 Estados-membros do Conselho Europeu e quatro Estados

não membros que participaram ativamente da redação do tratado internacional, quais sejam Estados Unidos, Canadá, Japão e África do Sul (COUNCIL OF EUROPE, 2017, *online)*.

1.2. A Convenção de Budapeste

Produto de quatro anos de trabalho intenso do comitê de especialistas em cibercrimes, a Convenção de Budapeste foi responsável por (i) estabelecer o conceito de certos delitos virtuais, possibilitando definições comuns entre diferentes nações; (ii) definir regras acerca de poderes investigativos e de persecução penal e; (iii) determinar formas de cooperação entre países, tanto tradicionais quanto novas, acelerando e tornando mais efetiva a investigação de delitos (BOITEUX, 2004, p. 170). A seguir, serão examinadas cada uma dessas melhorias previstas neste tratado internacional.

A primeira parte da Convenção de Budapeste dedica-se a definir e tipificar o cibercrime, possibilitando a dupla criminalidade, ou seja, que a conduta seja considerada um delito em mais de um país e possa haver uma organização no combate à criminalidade transnacional (ALVES, 2018, p. 11). Salienta-se que todos os crimes previstos no tratado são dolosos, em outras palavras, apenas são punidas as condutas em que o agente teve a intenção de produzir o resultado ou assumiu o risco de produzi-lo (BOITEUX, 2004, p. 171). Os delitos previstos no tratado se amoldam em quatro categorias diferentes.

O tratado prevê como categoria inicial as "ofensas contra a confidencialidade, integridade e disponibilidade de dados ou sistemas de informação" (CONVENÇÃO DE BUDAPESTE, 2001). São inseridos nessa categoria os delitos que possuem como alvo o sistema informático ou os dados, ligados intrinsecamente ao ambiente informático no qual ocorrem (CSONKA, 2004, p. 22).

A segunda categoria de delitos abrange as versões computadorizadas de fraude e falsificação, que consistem essencialmente em manipulações de *input* (entrada), ou seja, dados incorretos inseridos no espaço virtual por manipulação de programas ou interferências no processamento de dados (CSONKA, 2004, p. 27).

A terceira categoria é aquela relativa à pornografia infantil, que foi considerada pelo Conselho Europeu como uma das mais perigosas (COUNCIL OF EUROPE, 2000, n.p.).

A quarta e última categoria de infrações refere-se às violações de direitos autorais e afins por meio de redes de computadores. No ponto, sublinha-se que as infrações aos direitos

de propriedade intelectual são as que mais comumente são cometidas na internet, podendo causar danos substanciais (CSONKA, 2004, p. 32).

No que tange à segunda parte da Convenção de Budapeste, que define os poderes investigativos e de persecução penal, o tratado lida com: preservação acelerada de dados de computador armazenados; conservação e divulgação parcial de dados de tráfego; ordem de produção; consulta de sistemas computadorizados; apreensão de dados de computador armazenados; levantamento de dados de tráfego em tempo real e; interceptação de dados de conteúdo (CSONKA, 2004, p. 32). Essa seção viabiliza a repressão de crimes informáticos.

A parte final da Convenção busca implementar um procedimento de cooperação internacional célere e concreto, que deve ocorrer "da forma mais extensa possível" (CONVENÇÃO DE BUDAPESTE, 2001). Uma inovação considerável prevista é a criação da base legal relativa a uma rede internacional de assistência específica ao crime informático, uma estrutura de pontos de contato nacional disponível permanentemente, "rede 24/7" (CSONKA, 2004, p. 48).

1.3. *Status* dos tratados internacionais no Direito brasileiro

Antes de adentrar no tema da adesão do Brasil à Convenção de Budapeste, é importante compreender a posição que os tratados internacionais ocupam na hierarquia das normas do Direito brasileiro.

Apesar de serem hierarquicamente inferiores à Constituição Federal brasileira[2], de sorte a não poderem dela divergir, os tratados internacionais posicionam-se em nível superior ao das leis ordinárias e complementares, pois, consoante preceituado João Bosco Lee "para que uma regra de direito internacional possa ser eficaz no território do país que ratificou o tratado, deve essa regra prevalecer sobre o direito interno" (BORGES, 2007, p. 230).

Da mesma maneira, o artigo 27 da Convenção de Viena sobre o Direito dos Tratados, firmada em 23 de maio de 1969, estabelece que um país não pode utilizar suas normas de direito interno "para justificar o inadimplemento de um tratado". Sublinha-se que o Brasil se

[2] Ressalvados aqueles que versarem sobre direitos humanos e que forem aprovados sob o rito previsto no art. 5º, §3º da Constituição Federal, os quais possuem status de emenda constitucional.

comprometeu, em 14 de dezembro de 2009, a cumprir essa convenção por meio do Decreto nº 7.030.

O Direito Internacional Público consiste no conjunto de normas autônomas que guiam as relações entre Estados soberanos, sendo os tratados os instrumentos responsáveis pela estruturação dessas relações, disciplinando as condutas entre diferentes nações. Em conformidade com as lições de REZEK (2000, p.14), "Tratado é todo acordo formal concluído entre sujeitos de direito internacional público, e destinado a produzir efeitos jurídicos".

Nesta oportunidade, explica-se resumidamente o rito de incorporação dos tratados internacionais ao ordenamento jurídico brasileiro, após as negociações entre os países, assim como disposto na Constituição Federal. No Brasil, como regra geral, o texto original é enviado ao Congresso Nacional, sendo discutido inicialmente na Câmara dos Deputados e, caso aprovado, seguindo ao Senado Federal (FLORIANI, 2019, p. 255 e 256).

Havendo aprovação nas duas casas do Congresso Nacional, o presidente do Senado promulga um Decreto Legislativo acerca da aprovação do texto do tratado, que deve ser analisado pelo Poder Executivo para definir se este tratado será ratificado ou não (BRASIL, CF, Senado, 1988). Frisa-se que o Poder Executivo não possui prazo ou obrigatoriedade de ratificar o tratado internacional, sendo um ato discricionário (FLORIANI, 2019, p. 256).

Em uma sociedade globalizada, o instrumento dos tratados internacionais ganha cada vez mais relevância. Quando se considera os crimes cibernéticos, essa afirmação é ainda mais palpável, pois o mundo virtual é capaz de romper fronteiras nacionais e integrar localidades fisicamente distantes (PINHEIRO, 2007, p. 45).

2. Crimes digitais no Brasil

A prática de crimes cibernéticos tem crescido com o desenvolvimento da Era da Informação em todo o mundo. De acordo com projeções realizadas pelo Fórum Econômico Mundial, os custos globais decorrentes desses delitos em 2023 serão de 8 trilhões de dólares e, em 2025, 10.5 trilhões de dólares. Hoje, se comparado às maiores economias do globo, o cibercrime representaria, em números, a terceira maior economia do mundo, atrás apenas dos Estados Unidos e da China (WORLD ECONOMIC FORUM, 2023).

O Brasil está incluído nessa tendência. Segundo dados fornecidos pelo diretor da Confederação Nacional de Seguradoras (CNseg), Alexandre Leal, o país foi o segundo país que

mais sofreu com crimes cibernéticos em 2022: foram aproximadamente cem bilhões de tentativas de ataques cibernéticos, número de ocorrências apenas menos do que o do México, no qual foram detectadas 187 bilhões de tentativas (FIDESRJ, 2023). Destarte, considerando que o Estado possui como função proteger os bens jurídicos fundamentais para a vida em sociedade, exercendo o monopólio do Direito Penal, a tipificação de crimes cibernéticos se revela essencial (JESUS, 2014, p. 46).

Iniciado em junho de 2018, o processo de adesão do Brasil à Convenção de Budapeste foi concluído em 30 de novembro de 2022, quando o País, em conjunto com o Conselho Europeu, depositou sua carta de adesão à Convenção de Budapeste (GOV, 2022). O próximo capítulo pretende estudar as leis já instituídas no Brasil acerca dos crimes digitais e os aspectos de sua adesão a esse tratado internacional.

2.1. Compilado legislativo nacional

O ordenamento jurídico brasileiro, até o presente momento, apresenta apenas três leis que tutelam os conflitos advindos da má utilização da internet: a Lei Carolina Dieckmann (Lei 12.737/12), a Lei Azeredo (Lei 12.735/12) e o Marco Civil da Internet (Lei 12.965/14), que altera o Código Penal (COLTRO, 2021, p. 108). As duas primeiras leis foram criadas a partir de situações específicas que resultaram em forte comoção social.

A Lei 12.737/2012 originou-se do fato de Carolina Dieckmann, atriz de renome nacional, ter sido vítima de invasão em seu computador com a consequente publicação de 36 fotos íntimas suas na internet. Em razão da rápida e significativa repercussão midiática do fato, alguns especialistas afirmam que a lei foi aprovada em regime de urgência, sem tempo hábil para o adequado debate sobre o tema em pauta, fato que teria resultado em uma norma com previsões excessivamente abertas e lacunas de definições técnicas imprecisas (CIDRÃO, 2018, p. 72). Confira-se, *in verbis*, a conduta tipificada:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput .
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Os críticos desse diploma legal, majoritariamente, consideram insuficiente a pena máxima estabelecida para o delito, que viabiliza a adoção do rito sumaríssimo dos juizados especiais e, por consequência, facilita "a suspensão condicional do processo, a conciliação, a composição civil dos danos e a transação penal" (GARCIA, 2017, p. 51). Ademais, o fato de a pena ser breve também resulta em curto prazo de investigação do delito, fazendo com que diversos crimes não sejam punidos em razão da prescrição (LIRA, 2014, p. 66).

De seu lado, a Lei Azeredo recebeu este nome em razão do autor do seu projeto (PL nº 84/1999) o Senador Eduardo Azeredo. O Projeto de Lei tipifica treze condutas como crimes virtuais, incluindo (COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, 2006, p. 4):

> (...) obrigar a todos os que desejarem acessar uma rede de computadores a identificar-se e cadastrar-se. Do outro lado, pretende obrigar a todos os que dispõem de rede a somente admitir como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que seja autenticado consoante validação positiva dos dados cadastrais

> previamente fornecidos, mediante contrato formalizado perante o fornecedor do serviço.

O PL nº 84/1999, à época em que foi apresentado, recebeu o apelido de "AI5 Digital" pela bancada do Partido dos Trabalhadores que o acusava de "incitar a criação de um estado policial na internet" (MOLITOR, 2017, p. 89).

Em seus quase 13 anos de tramitação, o projeto original sofreu diversas alterações e cortes, resultando na Lei 12.735/12, nota-se que sua publicação ocorreu no mesmo ano da Lei Carolina Dieckmann, após a grande repercussão do vazamento de fotos íntimas da atriz. Em sua versão final, a lei aprovada levantou apenas dois pontos (MOLITOR, 2017, p. 90):

> a criação de delegacia de polícia especializada em crimes informáticos e inclui na legislação crimes de preconceito de raça ou cor para que a publicação seja interrompida.

Ulteriormente, foi sancionado o Marco Civil da Internet, em 23 de abril de 2014, mesmo ano em que foi revelado o esquema de espionagem do governo norte-americano, no qual foram grampeados 29 telefones de líderes políticos do Brasil (G1, 2015).

A Lei nº 12.965 de 2014 foi essencial para a regulação da utilização da internet no Brasil pela "previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado" (HUDSON, 2014, p. 1).

O texto do Marco Civil da Internet apresenta 32 artigos divididos em cinco capítulos, são eles: (I) apresentação dos princípios e finalidades da utilização da internet no Brasil, (II) identificação dos direitos e garantias dos usuários, (III) fornecimento de conexão de aplicativos no ambiente virtual, (IV) a atuação do Poder Público na regulação da internet e (V) as disposições finais (ANTUNES, 2022, p. 64 e 65). No entanto, não há previsão na lei sobre a responsabilização penal dos agentes envolvidos nas más condutas.

2.2. Aplicação da Convenção de Budapeste no combate aos crimes digitais no Brasil

Consoante exposto anteriormente, a Convenção sobre Crimes Cibernéticos tipificou dez condutas diferentes como criminosas, que devem ser observadas pelos países signatários (DUARTE, 2022, p. 22).

Um dos pontos positivos da adesão do Brasil a esse tratado internacional é sua compatibilidade com as normas internas, consoante demonstrado pelo Conselho Europeu, em tabela elaborada em 2020:

Tabela 1: Correlação entre a Convenção de Cibercrimes e a lei penal brasileira.

Prescrições legais sobre a Convenção de Crimes Cibernéticos		**Prescrição penal no direito brasileiro: Código Penal (CP), Lei de Propriedade intelectual de programa de computador (Lei nº 9.609/98), Estatuto da Criança e do Adolescente (ECA), Norma de Interceptação de Comunicações Telefônicas e Informáticas (Lei nº 9.296/96).**	
Artigo 2	**Acesso ilegal.**	Artigo 154-A e 154-B (CP)	É uma invasão de um dispositivo informático (público ou privado).
Artigo 6	**Uso abusivo de dispositivo digital.**		
Artigo 3	**Interceptação ilegal.**	Artigo 10 (Lei nº 9.296/96)	Interceptação sem autorização judicial.
Artigo 4	**Interferências em dados informáticos.**	-	Sem previsão.
Artigo 5	**Interferência em sistemas.**	Artigo 313-B (CP).	Modificação ou alteração ilícita de sistemas de informação.
Artigo 7	**Falsidade informática**	Artigo 297 (CP)	Falsificação de documentos públicos.
		Artigo 298 (CP)	Falsificação de documentos particulares.
		Artigo 298, parágrafo único (CP)	Falsificação de cartões de crédito ou débito
		Artigo 313-A (CP)	Inserção de dados falsos em sistemas de

			informações
Artigo 8	**Fraude Informática**	Artigo 171 (CP)	Estelionato.
		Artigo 155 (CP)	Furto por fraude.
		Artigo 240 (ECA)	É a produção ou reprodução de conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241 (ECA)	Oferecer, comercializar, publicar ou distribuir conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241-A (ECA)	Oferecer, comercializar, publicar ou distribuir conteúdo explícito envolvendo crianças ou adolescentes, usando computadores ou redes.
		Artigo 241-B (ECA)	Comprar, possuir ou armazenar conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241-C (ECA)	Simular a participação de crianças ou adolescentes em conteúdos explícitos.
Artigo 10	**Infrações relacionadas com a violação dos direitos autorais e direitos conexos.**	Artigo 184 (CP). Artigo 2 (Lei nº 9.609/98).	É uma violação de direitos autorais e direitos relacionados.
Artigo 11	**Tentativa e ajuda ou cumplicidade.**	Artigo 14 (CP)	A tentativa de produzir conduta criminosa é punível.

Fonte: DUARTE, 2022, p. 22

Insta destacar que o Brasil não possui, até o momento, uma compatibilidade completa com a Convenção de Budapeste haja vista não ter assinado o protocolo adicional concernente

à criminalização de condutas de racismo e xenofobia utilizando-se de sistemas informáticos (CONSELHO DA EUROPA, 2022).

Não obstante, o ordenamento jurídico brasileiro apresenta normas compatíveis com as previsões normativas de processo penal dispostas no tratado internacional (CONSELHO EUROPEU, 2022), veja-se:

Tabela 2: Leis processuais penais brasileiras que atendem às determinações da Convenção de Cibercrimes.

Prescrição processual penal no direito brasileiro: ● Código de Processo Penal (CPP) ● Marco Civil da Internet (MCI) ● Lei de Organização Criminosa (Lei nº 12.850/2013) ● Norma de Interceptação de Comunicações Telefônicas e Informáticas (Lei nº 9.296/96) ● Resolução 596/2012 da ANATEL	
Artigo 10 (MCI).	Permite que autoridades policiais e Ministério Público solicitem diretamente aos prestadores de serviços a concessão de acesso aos dados de assinantes dos usuários, isso não inclui endereços IP que necessitam de dependam de ordem judicial.
Artigo 10, §3º (MCI).	Prevê que é necessária uma ordem judicial para que os provedores disponibilizem registros de conexão, bem como conteúdo armazenado de comunicações privadas.
Artigo 240 (CPP)	Fala sobre busca e apreensão tradicionais, mas que também são utilizadas para busca e apreensão de dados informáticos armazenados.
Lei 9.296/1996	Regulamenta a interceptação de comunicação, permitindo a interceptação em sistemas telefônicos e de informática no âmbito de investigações criminais. Essa interceptação está condicionada por ordem judicial e o pedido deve ser justificado por suspeita razoável do crime e pela

	impossibilidade de obtenção de prova por outros meios.
Artigo 10-A (Lei nº 12.850/2013)	Inclui e regulamenta a possibilidade de infiltração virtual de agentes policiais.
Resolução 596/2012 (ANATEL)	Permite que o órgão solicite diretamente às prestadoras de serviços o acesso às informações da conta e aos registros de chamadas dos usuários.
Artigo 10 (MCI).	Permite que autoridades policiais e Ministério Público solicitem diretamente aos prestadores de serviços a concessão de acesso aos dados de assinantes dos usuários, isso não inclui endereços IP que necessitam de dependam de ordem judicial.

Fonte: DUARTE, 2022, p. 24

Para além da compatibilidade entre o tratado internacional e a legislação pátria, a adesão do Brasil à Convenção de Budapeste também representa uma grande mudança do país com relação à cooperação internacional. Considerando que a cooperação jurídica entre nações é uma ferramenta fundamental na repressão dos crimes cibernéticos, esse avanço é positivo para que o Brasil possa tornar mais efetivo o controle de condutas delituosas no meio virtual (VERONESE e CALABRICH, 2022).

Considerações Finais

Apesar de ser um tema discutido desde 1989 em convenções internacionais, a iniciativa brasileira de combater cibercrimes tardou a aparecer e não se mostrou suficiente para responsabilizar os agentes responsáveis pelas más condutas, o que pode ser atestado a partir dos dados apresentados acima sobre o aumento desses crimes no Brasil. Da mesma maneira, ainda que duas leis tenham sido promulgadas nesse sentido em 2014 no país, houve um foco específico e motivado mais pela pressão social do que por uma conscientização geral sobre os perigos envolvendo a utilização do ambiente virtual.

Por outro lado, a Convenção de Budapeste é a norma internacional mais completa, específica e com a maior quantidade de países signatários sobre este tema, de sorte que pode

ser considerada um instrumento eficaz para a investigação e repressão de crimes digitais. Isto posto, a adesão do Brasil a esse tratado revela-se como um progresso na tipificação penal dos delitos cometidos na internet, o que é esperado há algum tempo por diversas autoridades brasileiras.

A Convenção sobre Crimes Cibernéticos é bastante condizente com a base de Direito Penal e Processual Penal brasileira e, por isso, o que poderia representar uma mera adesão a um tratado, em realidade traduz uma solidificação das discussões sobre estes crimes no Brasil. Espera-se que, em breve, o Brasil possa apresentar ainda mais iniciativas para a repressão efetiva dos crimes digitais a fim de acompanhar harmonicamente o progresso mundial no que concerne à regulamentação do ambiente virtual.

Referências bibliográficas

ALVES, Ana Abigail Costa Vasconcelos; MUNIZ, Antônio Walber Matias; CIDRÃO, Taís Vasconcelos. A oportuna e necessária aplicação do direito internacional nos ciberespaços: uma avaliação sobre a convenção de Budapeste. V. 1, 2018.

ALVES, Paulo. Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso [Online]. Techtudo. 2020. Disponível em: < https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml Acesso em 29 de jan. 2023.

ANTUNES, Priscila Lucas. Da tipificação penal dos ataques cibernéticos no contexto da sociedade de risco: uma abordagem a partir da convenção de Budapeste. *Repositório Institucional da Universidade Federal de Santa Catarina*, 2022. Disponível em: <https://repositorio.ufsc.br/handle/123456789/232487>. Acesso em 19 de jan. 2023.

BRASIL. Constituição da República Federativa do Brasil. 1988.

BRASIL. Decreto nº 7.030/2009. Promulga a Convenção de Viena sobre Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos artigos 25 e 66. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7030.htm>. Acesso em: 23 de fev. 2023.

CYBERCRIME mobilizes insurance market. *FIDESRJ*, 17 de abr. 2023. Disponível em: <https://fidesrio2023.com.br/en/2023/04/17/cybercrime-mobilizes-insurance-market/#:~:text=The%20technical%20director%20of%20the,where%20there%20were%20187%20billion.>. Acesso em 27 de junho de 2023.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. *Revista Brasileira de Ciências Criminais*. São Paulo: Revista dos Tribunais, 2004.

BORGES, José Souto Maior. *Curso de Direito Comunitário*. 2. ed. São Paulo: Saraiva, 2009.

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira: The timely and necessary

implementation of International Law in the ciberspace: from the Budapest Convention to Brazilian legislation. *Brazilian Journal of International Relations*, v. 7, n. 1, p. 66-82, 2018.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. CRIMINALIDADE DIGITAL NO BRASIL: A PROBLEMÁTICA E A APLICABILIDADE DA CONVENÇÃO DE BUDAPESTE. *Revista Em Tempo*, v. 21, n. 1, p. 104-123, 2021.

COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, Parecer sobre e o Projeto de Lei da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática, 2006. Disponível em: <https://www.safernet.org.br/site/sites/default/files/PLS_Azeredo-CCJ-versao-de-19-08-2006.pdf>. Acesso em 5 de mar. 2023.

CONSELHO EUROPEU. Chart of signatures and ratifications of Treaty 185. 16 jun. 2017. Disponível em: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>. Acesso em 21 de jan. 2023.

CONSELHO EUROPEU. Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime. Estraburgo. Disponível em: <https://www.coe.int/en/web/cybercrime/protocol-consultations> Acesso em 7 de mar. 2023.

CONSELHO EUROPEU. Country Wiki [Online]. Estraburgo. 2021. Disponível em: <https://www.coe.int/en/web/octopus/country-wiki> Acesso em: 7 de mar. 2023.

CONSELHO EUROPEU. Minutes of the Committee PC-CY, 2000 (unpublished)

CONVENÇÃO DE BUDAPESTE. Convenção sobre o Cibercrime. 2001. Disponível, em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf >. Acesso em 17 de jan. 2023.

CSONKA, Peter. The council of europe's convention on cyber-crime and other European initiatives. Revue internationale de droit pénal 2006/3-4 (Vol. 77), p. 473 a 501. Disponível em: <https://doi.org/10.3917/ridp.773.0473>. Acesso em 2 de mar. 2022.

DUARTE, Ana Luísa Vieira. Análise do encaixe da convenção de Budapeste no ordenamento jurídico brasileiro. 2022.

EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks. *G1*, 2015. Disponível em: <https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. Acesso em 4 de mar. 2023.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. *Revista da Faculdade de Direito da UFMG*. Belo Horizonte, n.62, p.139-178, jan/jun. 2013.

FLORIANI, Lara Bonemer Rocha; SANTOS, Luccas Farias. A hierarquia dos tratados internacionais e seus reflexos jurídicos e extrajurídicos. *Revista Direitos Sociais e Políticas Públicas–Unifafibe*, v. 7, n. 1, 2019.

GARCIA, Alline Tavares. O DIREITO À INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann. 2017.

GARCIA, O.M. La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime. In Il diritto penale dell'informatica nell'epoca di

internet, di L. Picotti. Padova: Cedam, 2004.

GROTTO, Marco. "Council of Europe Convention on cybercrime and its ratification in the Italian legal system." Sistema Penal & Violência 2010.2 (2010): 5.

HENRIK W. K. KASPERSEN, Implementation of Recommendation No R (89) 9 on computer-related crime, Report prepared for the European Committee on Crime Problems, doc. CDPC (97) 5 (não publicado), Strasbourg, 1997, p. 104 a 106).

HUDSON, Alex. O Marco Civil da Internet. Disponível em: <http://rbrj.com.br/tecnologia/>. Acesso em 27 de fev. 2023.

JESUS, Damásio de. *Direito Penal, volume I: parte geral*. 35. ed. São Paulo: Saraiva, 2014.

LIRA, Leide de Almeida. Lei Carolina Dieckmann: (in) eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos. Conteudo Juridico, Brasilia-DF: 01 jul 2014, 06:45. Disponivel em: <https://conteudojuridico.com.br/consulta/Artigos/40026/lei-carolina-dieckmann-in-eficacia-na-protecao-dos-direitos-fundamentais-a-intimidade-e-a-vida-privada-em-face-da-pena-cominada-aos-delitos-informaticos>. Acesso em 07 de mar. 2023.

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina. BREVE PANORAMA SOBRE A LEGISLAÇÃO APLICADA NOS CRIMES ELETRÔNICOS. *Revista de Direito, Governança e Novas Tecnologias*, v. 3, n. 2, p. 81-96, 2017.

NASCIMENTO, Samir de Paula. *Cibercrime:* Conceitos, modalidades e aspectos jurídicos penais. Âmbito Jurídico, 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitosmodalidades- e-aspectos-juridicos-penais/>. Acesso em: 20 de fev. 2023.

NOTA À IMPRENSA Nº 186. Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública – Adesão do Brasil à Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: <https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica-2013-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico-celebrada-em-budapeste-em-23-de-novembro-de-2001>. Acesso em 30 de nov. 2022.

PINHEIRO, Patrícia P. Direito Digital. 2. ed. São Paulo: Saraiva, 2007.

REZEK, José Francisco. Direito Internacional Público: curso elementar. 8. ed. rev. atualizada. São Paulo. Saraiva, 2000.

SENADO FEDERAL. Lei nº 12.737/2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_

ato2011-2014/2012/lei/l12737.htm>. Acesso em: 6 de mar. 2023.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÃO - UIT. Relatório Global de Conectividade 2022. Disponível em: <https://www.itu.int/hub/publication/d-ind-global-01-2022/#> Acesso em 5 de mar. 2023.

VERONESE, Alexandre. CALABRICH, Bruno. Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional

Cooperation for Investigations and Prosecutions. 2022. WORLD ECONOMIC FORUM, Global Cyber Security Outlook, 2023. Disponível em: <https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf >. Acesso em 5 de mar. 2023.


OBSERVATÓRIO DA
LGPD
UNIVERSIDADE DE BRASÍLIA