

DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE COMPARADA DA GDPR DO PARLAMENTO EUROPEU E DO CONSELHO DA UNIÃO EUROPEIA E A LGPD BRASILEIRA¹

Leonardo Castro de Bone*

Maria Vitória Galvan Momo**

Resumo: Apesar de antiga, a discussão sobre a adequada tutela jurídica dos dados pessoais ganhou notoriedade com os recentes episódios de utilização indevida de dados pessoais, como nos casos do website “tudosobretodos.se”, do ex-técnico da CIA, Edward Snowden e do escândalo envolvendo a empresa *Cambridge Analytica*. Nessa toada, com a entrada vigor da *General Data Protection Regulation* (GDPR) do Parlamento Europeu e do Conselho da União Europeia e da aguardada Lei Geral de Proteção de Dados (LGPD), que somente entrará em vigor em agosto de 2020, inadiável voltamos nossa atenção aos importantes avanços legislativos alcançados nos últimos anos quanto à matéria da proteção dos dados pessoais.

Palavras-Chave: Tratamento dos dados pessoais. Lei Geral de Proteção de Dados Pessoais. LGPD. *General Data Protection Regulation*. GDPR.

¹ Trabalho desenvolvido antes da entrada em vigor da Lei Geral de Proteção de Dados Pessoais no Brasil, que somente acontecerá em agosto de 2020.

* Mestrando em Direito Civil pela Faculdade de Direito da Universidade de Lisboa. Especialista em Direito Tributário e Processo Tributário pela Faculdade de Direito de Vitória. Advogado.

** Doutoranda em Direito Civil pela Universidade de Lisboa. Mestra em Direito Empresarial pela Universidade de Coimbra. Advogada.

FROM PRIVACY TO PERSONAL DATA PROTECTION: A COMPARATIVE ANALYSIS OF THE GDPR OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION AND THE BRAZILIAN LGPD

Abstract: Although old, the discussion about the adequate legal protection of personal data gained notoriety with the recent episodes of misuse of personal data, as in the cases of the website “tudosobretodos.se”, of the former CIA technician, Edward Snowden and the scandal involving Cambridge Analytica. In this light, with the entry into force of the General Data Protection Regulation (GDPR) of the European Parliament and of the Council of the European Union and the awaited General Data Protection Law (LGPD), which will only come into force in August 2020, we cannot postpone our attention to the important legislative advances achieved in recent years in the area of the protection of personal data.

Keywords: Processing of personal data. General Law on Protection of Personal Data. LGPD. General Data Protection Regulation. GDPR.

Sumário: Introdução. 1. O Modelo Regulatório Europeu e a Proteção de Dados Pessoais. 1.1. Da Convenção Europeia de Direitos Humanos à GDPR. 1.2. *General Data Protection Regulation*. 2. Da Proteção de Dados Pessoais no Brasil; 2.1. A Proteção de Dados Pessoais Pré LGPD. 2.2. A Lei Geral de Proteção de Dados Pessoais. Considerações Finais.

INTRODUÇÃO



preocupação com a proteção de dados pessoais pode parecer algo novo, mas não é. Na verdade, conhecimento e informação sempre permearam as relações sociais, “visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processo da informação”², o que há muito já demandava do legislador um olhar mais atento sobre o *tratamento jurídico dos dados pessoais*³. Contudo, com a evolução tecnológica as relações sociais transformaram-se e passaram a integrar o sistema digital⁴ - num movimento de “virtualização”⁵ da sociedade – e, com isso, o valor agregado da informação maximizou-se, colocando a proteção de dados pessoais numa posição de destaque na sociedade globalizada.

Se, por um lado, as novas tecnologias permitiram que o indivíduo realize todas as suas funções por plataformas digitais, o que acaba por revolucionar toda a estrutura política, econômica e social⁶, por outro, exige do legislador um olhar ainda mais minucioso sobre os problemas advindos da nova era digital. O “ciberespaço”⁷, ao armazenar informações pessoais cedidas

² CASTELLS, Manuel. *A sociedade em rede*. Trad. de Roneide Venancio Majer. Vol. 1. 8.^a ed. revista e ampliada. São Paulo: Paz e Terra, 2005, pp. 53-54.

³ A esse propósito, MAYER-SCÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip e ROTENBERG, Marc (Org.). *Technology and privacy: The new landscape*. Cambridge: MIT Press, 1997, p. 219-242, identifica diferentes gerações de leis de proteção de dados, desde modelos regulatórios pós Segunda Guerra Mundial (como, por exemplo, a Lei do *Land*, de 1970 na Alemanha; a *DataLegen 289*, de 1973 na Suécia; e a *Privacy Act*, de 1974 nos Estados Unidos) até as legislações mais atuais (como, por exemplo, a Diretiva 2000/58/CE, a Diretiva 95/46/CE, etc.).

⁴ Propiciando a criação de laços fracos, conforme sinaliza CASTELLS, Manuel. *A Sociedade em Rede*. Trad. de Roneide Venancio Majer. Vol. 1. 8.^a ed. revista e ampliada. São Paulo: Paz e Terra, 2005, p. 445.

⁵ LÉVY, Pierre. *O Que é o Virtual?*. Trad. de Paulo Neves. Rio de Janeiro: Editora 34, 1997, p. 11, considera que atualmente existe um movimento de virtualização da sociedade, da economia, da informação, das comunicações etc.

⁶ COELHO, Helder. A agenda digital europeia. In: ASCENSÃO, José de Oliveira (coord.). *Direito da sociedade da informação e direito de autor*. v. 10. Coimbra: Coimbra Editora, 2012, p. 76.

⁷ Termo utilizado por LÉVY, Pierre. *Cibercultura*. Trad. de Carlos Irineu da Costa.

livremente por usuários (nome civil, moradia, contatos, gosto musical, posicionamento político, dados de consumo etc.), atrela às diversas vantagens⁸ do avanço tecnológico, desafios éticos, morais e legais⁹.

Casos de utilização indevida de dados pessoais, como nos episódios do website “tudosobretodos.se”¹⁰, do ex-técnico da CIA, Edward Snowden¹¹ e do recente escândalo envolvendo a empresa *Cambridge Analytica*¹², revolucionam a esfera jurídica e despertam a necessidade cada vez mais iminente de os países adotarem legislações mais atuais e condizentes com a profundidade tecnológica utilizada no tratamento de dados¹³, pois, afinal, “*The invasion of privacy is of course, only the beginning. The information gained about people; can of course, be used to manipulate and control them*”¹⁴.

Dessa forma, reconhecendo a importância que a proteção de dados pessoais assume na sociedade atual, imperioso o

São Paulo: Editora 34, 1999, p. 17.

⁸ Principalmente no funcionamento da economia, posto que “ao aumentar a transparência do mercado, ao facilitar as transações diretas entre fornecedores e consumidores, o ciberespaço certamente acompanha e favorece a evolução liberal na econômica da informação e do conhecimento”, cfr. LÉVY, Pierre. *Cibercultura*. Trad. de Carlos Irineu da Costa. São Paulo: Editora 34, 1999, p. 232.

⁹ A esse respeito, LEAL, Fernando. Ethics is fragile, Goodness is not. *AI Society*. v. 9, n. 1, p. 29-42, march 1995, 1995, p. 32, elenca a perda da privacidade como um dos principais problemas da nova sociedade de informação.

¹⁰ O referido site divulgou e colocou a venda, sem a autorização dos usuários, informações pessoais (nome, endereço etc.).

¹¹ Um dos grandes escândalos da atualidade envolvem ex-técnico da CIA, Edward Snowden, que vazou documentos da NSA que comprovam que o governo americano desenvolveu programas de vigilância global de espionagem, o que, inclusive, incluiria o governo brasileiro.

¹² O escândalo envolvendo a empresa *Cambridge Analytica* tornou pública a informação de que a empresa coletava informações de usuários do *Facebook* com o objetivo de manipular campanhas políticas.

¹³ O que já era suscitado desde 1980, por CATALA, Pierre. Ebauche d’une théorie juridique de l’information. *Informatica e Diritto*, a. 9, janv./avril, p. 15-31, 1983, pp. 15-16.

¹⁴ LEAL, Fernando. Ethics is fragile, Goodness is not. *AI Society*. v. 9, n. 1, p. 29-42, march 1995, 1995, p. 32.

operador do direito, especialmente aquele afeto ao tema, compreender que os importantes avanços alcançados com a Lei Geral de Proteção de Dados Pessoais (LGPD) consistem em influência direta do regulamento europeu sobre proteção de dados (GDPR), o que, a partir de agora, propomo-nos a analisar conjuntamente.

1. O MODELO REGULATÓRIO EUROPEU E A PROTEÇÃO DE DADOS PESSOAIS

1.1. DA CONVENÇÃO EUROPEIA DE DIREITOS HUMANOS À GDPR

Em 25 de maio de 2018 entrou em vigor o Regulamento 2016/679 da União Europeia, também conhecido como *General Data Protection Regulation* ou apenas GDPR. O Regulamento europeu, apesar de inserir profundas – e necessárias – reformas nas regras de proteção de dados pessoais, não foi o primeiro instrumento normativo a se preocupar com o tema.

Criado do rescaldo da Segunda Guerra Mundial, a *Convenção Europeia dos Direitos do Homem* de 1950, já garantia aos cidadãos europeus o direito à privacidade (art. 8.º), o que, na jurisprudência do TEDH, abarcaria situações de proteção de dados pessoais, como questões relacionadas a interceptações de comunicações¹⁵, formas de vigilância¹⁶ e o armazenamento de dados pessoais por autoridades públicas¹⁷.

Contudo, editada num período em que não havia ameaças aos direitos humanos por novas tecnologias, o art. 8.º da CEDH não conferia uma tutela jurídica adequada à proteção de

¹⁵ Ac. do TEDH, no caso *Malone v. United Kingdom*, de 2 de agosto de 1984, proc. n.º 8691/79.

¹⁶ Ac. do TEDH, no caso *Klass and Others v. Germany*, de 6 de setembro de 1978, proc. n.º 5029/71.

¹⁷ Ac. do TEDH, no caso *Leander v. Sweden*, de 26 de março de 1987, proc. n.º 9248/81.

dados pessoais, o que conduziu a Assembleia Parlamentar do Conselho da Europa, influenciada pelas *guidelines* de 1980 da OCDE¹⁸, a adotar, em 1981, a *Convenção 108*, também conhecida como *Convenção de Strasbourg*, para proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, regulando, inclusive, o fluxo transfronteiriço desses dados¹⁹ e o tratamento dos dados tidos como “sensíveis”²⁰.

Todavia, apesar de a *Convenção 108* do Conselho da Europa adotar importantes medidas, conhecidas como *Fair Information Principles*, que formam hoje a espinha dorsal de diversas legislações sobre proteção de dados pessoais²¹, e de estabelecer que a proteção de dados pessoais se liga diretamente à proteção e o desenvolvimento dos direitos do homem e das liberdades fundamentais (preâmbulo), o rápido e constante desenvolvimento tecnológico e a necessidade de uma regulamentação

¹⁸ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 174.

¹⁹ Handbook on European data protection law (2014 edition), p. 16. Disponível em: <<https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>>. Acesso em: 04 nov. 2019.

²⁰ Nos termos do art. 6.º da *Convenção 108*, os “dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objecto de tratamento automatizado desde que o direito interno preveja garantias adequadas. O mesmo vale para os dados de carácter pessoal relativos a condenações penais”.

²¹ DONEDA, Danilo. A Proteção dos Dados Pessoais Como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, Vol. 12, n.º 2, p. 91-108, jul./dez. 2011, pp. 100-101 elabora uma síntese desses princípios: “princípio da publicidade ou transparência, pelo qual todos os bancos de dados que contenham dados pessoais devem ser de conhecimento público; princípio da exatidão, pelo qual os dados armazenados em bancos de dados devem ser fiéis à realidade, demandando um cuidado e correção na coleta e no tratamento dos dados e, até mesmo, necessárias e periódicas atualizações; princípio da finalidade, pelo qual a utilização de dados pessoais deve obedecer à finalidade informada antes de sua coleta, coibindo a utilização dos dados para fins diversos ou ainda sua transferência para terceiros; princípio do livre acesso, pelo qual os bancos de dados devem garantir o acesso aos indivíduos sobre suas informações armazenadas, podendo, para tanto, obter cópias e controle desses dados, bem como a possibilidade de alterá-los, corrigi-los ou excluí-los; e o princípio da segurança física e lógica, os dados devem ser protegidos contra extravios, destruição, modificação, transmissão ou acesso sem autorização.

uniformemente elevada conduziram a Comunidade Europeia a aprovar em 1995 a *Diretiva 95/46/CE*²², objetivando “a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais” (art. 1.º, n.º 1), a “a livre circulação de dados pessoais entre Estados-membros” (art. 1.º, n.º 2) e a harmonização das legislações sobre proteção de dados pessoais a nível nacional²³.

A Diretiva Europeia de Proteção de Dados Pessoais de 1995, apesar de representar crucial instrumento normativo, estabelecendo uma normatização extensiva e complexa no tratamento da proteção de dados pessoais, incorporando os princípios já consagrados na Convenção 108²⁴ e, influenciando, inclusive, na aprovação do art. 8.º da Carta dos Direitos Fundamentais da União Europeia – que conferiu à proteção de dados pessoais a qualidade de direito fundamental²⁵ -, trata-se de regulamentação anterior e revogada pela GDPR, que entrou em vigor em 25 de

²² Handbook on European data protection law (2014 edition), p. 18. Disponível em: <<https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>>. Acesso em: 04 nov. 2019.

²³ A esse propósito, o TJUE, no caso *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEDM) v. Administración del Estad*, de 24 de novembro de 2011, nos processos apensos C-468/10 e C-469/10, entendeu que “a Diretiva 95/46 visa [...] tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais [...] A aproximação das legislações nacionais aplicáveis na matéria não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União Assim, [...] a harmonização das referidas legislações nacionais não se limita a uma harmonização mínima, mas conduz a uma harmonização que é, em princípio, completa”

²⁴ Handbook on European data protection law (2014 edition), p. 19. Disponível em: <<https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>>. Acesso em: 04 nov. 2019.

²⁵ Importante observar que com a assinatura do Tratado de Lisboa em 2009, a CDFUE tornou-se juridicamente vinculativa, como direito primário da União Europeia (art. 6.º, n.º 1, do TUE). Sobre o tema, cfr. Handbook on European data protection law (2014 edition), pp. 20-21. Disponível em: <<https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>>. Acesso em: 04 nov. 2019.

maio de 2018, a qual merece nossa especial atenção.

1.2. GENERAL DATA PROTECTION REGULATION

A preocupação com o tratamento de dados de caráter pessoal conduziu a União Europeia a adotar uma *regulamentação abrangente*²⁶, o que resultou num modelo regulatório extensivo e complexo, aplicável tanto para o setor privado, quanto para o setor público.

A atualização proposta pela GDPR - ou, em português, Regulamento Geral de Proteção de Dados -, intensifica a proteção dada pela Diretiva 95/46/CE, e representa um modelo mais atual e condizente com a profundidade tecnológica utilizada no tratamento de dados, sem, para tanto, abandonar as construções normativas realizadas até aqui.

A *General Data Protection Regulation* começa por estabelecer algumas definições básicas e essenciais, como *conceito de dados pessoais*, que, nos termos da norma europeia, compreendem toda informação relativa a uma pessoa singular, que pode ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (art. 4.º, n.º 1). É explícito, portanto, que para considerar uma informação como pessoal, deverá ser possível vincular essa informação a uma pessoa determinada, revelando aspectos objetivos de sua vida²⁷, constituindo *expressão direta da própria personalidade do indivíduo*²⁸.

²⁶ MOSHELL, Ryan. And There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection. *Texas Tech Law Review*, Vol. 37, 2005, p. 357-432, pp. 366-367.

²⁷ DONEDA, Danilo. A Proteção dos Dados Pessoais Como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, Vol. 12, n.º 2, p. 91-108, jul./dez. 2011, p. 94.

²⁸ CATALA, Pierre. Ebauche d'une théorie juridique de l'information. *Informatica e*

No *processamento ou o tratamento desses dados pessoais* – que pode ser compreendido como toda operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (art. 4.º, n.º 2) -, o *consentimento prestado pelo titular* dos dados deve ser uma manifestação de vontade, livre, específica, informada e explícita, pela qual aceita, mediante declaração ou ato positivo inequívoco, que seus dados pessoais sejam objeto de tratamento (art. 4.º, n.º 11), podendo ainda o usuário *revogar o consentimento* prestado a qualquer momento (art. 7.º, n.º 3), reforçando a ideia de que “o consentimento avoca para si o papel de protagonista, sendo, inclusive, um dos fios condutores da recente reforma (regulação) da diretiva europeia de proteção de dados pessoais”²⁹, devendo ele corresponder aos anseios e expectativas do próprio titular dos dados pessoais.

Ainda no que concerne ao tratamento dos dados pessoais, a GDPR estabelece *princípios relativos à qualidade dos dados*, definindo que os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (art. 5.º, n.º 1, a); recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (art. 5.º, n.º 1, b); adequados pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (art. 5.º, n.º 1, c); exatos e atualizados sempre que necessário, devendo os dados inexatos serem apagados ou retificados sem demora (art. 5.º, n.º

Drito, ano 9, janv./avril, 1983, p. 15-31, p. 20, explica que “*quand l’objet des donnés est un sujet de droit, l’information est un attribut de la personnalité*”.

²⁹ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 180.

1, d); conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (art. 5.º, n.º 1, e); tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizativas adequadas (art. 5.º, n.º 1, f); sendo ainda o responsável pelo tratamento dos dados o responsável pelo cumprimento dessas exigências (art. 5.º, n.º 2).

Dessa forma, nos termos do regulamento, *o tratamento de dados apenas será lícito* se e na medida em que se verifique pelo menos uma das seguintes situações (art. 6.º, n.º 1): a) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

De igual rigor, a norma europeia ainda impõe *ressalvas quanto ao tratamento de determinados dados pessoais*, como no caso dos dados de crianças menores de 16 anos de idade, onde o seu tratamento somente será lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais (art. 8.º, n.º 1). Não obstante a isso,

considera-se ainda *proibido o tratamento de dados pessoais* que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (art. 9.º, n.º 1), o que, contudo, nos termos do regulamento europeu comportaria exceções, como no caso de o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais (art. 9.º, n.º 2, a)³⁰.

Com vistas à efetivação da proteção de dados pessoais do usuário, o Regulamento Geral de Proteção de Dados do Parlamento Europeu e do Conselho da Europa ainda estabelece *direitos que o titular dos dados possui*, como o maior poder e controle do usuário sobre seus dados pessoais, com o fornecimento de informações mais claras, concisas, transparentes, inteligíveis e de fácil acesso pela empresa responsável (art. 12.º ao 14.º), sendo resguardado ainda o direito de acesso (art. 15.º), de retificação (art. 16.º), de apagamento (art. 17.º), de limitação do tratamento (art. 18.º) e de portabilidade dos dados pessoais (art. 20.º).

Já no que diz respeito à *segurança dos dados pessoais*, além da GDPR exigir que os dados pessoais sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, deverá o responsável pelo tratamento dos dados e o subcontratante aplicarem as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco (arts. 5.º, n.º 1, f e 32.º, n.º 1). Em caso de *violação dos dados pessoais*, deverá o responsável pelo tratamento notificar o fato a autoridade de controle

³⁰ O art. 9.º, n.º 2 da GDPR ainda estabelece outras exceções que permitiriam o tratamento desses dados pessoais.

competente³¹, no prazo de setenta e duas horas (art. 33.º) e, caso a violação seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deverá comunicar a violação dos dados pessoais também ao titular dos dados (art. 34.º)³².

Com o objetivo de efetivar as medidas implementadas, o regulamento europeu garante o *acesso à via judiciária* para defesa do indivíduo e seus dados, estabelecendo que o titular dos dados possui o direito a apresentar reclamação a uma autoridade de controle, se considerar que o tratamento dos dados pessoais que lhe diga respeito viola as normas contidas na GDPR (art. 77.º); o *direito à ação judicial contra uma autoridade de controle* caso ela não trate a reclamação ou não informe ao titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado (art. 78.º); o *direito à ação judicial contra o responsável pelo tratamento ou o subcontratante*, se o titular dos dados considerar ter havido violação dos direitos que lhe assiste o regulamento (art. 79.º); e o *direito a indenização pelos danos sofridos* (art. 82.º), aplicando-se ainda elevadas *sanções pecuniárias* as empresas que violarem as normas contidas no Regulamento Geral de Proteção de Dados (art. 83.º).

Por fim, ponto relevante reside na transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após *transferência para um país terceiro ou uma organização internacional*, pois, de acordo com o regulamento europeu, essa

³¹ Estabeleceu os art. 51.º e ss. da GDPR a possibilidade de criação de autoridades independentes de controle pelos estados-membros, para assegurar o melhor cumprimento das regras de proteção de dados estabelecidas no regulamento

³² Pela redação do art. 34.º da GDPR, consta que o responsável pelo tratamento dos dados deverá comunicar o titular dos dados sem demora injustificada, sem para tanto estabelecer um prazo certo e determinado. Contudo, socorrendo-nos de disposição similar no art. 33.º, estabelece o legislador que o responsável deverá notificar a autoridade de controle competente, sem demora injustificada, até 72 horas após ter tido o conhecimento do fato, o que nos leva a sustentar a aplicação do mesmo prazo para o caso do art. 34.º.

transferência apenas é realizada se, as condições estabelecidas no capítulo V da GDPR forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional (art. 44.º). Em outras palavras, a transferência internacional de dados pessoais para países terceiros ou organizações internacionais, somente será permitida se o receptor respeitar as condições estabelecidas nos arts. 44.º ao 55.º do regulamento, o que, em outros termos, garante um nível adequado de proteção dos dados pessoais para além da UE e do EEE³³.

Nesse ponto, interessante notar que antes mesmo da entrada em vigor da *General Data Protection Regulation*, a Diretiva 95/46/CE possuía norma similar (art. 25.º, n.º 1), ao estabelecer que a transferência de dados para países terceiros fora da União Europeia e da zona do Espaço Econômico Europeu, apenas poderia ocorrer se o país receptor dispusesse de normas adequadas de proteção de dados³⁴, o que resultou em severas repercussões no cenário internacional, levando países como a Letônia e a Noruega a adotarem medidas de proteção similares a europeia³⁵ ou ainda a acordos de transferência de dados pessoais,

³³ Com âmbito de aplicação territorial, a GDPR não se limita aos estados-membros da União Europeia, abrangendo países membros do chamado Espaço Econômico Europeu.

³⁴ Nos termos do art. 25.º da Diretiva 95/46/CE, a “adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país”.

³⁵ TAVARES, Letícia Antunes e ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. In: ONODERA, Marcus Vinicius Kiyoshi e FILIPPO, Thiago Baldani Gomes De (Coord.). *Brasil e EUA: Temas de Direito Comparado*. São Paulo: Escola Paulista da Magistratura, 2017, p. 155-204, p. 173.

como no caso dos EUA³⁶.

Assim, percebe-se que a preocupação com a proteção de dados pessoais no Direito Comunitário Europeu possui reflexos transfronteiriços, conduzindo o mundo na criação de um *mercado único digital*, advindo das necessidades comerciais de intercâmbio entre países europeus e não europeus, reforçando a necessidade do adequado tratamento jurídico à proteção de dados de caráter pessoal, preservando, dessa forma, um diálogo harmonioso entre os diversos ordenamentos jurídicos quando o assunto é a proteção de dados pessoais.

2. DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

2.1. A PROTEÇÃO DE DADOS PESSOAIS PRÉ LGPD

No Brasil, a proteção de dados pessoais ganha traços similares ao modelo regulatório europeu – que optou por uma normatização extensa e exaustiva sobre a proteção de dados pessoais (*regulamentação compreensiva*) -, distanciando-se de *modelos híbridos de regulamentação*³⁷, como acontece com os

³⁶ Os Estados Unidos da América optaram por um modelo regulatório distinto da União Europeia e considerado inadequado para a proteção de dados pessoais. Dessa forma, para preservar as relações comerciais que envolviam a colheita e transferência de dados entre empresas dos EUA e da UE, foi firmado acordo de transferência de dados pessoais, conhecido como *Safe Harbor*, que autorizava a coleta e transferência de dados de cidadãos europeus para estabelecimentos situados em território americano, desde que essas companhias se adequassem voluntariamente às disposições da Diretiva 95/46/CE. Contudo, importante destacar decisão do TJUE, no processo C-362/14, que julgou o referido acordo como inválido, por considerar frágil o sistema de “autocertificação” das companhias norte americanas pela simples adequação aos princípios estabelecidos pelo *Safe Harbor*.

³⁷ Modelos híbridos de regulamentação possuem características setoriais e autorregulatórias (MOSHELL, Ryan. *And There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*. *Texas Tech Law Review*, Vol. 37, 2005, p. 357-432, pp. 366-367), partindo-se da premissa de que “ninguém melhor do que o próprio interessado para saber quais são as lacunas que o Direito deve proteger, quais são as situações práticas do dia a dia que estão sem proteção jurídica e que caminhos de solução viável podem ser tomados”, conforme

Estados Unidos da América³⁸.

O primeiro instrumento jurídico voltado à análise do uso da tecnologia e suas implicações na sociedade brasileira remonta ao ano de 1984, com o advento da Lei n.º 7.232/1984, que estabeleceu a *Política Nacional de Informática*. Apesar de limitada às atividades de informática, a referida lei introduziu importantes princípios, como o “estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas” (art. 2.º, VIII) e o “estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas” (art. 2.º, IX).

Posteriormente à Lei n.º 7.232/1984, em 1990 entrou em vigor a Lei n.º 8.078/1990, também conhecida como *Código de Defesa do Consumidor*, que disciplinou sobre os bancos de dados e cadastros de consumidores, conferindo ao consumidor o direito de controlar suas informações pessoais³⁹, na medida em

observa PINHEIRO, Patricia Peck. *Direito digital*. 5.ª ed. rev. atual. e ampl., de acordo com as leis 12.735 e 12.737 de 2012. São Paulo: Saraiva, 2013. p. 103.

³⁸ FROMHOLZ, Julia M. The European Union data privacy directive. *Berkeley Technology Law Journal*, v. 15, 2000, p. 461-484, p. 461, observa que “the government has largely refrained from such regulation, instead allowing companies and associations to regulate themselves, save for a small number of narrowly drawn regulations targeting specific industries”. Contudo, apesar de optarem por uma regulamentação híbrida, os Estados Unidos América, para preservar as relações comerciais que envolviam a colheita e transferência de dados entre empresas dos EUA e da UE, firmaram acordo de transferência de dados pessoais, conhecido como *Safe Harbor*, que autorizava a coleta e transferência de dados de cidadãos europeus para estabelecimentos situados em território americano, desde que essas companhias se adequassem voluntariamente às disposições da Diretiva 95/46/CE, o que, contudo, fora considerado frágil pelo TJUE, no processo C-362/14, que julgou o referido acordo como inválido, devido a débil proteção conferida pelo sistema de “autocertificação” das companhias norte americanas pela simples adequação aos princípios estabelecidos pelo *Safe Harbor*.

³⁹ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 180.

que permite o “acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes”⁴⁰ (art. 43.º). Adicionalmente, estabelece que “os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos” (art. 43.º, § 1º); que “a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele” (art. 43.º, § 2º); e que “o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas” (art. 43.º, § 3º).

Já em 2011, ainda sem uma normatização adequada à proteção de dados pessoais, entrou em vigor no ordenamento jurídico brasileiro a Lei n.º 12.414/2011 (*Lei do Cadastro Positivo*), que veio disciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito (preâmbulo)⁴¹. Apesar de seu âmbito de aplicação restrito, a referida lei trouxe importantes reflexões inerentes ao tema em cotejo, como o conceito de banco de dados (art. 2.º, inciso I); o conceito de gestor (art. 2.º, inciso II); a proibição do armazenamento de dados que não sejam objetivos, claros, verdadeiros e de fácil compreensão (art. 3.º, § 1º), bem como o conceito do que é

⁴⁰ Com o advento do Decreto n.º 7.962/2013, estabeleceu-se no art. 4.º, inciso VII que “para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: (...) utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor”.

⁴¹ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 182, observa que a Lei do Cadastro Positivo permitiu que “a situação econômica do postulante ao crédito não é mais, somente, analisada a partir de dados relativos a dívidas não pagas, mas, também, a partir de outras informações que possam exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento”.

entendido como informações objetivas, claras, verdadeiras e de fácil compreensão (art. 3.º, § 2º, incisos I, II, III e IV); a proibição do tratamento de informações que sejam excessivas e sensíveis (art. 3.º, § 3º, incisos I e II), bem como o entendimento do que seriam informações excessivas e sensíveis (art. 3.º, § 3º, incisos I e II); direitos do cadastrado (art. 5.º); obrigações dos gestores de bancos de dados (art. 6.º); utilização específica dos dados coletados (art. 7.º); o compartilhamento de informações entre gestores (art. 9.º); e a responsabilidade civil dos bancos de dados, fontes e consulentes (art. 16.º).

Contudo, apesar dos importantes avanços legislativos a nível de direito comparado (v.g. o direito europeu), apenas em 2014, com a entrada em vigor da Lei n.º 12.965/2014, denominada de *Marco Civil da Internet* (MCI)⁴², o Brasil ganhou proteção normativa específica nas relações travadas na internet, estabelecendo princípios, garantias, direitos e deveres dos usuários, dos prestadores de serviço e do poder público (preâmbulo)⁴³. No que concerne à proteção de dados pessoais, verifica-se que todas as normas deságuam na figura do usuário, tendo o legislador nacional eleito como parâmetro normativo do MCI a *autodeterminação informacional*⁴⁴, na medida em que o consentimento prestado pelo usuário deverá ser “expresso sobre a coleta, o uso, o armazenamento e o tratamento de dados pessoais” (art. 7.º, inciso IX), inclusive para o caso de sua transferência para terceiro, salvo consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7.º, inciso VII); sendo vedada ainda a guarda “de dados pessoais que sejam excessivos

⁴² Importa registrar que a Lei n.º 12.965/2014, teve sua tramitação acelerada pelos escândalos de espionagem envolvendo Edward Snowden e a NSA.

⁴³ TAVARES, Letícia Antunes e ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. In: ONODERA, Marcus Vinicius Kiyoshi e FILIPPO, Thiago Baldani Gomes De (Coord.). *Brasil e EUA: Temas de Direito Comparado*. São Paulo: Escola Paulista da Magistratura, 2017, p. 155-204, p. 191.

⁴⁴ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 184.

em relação à finalidade para a qual foi dado consentimento pelo seu titular” (art. 16.º, inciso II); podendo, por fim, requerer o usuário a “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 na MCI (art. 7.º, inciso X). Adicionalmente, ao usuário são assegurados outros direitos, como: “inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação” (art. 7.º, inciso I); “inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei” (art. 7.º, inciso II); “inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial” (art. 7.º, inciso III); e “informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais”, que somente poderão ser utilizados para finalidades estabelecidas em lei (art. 7.º, inciso VIII, alíneas “a”, “b” e “c”).

Apesar de contemporâneo e de estabelecer também meios para proteção dos dados pessoais (arts. 10 a 12), o Marco Civil da Internet mostrou-se tímido e limitado⁴⁵, sendo insuficiente a proteção conferida pelo legislador aos dados pessoais, impossibilitando, inclusive, o cumprimento das normas estabelecidas em 2013 na Resolução n.º 68/167 da ONU (“*The right to privacy in the digital age*”), ironicamente de iniciativa do próprio governo brasileiro em parceria com o governo alemão.

No âmbito constitucional a proteção aos dados pessoais parece carecer do mesmo amparo legislativo, apesar da *Proposta*

⁴⁵ O MCI não conceituou o que seria banco de dados, não possibilitou expressamente a retificação de dados pessoais constantes em bancos de dados, não previu a transferência internacional de dados pessoais, não estabeleceu a criação de uma autoridade nacional supervisora, não trabalhou a totalidade dos *Fair Information Principles* (apesar de alguns princípios citados no art. 3.º) e postergou a proteção de dados pessoais a lei específica (art. 3.º, inciso III), que só veio a ocorrer com a edição da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018).

de Emenda à Constituição n.º 17/2019, ainda em tramitação no Congresso Nacional, buscar introduzir na CRFB a inclusão da proteção de dados pessoais no rol de direitos e garantias fundamentais^{46 47} (o que alteraria o art. 5.º da Constituição e incluiria o inciso XII-A). Seria possível, de forma temerária⁴⁸, extrair de nosso atual texto constitucional alguma proteção aos dados pessoais através de uma interpretação extensiva de alguns preceitos, como, por exemplo, o respeito à intimidade, à vida privada, à honra, à imagem das pessoas (art. 5.º, inciso X), à inviolabilidade das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5.º, inciso XII) e o *habeas data* (art. 5.º, inciso LXXII). Acontece que, eventual interpretação sistemática suscitaria dúvidas e dependeria inevitavelmente do arbítrio do próprio operador do direito, na medida em que o direito à privacidade ou o direito ao sigilo das comunicações – enquanto direitos fundamentais expressos -, confeririam uma tutela deficiente à proteção de dados pessoais (apenas ao fluxo de informações e não aos dados pessoais em si enquanto

⁴⁶ Importa registrar que o Brasil já reconhece desde 2003, na Declaração de *Santa Cruz de La Sierra*, que a proteção de dados é um direito fundamental das pessoas e sua regulamentação constitui importante iniciativa para proteger a privacidade dos cidadãos.

⁴⁷ Em contrapartida, a nível internacional, a proteção de dados pessoais já é reconhecida como direito autônomo e fundamental do indivíduo. Veja-se, como exemplo, a Convenção de *Strasbourg* (preâmbulo), a Diretiva 95/46/CE (art.º 1, n.º 1), a Carta dos Direitos Fundamentais da União Europeia de 2000 (art. 8.º) e a *General Data Protection Regulation* (preâmbulo), que consideram a proteção de dados pessoais direito fundamental do indivíduo e essencial para a proteção da pessoa humana; a Constituição Chilena, que com a reforma introduzida pela *Ley nº 21.096/2018*, passou a conferir uma proteção constitucional expressa a proteção dos dados pessoais (art. 19.º, n.º 4); as Constituições Portuguesa de 1976 (art. 35.º) e Espanhola 1978 (arts. 18.º, n.º 4 e 105.º), que regulam a utilização da informática, estabelecendo também, no caso da Constituição Portuguesa, referência expressa à proteção de dados pessoais.

⁴⁸ Para DONEDA, Danilo. A Proteção dos Dados Pessoais Como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n.º 2, p. 91-108, jul./dez. 2011, p. 104, parece existir “de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações”.

dados estáticos)⁴⁹. Interpretação similar se aplica ao *habeas data* enquanto remédio constitucional impetrado somente em face de entidades governamentais ou de caráter público (o que limitaria a proteção de dados pessoais, excluindo-se, por exemplo, as empresas privadas).

Não obstante a isso, enquanto aguardamos o Congresso Nacional na apreciação e aprovação da PEC n.º 17/2019 (ou de propostas similares), o constante desenvolvimento tecnológico e a rapidez no processamento de dados acelerou a busca por um modelo normativo mais técnico e restrito, condizente com a profundidade tecnológica utilizada no tratamento de dados pessoais tornou-se cada vez mais necessária e iminente, o que conduziu o legislador brasileiro a aprovar em 2018 a Lei n.º 13.709/2018, também conhecida como *Lei Geral de Proteção de Dados*, que “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado” (art. 1.º, primeira parte).

2.2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Influenciado diretamente pelo modelo regulatório europeu da *General Data Protection Regulation* (Regulamento 2016/679 da União Europeia) – não apenas por um *modelo regulatório compreensivo*⁵⁰, mas também pela criação de um *mercado único digital* - a atualização proposta pela LGPD – postergada pelo MCI (art. 3.º, inciso III) -, que somente entrará em vigor em agosto de 2020, surge em complementação as normas contidas no Marco Civil da Internet e representam importante avanço legislativo rumo a concretização de uma tutela jurídica

⁴⁹ Inclusive, o Supremo Tribunal Federal, no julgamento do Recurso Extraordinário n.º 418.516, de relatoria do ministro Sepúlveda Pertence, reconheceu a inexistência de proteção constitucional aos dados armazenados em computadores

⁵⁰ MOSHELL, Ryan. And There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection. *Texas Tech Law Review*, Vol. 37, 2005, p. 357-432, pp. 366-367.

adequada a proteção de dados pessoais a nível nacional.

Nessa toada, a Lei Geral de Proteção de Dados, começa por especificar que possui como *objetivos* a proteção dos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1.º, segunda parte), em consonância com o disposto pelo Parlamento Europeu (art. 1.º, n.º 2 da GDPR⁵¹).

Em seguida, estabelece de forma clara os *fundamentos da proteção de dados pessoais* eleitos pelo legislador ordinário, como o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2.º).

Mais adiante, num movimento de internacionalização das normas protetivas, estipula o legislador o *âmbito de aplicação* da Lei n.º 13.709/2018, resguardando a proteção dos dados coletados e tratados em território nacional, pouco importando se a operação de coleta ou tratamento seja realizada por pessoa natural ou jurídico, de direito público ou privado, e independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (art. 3.º), salvo se o tratamento de dados pessoais seja realizado nas hipóteses excetuadas no art. 4.º da LGPD, oportunidade em que a lei não será aplicada (v.g. para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais etc).

O artigo 5.º da lei veio para estabelecer *conceitos* importantes atinentes à proteção de dados pessoais, como: *dado pessoal*, compreendido como a “informação relacionada a pessoa natural identificada ou identificável”⁵² (art. 5.º, inciso I); *dado*

⁵¹ De acordo com o art. 1.º, n.º 2 da GDPR: “O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais”.

⁵² Repare que a definição adotada na legislação brasileira é limitada, isso porque a *General Data Protection Regulation* explica que os dados pessoais são informações

pessoal sensível, considerado os dados pessoais “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” (art. 5.º, inciso II); *dado anonimizado*, entendido como o “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (art. 5.º, inciso III); *banco de dados*, conceituado como o “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico” (art.º 5, inciso IV); *titular dos dados*, que seria a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (art. 5.º, inciso V); *bloqueio*, compreendido como a “suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados” (art. 5.º, inciso XIII); e *eliminação*, que seria a “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado” (art. 5.º, inciso XIV).

Por sua vez, o art. 6.º da LGPD determina que as atividades de tratamento de dados pessoais deverão observar a *boa-fé* e serão submetidas, por exemplo, a *princípios* relativos à finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, garantido a realização do tratamento dos dados para propósitos legítimos, específicos, explícitos e previamente informados ao titular, sem possibilidade de tratamento de forma incompatível com essas finalidades ou com as finalidades

relativas a uma pessoa singular identificada ou identificando, conceituando ainda que “é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular” (art. 4.º, n.º 1 da GDPR).

informadas ao titular, devendo-se limitar esse tratamento ao mínimo necessário para a realização das finalidades do pretendidas.

Já os artigos 7.º ao 14.º da Lei Geral de Proteção de Dados Pessoais estabelecem os *requisitos para o tratamento* dos dados pessoais, dados pessoais sensíveis e de dados pessoais de crianças e adolescentes, inclusive quando tratados pelo poder público (art. 23.º e ss.), assumindo o *consentimento* prestado especial condição, na medida em que ele deverá ser uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5.º, inciso XII), tendo o titular dos dados livre acesso e o direito de correção ou atualização de seus dados (art. 18.º, incisos II e III), permitindo-se ainda a revogação do consentimento prestado (arts. 8.º, § 5º e 18.º, inciso IX), a eliminação dos dados armazenados em bancos de dados (arts. 5.º, XIV e 18.º, incisos IV e VI), bem como solicitação da portabilidade de seus dados pessoais para outro responsável (art. 18.º, inciso V).

Para além dessas considerações, há de se observar que a LGPD adotou *medidas importantes para a proteção efetiva dos dados pessoais*, tais como: permitir a *transferência internacional* de dados pessoais somente para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na lei, o qual será avaliado pela autoridade nacional levando em consideração critérios como as normas gerais e setoriais existentes no país de destino ou organismo internacional, a natureza dos dados, a observância dos princípios gerais de proteção de dados e direitos dos usuários, a adoção de medidas de segurança, existência de garantias judiciais e institucionais, dentre outras circunstâncias (art. 33.º e ss) – o que coaduna com as medidas adotadas no capítulo V da GDPR, contribuindo para a criação de normas nacionais e internacionais efetivas quanto a proteção de dados pessoais -; obrigação de adotar

medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6.º, inciso VII); obrigatoriedade de o controlador de dados comunicar, em prazo razoável, à autoridade nacional e ao titular dos dados, a ocorrência de *incidente de segurança* que possa acarretar risco ou dano relevante ao titular (art. 48.º); previsão de uma *Autoridade Nacional de Proteção de Dados*⁵³ para zelar, implementar e fiscalizar o cumprimento da lei de dados brasileira em todo o território nacional (art. 5.º, inciso XIX); previsão de *sanções pecuniárias* elevadas em caso de infrações cometidas às normas estabelecidas na lei (art. 52.º e ss.).

Assim sendo, feitas tais considerações, percebe-se que a proteção de dados pessoais no ordenamento jurídico brasileiro galgou posição de destaque, não limitando-se a interpretações extensivas e esparsas sobre o tema. A positivação autônoma da proteção de dados pessoais a nível legal, confere o cuidado necessário ao tema, há muito negligenciado pelo nosso legislador.

CONSIDERAÇÕES FINAIS

A influência da *General Data Protection Regulation* do Parlamento Europeu e do Conselho da União Europeia (Regulamento 2016/679 da União Europeia) na Lei de Proteção de Dados Pessoais brasileira é indubitável e, em verdade, contribui para a criação de um *mercado único digital* indiscutivelmente forte e garantidor. Efetivamente, a semelhança no tratamento jurídico conferido à proteção dos dados pessoais permite-nos resgatar a segurança do cidadão enquanto usuário quando da utilização de seus dados pessoais.

Cumprido recordar, contudo, que a Europa - assim como já reconhecido pelo nosso governo na Declaração de *Santa Cruz*

⁵³ Criada posteriormente pela Lei nº 13.853/2019.

de *La Sierra* de 2003⁵⁴ - atribui expressamente o caráter de *direito fundamental* à proteção de dados pessoais (art. 8.º da Carta dos Direitos Fundamentais da União Europeia, juridicamente vinculativa, como direito primário da União Europeia (art. 6.º, n.º 1, do TUE), após a assinatura do Tratado de Lisboa em 2009), enquanto no ordenamento constitucional brasileiro limitamos a interpretações generalistas e temerárias, sem, para tanto, reconhecer o necessário tratamento autônomo do tema a nível constitucional⁵⁵.

Nesse sentido, em termos de conclusão, observa-se, hodiernamente, que o ordenamento jurídico brasileiro – ao menos em termos legais – acompanha a experiência legislativa de países europeus e confere efetivamente níveis adequados de proteção aos dados pessoais coletados e tratados em território nacional, principalmente se levarmos em consideração que as Leis n.º 7.232/1984 (*Política Nacional de Informática*), n.º 7.232/1984 (*Código de Defesa do Consumidor*), n.º 12.414/2011 (*Lei do Cadastro Positivo*) e n.º 12.965/2014 (*Marco Civil da Internet*) não conferiam tutela jurídica adequada e suficiente à proteção de dados pessoais⁵⁶. Nesse passo, a LGPD veio modificar o cenário

⁵⁴ Importa lembrar que o Brasil já reconhece desde 2003, na Declaração de *Santa Cruz de La Sierra*, que a proteção de dados é um direito fundamental das pessoas e sua regulamentação constitui importante iniciativa para proteger a privacidade dos cidadãos.

⁵⁵ HÄBERLE, Peter. *La Garantía del Contenido Esencial de los Derechos Fundamentales*. Trad. de Joaquín Brage Camazano. Madrid: Dykinson, 2003, p. 20, afirma que os direitos fundamentais são o fundamento funcional da democracia, transformando-se no “estatuto dos cidadãos nas suas relações com o poder”, conforme ensina MORAIS, Carlos Blanco de. *Fiscalização da Constitucionalidade e Garantia dos Direitos Fundamentais: Apontamento sobre os passos de uma evolução subjectivista*. In: CORDEIRO, António Menezes; LEITÃO, Luís Menezes; GOMES, Januário da Costa (Org.). *Estudos em Homenagem ao Prof. Dr. Inocêncio Galvão Telles*. v. 5. Coimbra: Almedina, 2003, p. 85-111, p. 86. Um direito, ao assumir o caráter de fundamental, adquire a posição de um *direito forte*, constituindo-se em verdadeiro trunfo político dos indivíduos face ao Estado (DWORKIN, Ronald. *Los Derechos en Serio*. 5.ª reimpr. Trad. de Marta Guastavino. Barcelona: Ariel, 2017, p. 37).

⁵⁶ Veja-se, como exemplo, o fato de a Lei n.º 7.232/1984, que estabeleceu a *Política Nacional de Informática*, ser limitada às atividades de informática, sem estabelecer

jurídico anterior, em que Leis eram promulgadas e entravam em vigor com disposições que já nasciam obsoletas⁵⁷, e promover um diálogo harmonioso entre os diversos ordenamentos jurídicos, tão necessário aos nossos tempos. Resta, agora, apenas aguardar a análise *in concreto* das implicações práticas da nova Lei Geral de Proteção de Dados, que entrará em vigor em agosto de 2020.

uma política nacional sobre a proteção de dados pessoais, apesar de já estar em vigor na Europa, desde 1981, a *Convenção 108 (Convenção de Strasbourg)*, para proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal; a Lei n.º 8.078/1990, também conhecida como *Código de Defesa do Consumidor*, se limitou a disciplinar sobre bancos de dados e cadastros de consumidores, num momento em que, repita-se, já encontrava-se em vigor na Europa a *Convenção 108 (Convenção de Strasbourg)*, que adotava medidas importantes para a proteção de dados pessoais, como as conhecidas *Fair Information Principles*; a Lei n.º 12.414/2011 (*Lei do Cadastro Positivo*), que possuía matéria restrita a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito; e a Lei n.º 12.965/2014, denominada de *Marco Civil da Internet*, que objetivava proteger juridicamente as relações travadas na internet, estabelecendo princípios, garantias, direitos e deveres dos usuários, dos prestadores de serviço e do poder público, derogando a proteção de dados pessoais a lei específica (art. 3.º, inciso III), isentando-se também de conceituar o que seria banco de dados, de não possibilitar expressamente a retificação de dados pessoais constantes em bancos de dados, de não prever a transferência internacional de dados pessoais, de não estabelecer a criação de uma autoridade nacional supervisora, e de não trabalhar a totalidade dos *Fair Information Principles*.

⁵⁷ Na medida em que, por exemplo, o *Marco Civil da Internet* – não tratava adequadamente a proteção de dados e até mesmo derogava sua proteção a lei futura – surgiu num dado período histórico onde já encontravam-se em vigor importantes normas jurídicas a nível internacional na proteção de dados pessoais, como a *Convenção 108* e a *Diretiva 95/46/CE*, que à época da promulgação do MCI já encontravam-se obsoletas no cenário europeu (já que a atualização proposta pela GDPR intensificou a proteção dada pela Diretiva 95/46/CE, e representou um modelo mais atual e condizente com a profundidade tecnológica utilizada no tratamento de dados).