Evolução legislativa do direito digital: a influência europeia na Lei Geral de Proteção de Dados e na criação da Autoridade Nacional de Proteção de Dados

Legislative evolution of digital law: the European influence on the General Data Protection Law and the creation of the National Data Protection Authority

Clara Amédée Péret Motta[1]

RESUMO

Este artigo busca analisar a Lei nº 13.709/2018, chamada de Lei Geral de Proteção de Dados, que entrou em vigor no dia 18 de setembro de 2020, a fim de melhor compreender a influência que o Regulamento Geral de Proteção de Dados, norma reguladora da União Europeia, teve na lei brasileira. Será abordada, inicialmente, a evolução do Direito Digital no Brasil, por meio de uma análise do arcabouço legislativo preexistente, que tratava do tema a fim de contextualizar o desenvolvimento do assunto no Brasil até chegar nos dias atuais, em que será analisada a Autoridade Nacional de Proteção de Dados, sua natureza jurídica e atividades que já estão sendo desempenhadas. Foram levados em conta vários artigos e todo o material educativo divulgado pela ANPD para, ao final, comprovar e justificar a enorme influência da legislação europeia ao tratar da visibilidade da legislação brasileira no contexto mundial.

Palavras-chave: Lei Geral de Proteção de Dados. Regulamento Geral de Proteção de Dados. Autoridade Nacional de Proteção de dados. Evolução. Natureza Jurídica.

1 Graduada em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas), pós-graduada em Lei Geral de Proteção de Dados pela Faculdade Legale. Membro da Associação Nacional dos Advogados de Direito Digital e integrante do Comitê de Startups e E-commerce. Atualmente, é consultora de proteção de dados na Camargo & Vieira Sociedade de Advogados. E-mail: clara.peretadv@outlook.com

ABSTRACT

This paper seeks to analyze Law nº 13.709/2018, called the General Data Protection Law, which came into force on September 18, 2020, in order to better understand the influence of the General Data Protection Regulation, a regulatory norm of the European Union, had on the Brazilian law. Initially, the evolution of Digital Law in Brazil will be addressed by means of an analysis of the preexisting legislative framework that dealt with the topic in order to contextualize the development of the subject in Brazil until the current days, in which the National Authority of Data Protection will be analyzed, its legal nature and activities that are already being performed. Several papers and all the educational material released by ANPD were taken into account to, at the end, prove and justify the enormous influence of the European legislation when dealing with the visibility of Brazilian legislation in the world context.

Keywords: General Data Protection Law. General Data Protection Regulation. National Data Protection Authority. Evolution. Legal Nature.

Recebido: 12-05-2021
Aprovado: 24-08-2021

1 EVOLUÇÃO HISTÓRICA DA LEI

No Brasil, a privacidade e a proteção de dados foram colocadas como direitos fundamentais diante de sua grande relevância, sendo previstos no art. 5º da Constituição Federal de 1988, em seu inciso X, em que é resguardada a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, e no inciso XII, que protege o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas.

No entendimento do professor Tércio Sampaio Ferraz Junior[2], a privacidade assegurada pela Constituição em relação ao sigilo de dados

2 FERRAZ, T. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, São Paulo, v. 88, p. 446-447, 1993.

se restringe à interpretação de que protege apenas os dados relativos à sua comunicação. Essa interpretação também ficou visível quando do julgamento do Recurso Extraordinário nº 418.416, em 10 de maio de 2006, em que o ministro Sepúlveda Pertence defendeu que "a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador".[3] Contudo, pode-se afirmar que esse entendimento não abarca a realidade atual decorrente do *Big Data*, definido comumente como a obtenção de informação por meio de um infinito conjunto de dados com o intuito de gerar ideias úteis, bens e serviços de valor significativo.

Em conformidade com a Constituição, ao definir sobre o tema, o Código Civil prevê, em seu art. 21, como um direito inviolável a vida privada da pessoa natural.[4] Também seguindo esse entendimento, o Código de Defesa do Consumidor define direitos básicos e invioláveis do consumidor, que podem ser feridos por algumas das práticas de negócios usadas para a captura de dados. No caput do art. 43[5], faz-se menção ao princípio da informação, determinando ser direito do titular ter informações sobre os dados coletados e armazenados, além de garantir a possibilidade da solicitação de exclusão.

O artigo também faz menção ao princípio da publicidade, em que o consumidor deve ser informado a respeito da coleta e do armazenamento dos dados, e do princípio da exatidão dos dados pessoais, concedendo ao titular o direito de alterar os dados incorretos.

A legislação não era específica para proteção de dados, sendo que eventuais disposições eram segmentadas em diferentes áreas da atividade econômica, tendo como exemplo a Lei do Cadastro Positivo (Lei nº

3 BRASIL. Superior Tribunal Federal. **Recurso Extraordinário nº 418.416, 10 de maio, 2006.** Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em: 17 set. 2020.

4 Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

5 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

12.414/2011) e a Lei de Acesso à Informação Pública (Lei nº 12.527/2011), de forma que foi criado um sistema fragmentado e pouco responsivo. Também houve episódios pontuais que atraíram a atenção pública e foram rapidamente transformados em lei, como o caso da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos. Tais fragilidade e insegurança jurídica às quais se submetiam empresas que tinham como um dos pilares de seus negócios o tratamento de dados foram bastante criticadas.

Em 23 de abril de 2014, foi promulgada a Lei nº 12.965, chamada de Marco Civil da Internet, que ratificou o que já havia sido vislumbrado pelas outras legislações: a garantia do princípio da privacidade na internet, protegendo tanto a segurança quanto a privacidade dos dados pessoais ao restringir o acesso ou o uso de informações privadas. No art. 7º[6] da referida lei, estão elencados os direitos do usuário, que definem a proteção da confidencialidade e a inviolabilidade da vida privada digital e os fluxos de tráfego da internet, disponibilização de registros de conexão e de acesso a aplicações à internet que resguardem a intimidade, a honra e a imagem de seus usuários.

Segundo o advogado e doutor em Ciência Política, Diego Rafael Canabarro, devido à sua importância legal, o Marco Civil da Internet foi uma das leis inspiradoras da Declaração de Direitos na Internet Italiana,

6 Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; [...]

publicada em 13 de outubro de 2014 (CANABARRO, 2014). A lei abriu caminho para a Lei Geral de Proteção de Dados Pessoais, uma vez que relacionou proteções, como direitos dos usuários de internet, à inviolabilidade da intimidade e da vida privada; à preservação do sigilo das comunicações privadas pela rede, transmitidas ou armazenadas; o não fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do usuário; além de ter estabelecido o dever de informar aos usuários acerca da coleta de dados sobre eles, quando houver justificativa para tal fato.

Em 2016, a União Europeia publicou o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*, ou GDPR) com o propósito de assegurar maior privacidade aos indivíduos, garantindo uma transparência maior no processo de coleta e de tratamento dos dados, e de acompanhar os avanços na regulação do mercado da comercialização de bens e serviços on-line. Em 25 de maio de 2018, a Lei de Proteção de Dados da União Europeia entrou em vigor e despertou a necessidade de outros países criarem leis específicas para a proteção de dados, além de fomentar o debate na implementação de leis a respeito do tema.

Em observância a esse novo contexto e diante da necessidade de tutela jurídica de defesa de dados pessoais, em 10 de julho de 2018 o Congresso Nacional aprovou o Projeto de Lei Complementar nº 53/2018, que deu origem à Lei Geral de Proteção de Dados. A Lei nº 13.709/2018 é a legislação brasileira que regula as atividades de tratamento de dados pessoais e foi sancionada em agosto de 2018 para entrar em vigor a partir de 16 de agosto de 2020. Acerca da harmonização do desenvolvimento da tecnologia e da preservação dos direitos de personalidade dos titulares de dados, atesta a professora adjunta de Direito Civil da Universidade de Brasília, Laura Schertel Mendes (2014, p. 58):

> A importância do modelo de lei geral reside no fato de que ela constrói uma arquitetura regulatória que busca consolidar o tema de proteção de dados pessoais como um setor de políticas

> públicas, composto por instrumentos estatutários, sancionatórios, assim como por um órgão administrativo, responsável pela implementação e aplicação da legislação.

Utilizando diferentes justificativas, como o curto período de tempo para que as empresas se adaptassem e se adequassem à lei; a morosidade na instalação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação; e a crise diante do novo coronavírus (COVID-19), surgiram diversos instrumentos estratégicos que tinham como objetivo prorrogar a vigência da LGPD. Entre eles, deve-se destacar o Projeto de Lei nº 1.179/2020 e a Medida Provisória nº 959/2020.

Em 30 de março de 2020, o Projeto de Lei nº 1.179/2020 surgiu com o objetivo de prorrogação da LGPD, com vigência em 1º de janeiro de 2021 e sanções aplicáveis a partir de 1° de agosto de 2021. No dia 3 de abril de 2020, esse Projeto de Lei foi aprovado no Senado Federal e encaminhado à Câmara dos Deputados para revisão.

No dia 24 de abril de 2020, a Medida Provisória nº 959/2020 surgiu com o objetivo de modificar a redação relativa à vigência da LGPD de "24 meses após a data de sua publicação" (dois anos depois) para "em 3 de maio de 2021", de forma que a prorrogação tanto da vigência quanto da aplicação de sanções seria a partir de 3 de maio de 2021. A Medida Provisória foi encaminhada à Câmara dos Deputados para análise.

No dia 14 de maio de 2020, o Projeto de Lei nº 1.179/2020 foi aprovado na Câmara dos Deputados, quanto aos dispositivos relativos às sanções, para que entrassem em vigor em agosto de 2021. Quanto à vigência dos demais dispositivos do Projeto de Lei, incluindo os que dispõem sobre o dia da vigência da LGPD, os deputados resguardaram-se de debates para que eles fossem pauta na apreciação da Medida Provisória nº 959/2020. Após isso, o projeto de lei foi reencaminhado ao Senado.

Em 19 de maio de 2020, o Senado Federal rejeitou o substitutivo da Câmara dos Deputados no Projeto de Lei nº 1.179/2020 e retomou o texto original da LGPD, a fim de que a vigência da lei ocorresse em agosto de 2020 e sanções aplicáveis para agosto de 2021. Eles justificaram a decisão dizendo que, neste momento de epidemia, é preciso que se colete e se faça o uso de dados pessoais com base em parâmetros legais, garantindo a segurança e a privacidade dos processos. O Projeto de Lei nº 1.179/2020 foi, então, encaminhado para sanção presidencial.

No dia 10 de junho de 2020, foi sancionada a Lei nº 14.010/2020 que, entre outras questões, altera a LGPD, determinando que as suas sanções só poderiam ser aplicadas a partir de 1º de agosto de 2021. No final do mesmo mês, o presidente do Congresso Nacional prorrogou por mais 60 dias a apreciação da MP nº 959/20.

Em agosto de 2020, a Câmara dos Deputados votou a Medida Provisória nº 959/20, alterando sua data de vigência para o dia 31 de dezembro de 2020, e o Senado reprovou o texto final. Em que pese que o dispositivo da MP que tratava da LGPD tivesse sido retirado do texto, era necessário um trâmite constitucional de 15 dias para que o dispositivo fosse aprovado ou rejeitado pelo presidente da República. Ainda em agosto, foi publicado o Decreto nº 14.474/2020, aprovando a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da Autoridade Nacional de Proteção de Dados (ANPD).

A Lei Geral de Proteção de Dados entrou em vigor em 18 de setembro de 2020, com exceção das sanções administrativas previstas na legislação, que começaram a ser aplicadas em agosto de 2021.

2 LEI GERAL DE PROTEÇÃO DE DADOS E O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados sofreu forte influência do Regulamento Geral de Proteção de Dados (RGPD), por ter valorizado a esfera

da proteção de dados pessoais, com sua aplicação extraterritorial, ao exigir conformidade de empresas situadas dentro e fora da União Europeia. Por mais que outros países tenham publicado, anteriormente, leis sobre a regulação da internet e da proteção de dados, nenhum país conseguiu ter uma regulamentação tão expressiva quanto o RGPD, de tal forma que a lei brasileira reproduziu grande parte de suas disposições. Assim, torna-se necessária a familiarização com os mecanismos do RGPD, pois, além da influência legislativa, também há reflexos na atuação das empresas no Brasil, de forma que aquelas que tenham negócios com empresas europeias devem implementar práticas de compliance que atendam ao RGPD. Sobre o tema, Renato Opice Blum, vice-presidente da Comissão Especial de Direito e Inovação da Ordem dos Advogados de São Paulo (OAB/SP), afirma que "o texto – enorme, detalhado e contundente, foi aprovado em 2016, cumpriu dois anos de vacância e destina-se a todos aqueles que possuem negócios ou ofertem serviços com coleta/tratamento de dados pessoais, mesmo que gratuitamente, ao público europeu"[7].

Podemos destacar como os principais pontos da lei europeia adotados pela lei brasileira: a abrangência da lei na tutela dos dados pessoais e sensíveis; a obrigatoriedade do consentimento dos titulares para o tratamento de seus dados pessoais; o direito ao esquecimento; a avaliação de impacto da proteção de dados quando o tratamento for suscetível a riscos dos direitos e liberdades individuais dos titulares; implementação de um programa de governança corporativa com responsabilidade das empresas e sanções quando do descumprimento da lei. Por mais que haja uma diferença geográfica, a aplicabilidade das leis se apresenta perfeitamente cabível. Nesse mesmo sentido, a mestre em Direito de Regulação e advogada da Petrobrás, Ludimilla Santos Derbili (2019, p. 188), aponta o seguinte:

7 BLUM, O.; SILVA, R. M. da. GDPR – General Data Protection Regulation: destaques da regra europeia e seus reflexos no Brasil. **Revista dos Tribunais** [recurso eletrônico], São Paulo, n. 994, ago. 2018. Disponível em: http://dspace.almg.gov.br/handle/11037/28636. Acesso em: 17 set. 2020.

> Acompanho o entendimento de Papadopoulos (2016, p. 894) no sentido de que é possível evoluir para se alcançar um ponto de equilíbrio ou um meio termo com os transplantes denominados heuristicamente de botânicos. As regras podem se deslocar, mas seu significado se adapta aos valores do país que a importa, desde que não sejam absolutamente discrepantes do seu significado no país de origem.
> De acordo com o que foi observado pela análise comparativa entre a legislação nacional e estrangeira, conclui-se que o regime de proteção de dados da União Europeia pode ter sido transferido para o cenário brasileiro, pois as regras do GDPR têm significado compatível e são plenamente adaptáveis ao modelo brasileiro. Dessa forma, entende-se que, uma vez consumado o transplante jurídico, na acepção botânica, não haverá impactos negativos na uniformidade e no processo de harmonização entre os sistemas jurídicos nacional e europeu.

Outro ponto que deve ser ressaltado em nível de comparação entre as legislações é o fato de que sempre houve uma tensão para elaborar normas em nível regional e transnacional convergentes que não restringissem o fluxo de informações. Tanto a LGPD quanto o RGPD ampliaram as formas pelas quais essa transferência internacional de dados pode ocorrer por criar ou reforçar válvulas de escape que têm como base compromissos privados de organizações que dependem desse livre trânsito de dados para suas operações. Ao analisar o desenvolvimento do tema de privacidade e proteção de dados em uma escala mundial, é possível concluir que houve um consenso em relação aos princípios básicos norteadores das atividades de tratamento de dados. Esses princípios impõem limitação ao tratamento e atribuem poderes ao titular, que é capaz de determinar o que é feito com seus dados.

Além das normas do RGPD serem coerentes com a realidade brasileira, a utilização do texto europeu como base para o brasileiro possibilita que o Brasil seja reconhecido, internacionalmente, como um país que preza pela segurança dos dados, por possuir uma regulação de proteção de dados robusta. O advogado Gustavo Tepedino, doutor em Direito Civil

pela Universidade de Camerino, na Itália, e Chiara Spadaccini de Teffé, doutoranda em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ), a respeito da LGPD, apontam (2019, p. 293):

> A Lei Geral de Proteção de Dados brasileira e o Regulamento Geral Europeu sobre a Proteção de Dados 2016/679 (General Data Protection Regulation – GDPR) representam no contexto atual instrumentos para a proteção e garantia da pessoa humana, uma vez que facilitam o controle dos dados tratados, impõem deveres e responsabilidades aos agentes de tratamento e proporcionam segurança para que as informações circulem. Os dois sistemas encontram-se fortemente alinhados, como desejou o legislador brasileiro, para que a norma nacional, nos próximos anos, seja reconhecida como adequada ao sistema europeu, uma vez que isso facilitará realizações de transações e cooperações com países do bloco.

É interessante destacar que, além da brasileira, o RGPD também influenciou a Lei de Privacidade do Consumidor da Califórnia[8], que obriga empresas, como as gigantes da tecnologia Amazon, Facebook, Google e Uber, a informar quais tipos de dados coletam de seus clientes, os motivos pelos quais o fazem e com quem compartilham as informações. A lei permite que os usuários neguem a venda de suas informações pessoais para empresas terceiras e dá aos californianos a capacidade de ter seus dados excluídos, além de tornar mais difícil o compartilhamento ou a venda de informações de crianças e adolescentes. A legislação também concede ao procurador-geral do Estado autoridade de fiscalização.

3 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A Autoridade Nacional de Proteção de Dados, também chamada de ANPD, tem por objetivo zelar pela implementação, pela fiscalização e

8 CALIFORNIA Consumer Privacy Act. **Lei de Privacidade do Consumidor da Califórnia**, de 24 de setembro de 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB112. Acesso em: 4 out. 2020.

pelo monitoramento do cumprimento da Lei Geral de Proteção de Dados. Esse órgão nacional editará normas e publicará orientações e instruções normativas, uma vez que ainda existem algumas lacunas e informações incompletas na estrutura da lei. Ainda não está definido como funcionará a fiscalização pela ANPD; contudo, há fortes influências e inspirações de outras legislações já vigentes ao redor do mundo, principalmente do Regulamento Europeu, como apresentado anteriormente.

As atribuições da ANPD estão elencadas no art. 55-J, em seus 16 incisos.[9] Entre as suas funções estão: zelar pela proteção dos dados pessoais, assim como estimular a adoção de padrões técnicos, prevendo regulamentações específicas, diante de eventuais lacunas de aplicabilidade, como códigos de conduta setoriais e de certificações que possam garantir a observância das regras da norma, chamados de Códigos de Conduta e Certificação. Caberá à ANPD incentivar a realização de relatórios de impacto, que são uma descrição de uma operação de tratamento de dados pessoais, executados pela empresa juntamente com as medidas que tenha adotado para aumentar a segurança e mitigar o risco presente no tratamento.

Também será realizada, pela ANPD, a fiscalização e a aplicação de sanções em caso de tratamento de dados realizado em descumprimento à legislação. Entre as sanções, podem ser aplicadas advertências e sanções administrativas, como proibição total ou parcial de tratamento de dados e multas, variando entre 2% do faturamento da empresa a cinquenta milhões de reais por infração, tendo, ainda, a possibilidade de multa diária para compelir a entidade a cessar as violações.[10]

No primeiro ano do RGPD, segundo estudo da *International Association of Privacy Professionals (IAPP)*, foram apresentadas mais de

9 Art. 55-J da Lei Geral de Proteção de Dados (LGPD) de 2018.

10 Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II;

281 mil notificações em 27 países.[11] Em relação ao papel fiscalizador da ANPD, diante da experiência europeia, é essencial que o órgão brasileiro de proteção de dados estabeleça um canal direto de comunicação com os titulares, de modo que facilite a apresentação de reclamações ou de preocupações em relação ao tratamento destinado a dados pessoais nos casos em que as reclamações encaminhadas ao(s) controlador(es) não tenham sido efetivamente solucionadas. Assim, a ANPD deve, também, promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança.

A ANPD deve assegurar o efetivo cumprimento da lei, atuando por iniciativa própria, promovendo ações de cooperação com autoridades de proteção de dados pessoais de outros países; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; e solicitar às entidades do Poder Público, que realizem operações de tratamento de dados pessoais, que informem especificamente o âmbito, a natureza e os demais detalhes dos tratamentos realizados nos dados; e realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.

A experiência trazida pela legislação europeia sobre a proteção de dados mostra a importância relacionada à existência de uma Autoridade Nacional específica para fiscalizar a aplicação da LGPD, de modo a garantir segurança jurídica, respeito ao direito à privacidade e proteção de dados dos titulares, fomentando o desenvolvimento socioeconômico do país, inserindo o Brasil no rol de países que conferem segurança jurídica relacionada à proteção de dados pessoais e à segurança da informação. Por fim, a ANPD deve atuar como facilitadora entre empresas, cidadãos e governo, promovendo medidas que difundam a cultura de proteção de dados

11 TCE-SC. **Seminário no TCE/SC mostra como é a GDPR, lei de proteção de dados europeia que serviu de base para o modelo brasileiro**. 5 nov. 2019. Disponível em: http://www.tce.sc.gov.br/intranet-acom-icon/noticia/51360/semin%C3%A1rio-no-tcesc-mostra-como-%C3%A9-gdpr-lei-de-prote%C3%A7%C3%A3o-de-dados. Acesso em: 4 out. 2020.

no Brasil, tornando as previsões da LGPD mais claras, acessíveis e palatáveis, tanto para os titulares de dados quanto para os agentes de tratamento.

Durante a ausência de diretrizes específicas da ANPD, imperam os parâmetros gerais de boas práticas e governança determinados pela LGPD, que devem ser ajustados de acordo com as especificidades de cada setor econômico. Entre essas diretivas, podem-se destacar algumas orientações que também estão presentes no RGPD, como a necessidade de demonstrar o comprometimento em adotar processos e políticas internas que assegurem o cumprimento de normas relativas à proteção de dados pessoais, estabelecer uma relação de confiança com o titular dos dados por meio de atuação transparente, estar integrado à sua estrutura geral de governança, estabelecer mecanismos de supervisão internos e externos, possuir planos de resposta a incidentes e remediação, atualizar-se constantemente e realizar um efetivo e contínuo monitoramento, além de avaliações periódicas.

Esses procedimentos adotados pelas empresas poderão ser reconhecidos, atualizados e publicados pela ANPD por meio da autorregulação regulada, prevista no art. 50, §3º da LGPD[12]. Assim, são conciliados os interesses do Estado e da sociedade, unindo o conhecimento da prática setorial e a necessidade de constante revisão de conceitos inerente à dinamicidade da sociedade atual.

É interessante ressaltar que, dos 120 países que têm Lei de Proteção de Dados, apenas 12 não criaram uma autoridade independente, como Angola e Nicarágua. Entre os países da América Latina, Argentina, Panamá e Colômbia são exemplos de países que já possuem uma Autoridade de dados pessoais. Outros, como Chile, Paraguai e Rússia, estão se organizando para, em breve, também instituir as respectivas Autoridades.

12 Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...] § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

3.1 NATUREZA JURÍDICA DA ANPD

A expectativa da Autoridade Nacional de Proteção de Dados, tal qual prevista no projeto de lei, era de que fosse uma autarquia federal, vinculada ao Ministério de Justiça, que gozaria de independência administrativa, ausência de subordinação hierárquica, autonomia financeira e mandato fixo e estabilidade de seus dirigentes. Contudo, de acordo com o texto da lei aprovado a criação foi de uma autoridade de proteção de dados integrante do Poder Executivo. Segundo as razões de veto da medida provisória que previa a outra natureza da ANPD, o Poder Legislativo não poderia criar órgãos que resultassem em novos gastos ao orçamento, ou seja, o Legislativo não poderia criar órgãos que gerassem despesas para o Executivo, de forma que essa seria uma prerrogativa do próprio Poder Executivo.

O art. 55-A determina que "fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República".[13] Assim, a ANPD não é uma autoridade totalmente independente em suas decisões e também depende do orçamento previsto pelo Poder Executivo. Com essa nova natureza jurídica, muitos especialistas da área criticaram a criação da ANPD nesse modelo, justamente por dificultar as decisões da autoridade, retirando sua tecnicidade diante da dependência da opinião do Poder Executivo e talvez dificultando a aplicação de sanções para o setor público. Isso também pode vir a ser uma barreira para o Brasil ser considerado um país com nível de proteção adequado aos dados pessoais pela comunidade europeia, tendo em vista que o RGPD prevê a necessidade de autonomia técnica e financeira para a validação da autoridade. Todavia, o §1º desse mesmo artigo define que essa natureza jurídica poderá mudar, prevendo sua transitoriedade. Veja-se a norma (BRASIL, 2019):

13 Art. 55-A da Lei Geral de Proteção de Dados (LGPD) de 2018.

> Art. 55-A. §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. (Incluído pela Lei nº 13.853, de 2019)

Caso seja transformada em entidade submetida ao regimento autárquico especial, a ANPD passará a integrar as agências reguladoras, como ANATEL, ANS, ANAC entre outras. Porém, não é apresentada uma condicionante para que essa transformação efetivamente aconteça.

Nesse período inicial de estruturação, a ANPD já apresentou sua composição e disponibilizou guias orientativos sobre temas que geravam distintas interpretações, como acerca da atuação dos agentes de tratamento existentes na lei. A Autoridade Nacional de Proteção de Dados também divulgou que exercerá, a princípio, majoritariamente seu papel educativo, a fim de instruir a população sobre a lei para, posteriormente, cumprir o seu papel fiscalizador. Contudo, diante de um cenário em que incidentes de segurança estão cada vez mais frequentes, é esperado que as penalidades comecem a ser aplicadas antes do que o esperado.

A ANPD deve cumprir suas funções, não obstante a possibilidade de alteração de sua natureza jurídica. Para tanto, deve assegurar o efetivo cumprimento da lei, atuando por iniciativa própria, promovendo ações de cooperação com autoridades de proteção de dados pessoais de outros países, dispondo sobre as formas de publicidade das operações de tratamento de dados pessoais e solicitando às entidades do Poder Público que realizem operações de tratamento de dados pessoais que informem especificamente o âmbito, a natureza e os demais detalhes dos tratamentos realizados nos dados. Ademais, deve realizar ou determinar a realização de auditorias no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.

4 CONSIDERAÇÕES FINAIS

O compartilhamento de dados surge como uma preocupação no cenário jurídico em razão dos desdobramentos da conectividade e da grande troca de informações e de armazenamento de dados por empresas, intensificados na medida em que mais equipamentos têm a possibilidade de interação virtual, o que impacta os direitos constitucionais de privacidade e dados pessoais, como preferências, localizações, rotinas e informações confidenciais. Nesse contexto, o Direito brasileiro tenta acompanhar as mudanças sociais e tem dado passos para a evolução do Direito Digital e suas aplicações. Por ainda ser um tema novo na seara jurídica, muito deve se aprofundar no assunto e ainda surgirão doutrinas e jurisprudências que solidificarão entendimentos práticos sobre a questão.

A LGPD sofreu uma grande influência do Regimento Geral de Proteção de Dados da União Europeia de uma forma altamente benéfica, tendo em vista que, diante de uma matéria pouco regulada tanto no Brasil quanto em outros países, este último serviu de referência para a elaboração da lei brasileira. Ao espelhar e incluir princípios e definições estabelecidos pelo RGPD, o Brasil conseguiu aproximar sua legislação da europeia e aumentar a chance de ser reconhecido como um país adequado no ponto de vista de privacidade e proteção de dados.

A Autoridade Nacional de Proteção de Dados é fundamental para garantir a efetividade dos direitos dos cidadãos, mas também deve ser considerada como um facilitador da adequação das empresas à lei ao determinar padrões de aplicação. Em relação à natureza jurídica da ANPD, sua autonomia se mostra cada vez mais necessária, uma vez que se apresenta como um requisito para que o país obtenha a validação de adequação europeia, o que permitiria o livre fluxo de dados entre Brasil e Europa, um mercado de 500 milhões de consumidores para empresas brasileiras, um grande benefício econômico e político, conforme também defende Bruno Bioni (2020). Entretanto, espera-se que, independentemente de sua

natureza jurídica, a ANPD seja considerada um órgão que preza pela segurança de dados e com autonomia suficiente para realizar suas funções nacionais e internacionais, visto que o Brasil apresenta uma lei robusta no sentido de proteção de dados e vêm dando relevância ao tema ao longo dos últimos anos. Apesar de já ter sido iniciado o processo de implementação da nova lei no Brasil, ainda há definições a serem feitas pela ANPD, que também devem ser favorecidas pelas experiências e inovações legislativas de países que estão avançando nesse campo.

A incorporação da legislação europeia pela LGPD foi essencial para a criação de uma cultura de proteção de dados, o que deve ser considerado um enorme avanço no ramo do Direito Digital. A mudança de mentalidade da população brasileira deve ser impulsionada também pelas penalidades a serem impostas àqueles que infringirem a lei, mas, acima de tudo, pela autodeterminação informativa que será desenvolvida; aspecto que norteia inúmeros princípios da lei brasileira e europeia.

Diante do contexto atual de intensas mudanças, mas muita insegurança sobre quais serão os padrões aceitáveis pela ANPD, espera-se que sejam suficientes as medidas estabelecidas para a proteção dos usuários e seus dados pela Lei Geral de Proteção de Dados, bem como seja realizada a aplicação das responsabilizações por infrações cometidas por empresas ou órgãos públicos, a fim de que seja resguardado o direito constitucional da privacidade. Espera-se, também, que, diante da importância que o Brasil deu ao tema e da forte influência europeia na lei brasileira, reste comprovado pelo sistema europeu de proteção de dados que o Brasil é um país adequado e que as entidades públicas e privadas possam tratar e transferir dados entre esses países.

REFERÊNCIAS

BIONI, B. R.; MENDES, L. S. O Regulamento Europeu de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, G. *et al*. (org.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

BLUM, O.; SILVA, R. M. da. GDPR – General Data Protection Regulation: destaques da regra europeia e seus reflexos no Brasil. **Revista dos Tribunais** [recurso eletrônico], São Paulo, n. 994, ago. 2018. Disponível em: http://dspace.almg.gov.br/handle/11037/28636. Acesso em: 17 set. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. *In*: Vade Mecum Saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 set. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. *In*: Vade Mecum Saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 17 set. 2020.

BRASIL. Superior Tribunal Federal. **Recurso Extraordinário nº 418.416, 10 de maio, 2006**. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em: 17 set. 2020.

CALIFORNIA Consumer Privacy Act. **Lei de Privacidade do Consumidor da Califórnia**, de 24 de setembro de 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB112. Acesso em: 4 out. 2020.

CANABARRO, D. R. **A contribuição do Brasil para o Marco Civil da Internet na Itália**. Disponível em: http://observatoriodainternet.br/post/a-contribuicao-do-brasil-para-o-marcocivil-da-internet-na-italia. Acesso em: 18 set. 2020.

DERBILI, L. S. O transplante jurídico do regulamento geral de proteção de dados da união europeia ("GDPR") para o direito brasileiro. **E-legis**, Rio de Janeiro, n. 30, p. 181-193, set./dez. 2019. ISSN 2175.0688.

FERRAZ, T. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, São Paulo, v. 88, p. 446-447, 1993.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental LGPD**. São Paulo: Saraiva, 2014.

PRIVAZYPLAN. **UE Regulamento Geral sobre a Proteção de Dados**: conteúdo. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a

Proteção de Dados). Alemanha, 5 set. 2018. Disponível em: https://www.privacy-regulation.eu/pt/. Acesso em: 19 set. 2020.

TCE-SC. **Seminário no TCE/SC mostra como é a GDPR, lei de proteção de dados europeia que serviu de base para o modelo brasileiro**. 5 nov. 2019. Disponível em: http://www.tce.sc.gov.br/intranet-acom-icon/noticia/51360/semin%C3%A1rio-no-tcesc-mostra-como-%C3%A9-gdpr-lei-de-prote%C3%A7%C3%A3o-de-dados. Acesso em: 4 out. 2020.

TEPEDINO, G.; TEFFÉ, C. S. de. Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.