UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
CURSO DE DIREITO

MYRLLA CARVALHO ALEXANDRE

A ALGORITMIZAÇÃO DAS PESSOAS SOB A PERSPECTIVA DO ARCABOUÇO JURÍDICO BRASILEIRO NA TUTELA DE DADOS PESSOAIS

SANTA RITA
2019

MYRLLA CARVALHO ALEXANDRE

A ALGORITMIZAÇÃO DAS PESSOAS SOB A PERSPECTIVA DO ARCABOUÇO JURÍDICO BRASILEIRO NA TUTELA DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, unidade Santa Rita, como exigência parcial da obtenção do título de Bacharela em Ciências Jurídicas.

Orientador: Prof. Dr. Adriano Marteleto Godinho

SANTA RITA

2019

Catalogação na publicação Seção de Catalogação e Classificação

A382a Alexandre, Myrlla Carvalho.
A algoritmização das pessoas sob a perspectiva do arcabouço jurídico brasileiro na tutela de dados pessoais / Myrlla Carvalho Alexandre. - Santa Rita, 2019.
134 f.

Orientação: Adriano Marteleto Godinho.
Monografia (Graduação) - UFPB/CCJ.

1. Proteção de dados pessoais. 2. Internet das Coisas. 3. Redes sociais. I. Godinho, Adriano Marteleto. II. Título.

UFPB/CCJ

MYRLLA CARVALHO ALEXANDRE

A ALGORITMIZAÇÃO DAS PESSOAS SOB A PERSPECTIVA DO ARCABOUÇO JURÍDICO BRASILEIRO NA TUTELA DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, unidade Santa Rita, como exigência parcial da obtenção do título de Bacharela em Ciências Jurídicas.

Orientador: Prof. Dr. Adriano Marteleto Godinho

Aprovado em: 23/09/2019

BANCA EXAMINADORA

_____

Prof. Dr. Adriano Marteleto Godinho (Orientador)

_____

Prof. Dra. Ana Paula Correia de Albuquerque da Costa (Examinadora)

_____

Prof. Dr. Valfredo de Andrade Aguiar Filho (Examinador)

A que possui a humanidade mais admirável: minha mãe.

AGRADECIMENTOS

A Deus, pois sem Ele nada seria.

A minha mãe, Maria de Lourdes de Carvalho, por ter me proporcionado a melhor educação que poderia, por seu estímulo incansável, pela dedicação, pelo amor, pela paciência, por acreditar em mim mesmo quando eu não acreditava, por ter respeitado todas as minhas escolhas, por ser meu maior exemplo de força e de ser humano, por ter essa alma tão simples (não simplória) e que, nessa simplicidade, faz exprimir toda a sua nobreza. Por fim, agradeço por muito mais do que alguém conseguiria transformar em palavras.

Aos meus amigos que prestaram palavras de incentivo e compreensão durante esses anos, em especial às que contribuíram imensamente nos estudos acadêmicos e ofereceram notável amizade e companheirismo: Josseana e Ana Júlia, minha simbiose. Tive imensa sorte em encontrar pessoas tão exemplares e disciplinadas, com as quais pude fazer incontáveis trabalhos, artigos, avaliações, além da participação conjunta em projeto de pesquisa e diversos eventos acadêmicos. Essa jornada não teria sido a mesma se eu não tivesse encontrado alguém compartilha a vontade de sempre fazer o melhor, como Josseana, tampouco se Ana Júlia não tivesse me inspirado com a sua determinação.

Ao meu namorado, Péricles, por toda a paciência, atenção, apoio, compreensão e por ter demonstrado como a caminhada é melhor quando se está acompanhada. Sua presença, ainda que apenas no último ano do curso, mostrou-se essencial para o desfecho. Em especial, agradeço por ter aderido às discussões a respeito do objeto desse estudo de forma tão atenciosa, provocando-me reflexões mais aprofundadas para consolidar o ponto de vista defendido no trabalho.

Ao meu orientador, Adriano Godinho, por ter lecionado o assunto de direitos da personalidade com tanta maestria e dedicação que me fez cultivar e manter o interesse pela matéria mesmo após o transcorrer de outros sete períodos. Como orientador, agradeço por toda a sua disponibilidade, incentivo e atenção.

“Devemos investir em humanidades tanto quanto investimos em tecnologia.” (LEONHARD, Gerd)

RESUMO

A algoritmização das pessoas consiste no manejo de algoritmos como um método de determinar diversos aspectos da vida humana, como a personalidade e as oportunidades, de forma a alterar o contexto individual e as condições socioeconômicas de modo geral. Nesse contexto, buscou-se perquirir como o ordenamento jurídico brasileiro visa efetivar a tutela de dados pessoais, em especial na Internet das Coisas e nas redes sociais. Para tanto, a questão foi analisada sob a perspectiva do tratamento de dados pelas empresas privadas e, metodologicamente, consiste numa pesquisa qualitativa, exploratória e documental. Nessa toada, foi promovida uma análise descritiva e crítica do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, diplomas legais específicos que versam acerca do recorte temático do presente estudo. Por conseguinte, foi verificado como o fenômeno da Internet das Coisas se relaciona com a coleta massificada de dados pessoais, bem como o seu liame com as expectativas da sociedade da informação e da vigilância. Após a explanação desses conceitos introdutórios acerca da Internet das Coisas, foi produzido um levantamento dos principais desafios da segurança cibernética e as possíveis soluções, cujo caráter sinuoso abrange tanto mecanismos a serem implementados pelas empresas, quanto posições a serem adotadas pela própria sociedade. Por fim, o trabalho também discorre sob a perspectiva das redes sociais, averiguando as disposições das Políticas de Privacidade a partir da base pricipiológica da Lei Geral de Proteção de Dados Pessoais, constatando como ocorre a monetização de tais dados e como os algoritmos são aplicados em benefício de quem os desenvolve, mecanismo que garante a rentabilidade da coleta de dados pessoais.

Palavras-chave: Proteção de dados pessoais; Internet das Coisas; Redes sociais.

ABSTRACT

The algorithmization of people consists in the management of algorithms as a method to determine several aspects of human life, like personality and opportunities, as a way to alter the individual context and socioeconomic conditions in general. In this context, it was inquired how the Brazilian legal system aims to apply the protection of personal data, especially in the Internet of Things and social networks. Therefore, the matter was analyzed from the perspective of data processing by private companies and, methodologically, consists of a qualitative, exploratory and documentary research. In this regard, it was promoted a descriptive and critical analysis of the Marco Civil da Internet and the Lei Geral de Proteção de Dados Pessoais, specific legal diplomas which disposes about the thematic of the present study. In sequence, it was verified how the Internet of Things phenomenon relates to the mass collection of personal data, as well as its link with the expectations of the information and surveillance society. After the explanation of these introductory concepts about the Internet of Things, a survey of the main cyber security challenges and possible solutions was produced, and the winding character encompasses both mechanisms to be implemented by companies and positions to be adopted by society itself. Lastly, the work also discusses from the perspective of social networks, investigating the provisions of Privacy Policies from the principle basis of the Lei Geral de Proteção de Dados Pessoais, noting how the monetization of these data occurs and how the algorithms are applied in benefit of the developer, a mechanism that ensures the profitability of collecting personal data.

Keywords: Protection of personal data; Internet of Things; Social networks.

LISTA DE SIGLAS

ANPD - Autoridade Nacional de Proteção de Dados

CC – Código Civil

CDC – Código de Defesa do Consumidor

CRFB/88 – Constituição da República Federativa do Brasil de 1988

DNT – Do Not Track

FDA - U.S. Food & Drug Administration

GDPR – General Data Protection Regulation

IoT – Internet of Things

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

MPDFT – Ministério Público do Distrito Federal e Territórios

NSA – National Security Agency

PEC - Proposta de Emenda à Constituição

PET - Privacy Enhancing Technologies

PNIC – Plano Nacional de Internet das Coisas

TJ-SP – Tribunal de Justiça do Estado de São Paulo

SUMÁRIO

1 INTRODUÇÃO

O advento dos avanços tecnológicos teve o condão de propiciar nítida modificação na sociedade, que passou a utilizar diversos dispositivos facilitadores para ações cotidianas, como conversar com amigos e familiares, fazer transferências bancárias, medir a quantidade de quilômetros percorridos numa corrida, ouvir áudios de aulas e o melhor: fazer tudo isso num mesmo momento, encaixando-se perfeitamente nos anseios imediatistas atuais. Nesse aspecto, houve a ascensão da sociedade da informação, visto que é movida por dados, mas também houve da sociedade da vigilância, como forma de potencializar a monetização dos dados pessoais e submetê-los à atuação de algoritmos, causando importante impacto nos âmbitos sociais, culturais, políticos e econômicos. Consequentemente, tanto na esfera internacional quanto no Brasil, foi reconhecida a necessidade de se criar um arcabouço jurídico apto a regular a proteção de dados pessoais. Nesse sentido, como modo de superar algumas normas setoriais, foi editada recentemente a Lei Geral de Proteção de Dados Pessoais, que entrará em vigor em agosto de 2020.

Considerando o recorte temático do direito à proteção de dados pessoais, o objeto do presente estudo consiste na algoritmização das pessoas sob o prisma do direito à proteção de dados pessoais, com enfoque nos dados tratados no âmbito da Internet das Coisas (IoT) e nas redes sociais. Por conseguinte, o problema consiste nos seguintes pontos: como o arcabouço jurídico brasileiro almeja proteger os dados pessoais das implicações negativas de ordem individual e social que podem advir da utilização da IoT e redes sociais? Quais são os resultados da aplicação de algoritmos na vida humana?

Nesse escopo, o objetivo geral do presente estudo se configura em pesquisar e analisar como o arcabouço jurídico atual pode servir como um instrumento ativo para a proteção de dados pessoais nos âmbitos das redes sociais e Internet das Coisas, bem como verificar as formas de utilização desses dados por empresas privadas que controlam esses âmbitos. Nesse contexto, insere-se os seguintes objetivos específicos: 1) examinar o tratamento jurídico brasileiro no que tange ao direito à proteção de dados pessoais, suscitando aspectos do direito comparado e conceitos de privacidade; 2) avaliar as particularidades relacionadas ao fornecimento de dados pessoais através do fenômeno da Internet das Coisas e o consequente aprimoramento da sociedade de vigilância; c) analisar as formas como as redes sociais se autorregulamentam para justificar a coleta de dados pessoais e como expõem a monetização desses dados, de modo a averiguar a diversidade de implicações que podem assumir através da aplicação de algoritmos.

Metodologicamente, no que tange à abordagem, será aplicada uma pesquisa qualitativa, uma vez que se busca, primordialmente, a qualidade dos dados a serem analisados em detrimento de quantificações, além de se ater nos aspectos relacionados à exploração, descrição e compreensão do problema (LAKATOS; MARCONI, 2017, p. 296). Quanto ao objetivo, será utilizada no presente estudo a pesquisa exploratória, visto que se almeja uma maior familiarização com o recorte temático a partir da perquirição de elementos relacionados, culminando no aprofundamento do objeto de estudo. Em concomitância, será efetuada uma pesquisa documental, pois se buscará o aprofundamento das informações acerca do tema sob a luz da perquirição normativa da Lei Geral de Proteção de Dados Pessoais, do Marco Civil da Internet, de algumas legislações estrangeiras, das Políticas de Privacidade de algumas empresas em destaque, além de serem utilizadas teses, dissertações, monografias, artigos e matérias jornalísticas, nacionais e internacionais. Desse modo, a pesquisa documental abrangerá diversos textos que contenham o recorte temático da proteção de dados pessoais no que diz respeito às implicações verificadas na seara da Internet das Coisas e das redes sociais.

Dito isso, a relevância científica deste trabalho consiste em abordar um tema em ascensão nas discussões da sociedade, mas que é muito mais pragmático do que teórico. Nesse ponto, é propício salientar que, embora haja um movimento crescente de estudo em tecnologia, ainda assim a quantidade de estudos jurídicos que tratam acerca do recorte temático abordado no presente trabalho não é tão expressiva e, por vezes, tais estudos se tornam limitados pelo objeto da pesquisa em si, pois se busca discutir aspectos que rapidamente são modificados no âmbito prático, em decorrência do advento de novas tecnologias. Dessa forma, o tema pesquisado se encontra num estágio em que está longe de ser esgotado, cabendo dizer que talvez nunca o seja. Assim, a contribuição teórica da presente pesquisa está em aprofundar questões que vêm sendo discutidas e que ainda estão em aberto, de modo a ampliar o debate e analisar as formas de propiciar a efetividade do arcabouço jurídico sobre o tema. Por outro lado, o presente estudo também possui relevante contribuição social, porquanto a violação do direito à proteção de dados pessoais e a algoritmização levam a implicações negativas concretas, seja em escala que atinge diretamente a autodeterminação das pessoas, seja no âmbito da sociedade em geral. Neste ponto, cabe adiantar que o manejo errôneo dos dados pessoais pode acarretar impactos negativos inclusive para a comunidade internacional, logo, evidencia-se a importância da proteção desses dados e da sua aplicação para os fins que estejam em consonância com a expectativa dos indivíduos.

Considerando o cenário exposto, o presente trabalho está dividido em três capítulos. O primeiro trata acerca da humanização do Direito Civil, buscando contextualizar a consolidação dos direitos da personalidade no ordenamento jurídico pátrio. Nesse sentido, será analisado o direito à privacidade e noções correlatas, propondo uma reflexão acerca de alguns dos conceitos mais notórios que foram atribuídos a esse direito, de modo a compreender como ele se relaciona com a conjuntura tecnológica atual. Após a explanação dessas noções iniciais, será promovida a perquirição normativa, primeiro traçando um panorama das legislações internacionais acerca da proteção de dados pessoais, visto que elas exerceram inegável influência no ordenamento jurídico brasileiro e, por fim, serão analisados o Marco Civil da Internet e, em especial, a Lei Geral de Proteção de Dados, por serem diplomas específicos da área e representarem a superação de um modelo normativo setorial.

O segundo capítulo, por sua vez, inicialmente abordará a consolidação da sociedade da informação e da vigilância sob o viés das empresas privadas e não do Estado, até mesmo porque para que o Estado exerça a sua vigilância, muito frequentemente se utiliza da tecnologia desenvolvida pelas empresas privadas. Nesse diapasão, serão apresentados aspectos relacionados à Internet das Coisas, bem como serão examinados os principais desafios para a promoção da segurança cibernética, ensejo no qual serão citados casos concretos para facilitar a visualização das problemáticas traçadas e realizar um levantamento dos principais mecanismos de efetivação da proteção de dados pessoais, não só pelas empresas, mas também pelos próprios indivíduos.

Por fim, o terceiro capítulo focará nas redes sociais, fazendo inicialmente uma perquirição das Políticas de Privacidade das redes sociais mais utilizadas no Brasil. Tal análise será promovida dialogando com a base principiológica da Lei Geral de Proteção de Dados Pessoais para, em seguida, discorrer acerca da monetização dos dados pessoais e a utilização cada vez mais expressiva de algoritmos, analisando os impactos individuais e sociais que podem causar.

Aqui, cabe adiantar que um dos pilares para a efetivação da tutela dos dados pessoais é que a própria sociedade também saiba proteger os seus dados e reconheça o valor que eles têm, de modo que se faz pertinente consignar que, não obstante o recorte temático seja complexo por envolver inúmeras áreas, buscou-se utilizar uma linguagem de fácil assimilação e extraindo a essência dos conteúdos, de forma a lograr êxito em viabilizar a democratização do conhecimento.

2 A PROTEÇÃO DOS DADOS PESSOAIS NA LEGISLAÇÃO BRASILEIRA E A PERSPECTIVA DO DIREITO CIVIL-CONSTITUCIONAL

A transição da vertente patrimonialista do Direito Civil brasileiro, consagrado no Código Civil de 1916, para a confirmação do viés humanístico adotado pela Constituição da República de 1988, estipulou expressivas modificações no que tange aos direitos da personalidade, que ainda hoje estão sendo paulatinamente acrescidos no ordenamento jurídico através de maior especificidade normativa, como é o caso do direito à proteção de dados pessoais. Em vista disso, neste capítulo será estudado o processo de humanização do Direito Civil, bem como será suscitada uma discussão preliminar acerca do direito à privacidade e noções correlatas, de modo a propiciar a análise do arcabouço legislativo internacional e brasileiro no que concerne à tutela de dados pessoais.

2.1 A humanização do Direito Civil

Em que pese o vasto histórico dos direitos da personalidade e as Constituições do México e de Weimar já terem disposto acerca da dignidade humana no início do século XIX, é notório que tais direitos se evidenciaram com o término da Segunda Guerra Mundial, que teve o condão de proporcionar mudanças significativas no que se refere ao reconhecimento da dignidade da pessoa humana, que passou a ser difundida nas constituições de inúmeros países e se tornou aspecto orientador das novas práticas estatais, tanto no cenário internacional[1], quanto no cenário nacional.

Neste âmbito, coube ao direito privado se readaptar, de modo a estar em consonância com o teor da Constituição de 1988 (CRFB/88). Tal situação engendrou o Código Civil de 2002 (CC), com nítida modificação de valores em relação ao de 1916, porquanto reafirmou o viés humanístico do ordenamento jurídico brasileiro, em detrimento do liberalismo com isonomia formal, individualismo e patrimonialismo exacerbado presente no Código de 1916. Registre-se que Orlando Gomes, em 1955, já preceituava esse fenômeno como a "despatrimonialização" ou "repersonalização" do Direito Civil (GOMES, 1955, p. 25).

Dessa maneira, a ascensão do que se passou a se chamar de Direito Civil-Constitucional ou Direito Civil Constitucionalizado colocou o ser humano no centro do

[1] A Declaração Universal dos Direitos Humanos pela Organização das Nações Unidas elencou a dignidade em seu artigo I. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 10 maio 2019.

ordenamento jurídico, afastando-se da tutela jurídica essencialmente patrimonial de outrora. A junção dos ramos em uma só denominação também possuiu outro objetivo: fazer com que o Código Civil seja visto como um diploma legal que deve ser objeto de hermenêutica à luz da Constituição, não bastando que seja analisado isoladamente, como acontecia antes.

Nesse aspecto, cumpre frisar que não se está pretendendo explanar que o Código Civil de 1916 não tinha nenhum dispositivo que abarcasse os direitos da personalidade, pois é consabido que tais direitos já eram reconhecidos mesmo durante a vigência desse Código, através da atividade interpretativa. Esse exercício hermenêutico ainda hoje se mostra fundamental, visto que se entende que não há um rol taxativo dos direitos da personalidade presente na legislação brasileira, configurando-se, portanto, num âmbito ainda em construção[2]. É nesse contexto que se insere os esforços do presente trabalho, pois os avanços tecnológicos impõem desafios cada vez mais expressivos para o desempenho da função dos direitos da personalidade, qual seja, a tutela da pessoa humana. Por tais razões e considerando a Era Digital vivenciada, acrescenta-se ao ordenamento a proteção de dados pessoais enquanto mais um direito da personalidade, conforme será melhor delineado posteriormente.

Destarte, o processo de humanização do Direito Civil e o seu alinhamento à Constituição da República, ao mesmo tempo em que dispôs expressamente sobre diversos direitos da personalidade, concedeu também a visão ampla necessária para a sua aplicação, pois as modificações sociais exigem atividade hermenêutica cada vez mais específica.

2.1.1 O direito à privacidade e noções correlatas

O direito à privacidade possui múltiplas definições, como não raro acontece no âmbito jurídico. Assim, para fins de melhor compreensão acerca do instituto, é imprescindível traçar um breve panorama sobre os conceitos desenvolvidos ao longo do tempo.

Em 1880, no livro "*A Treatise on the Law of Torts*", o Juiz Thomas Cooley explicou que a privacidade consistiria no "direito de ficar sozinho"[3] (HARDWICK, 2000, p. 674, tradução nossa). Posteriormente, em 1890, Louis Brandeis e Samuel Warren publicaram um artigo na *Harvard Law Review* intitulado "*The Right to Privacy*", que recebeu a alcunha de ser a primeira publicação acadêmica nos Estados Unidos a versar sobre esse direito, afastando

[2] Enunciado 274 da IV Jornada de Direito Civil: "Os direitos da personalidade, regulados de maneira não-exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1º, inc. III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação."

[3] No original: "Right to be let alone".

o caráter de propriedade aplicado até então e delimitando-o como uma tutela da personalidade humana. Os célebres juristas foram motivados a escrever o artigo em decorrência da exposição que os jornais da época desferiram a fatos relacionados ao casamento da filha de Warren (CANCELIER, 2017, p. 217), razão pela qual chegaram a inserir no artigo a afirmação de que a imprensa estaria ultrapassando os limites da propriedade e da decência (WARREN; BRANDEIS, 1890), ensejo no qual aludiram ao direito a ser deixado só, exarado por Cooley anteriormente. Assim, esse artigo teve o condão de potencializar o pensamento acadêmico e jurisdicional acerca do tema, suscitando discussões acerca dos limites que deveriam ser respeitados pela imprensa.

Por conseguinte, em 1891, a Suprema Corte dos Estados Unidos foi instada a apreciar o caso *Union Pacific Railway Company v. Botsford*. O processo foi motivado pela alegação de conduta negligente da empresa, que engendrou um acidente causando danos físicos a autora. Como estratégia de defesa, a empresa pugnou pela possibilidade de examinar cirurgicamente a autora, sem o seu consentimento, para determinar a extensão dos ferimentos. Nesse caso, a Corte exarou o seguinte entendimento[4] acerca do direito à privacidade (tradução nossa):

> Nenhum direito é considerado mais sagrado, ou mais cuidadosamente amparado pelo direito comum, do que o direito de todo indivíduo à posse e ao controle de sua própria pessoa, livre de toda restrição ou interferência de outros, a menos que por clara e inquestionável autoridade da lei.[5]

A partir dessa interpretação, foi consolidada a inserção do elemento "controle" para fins de definição de direito à privacidade. Posteriormente, a privacidade foi definida como a "condição da vida humana em que o conhecimento sobre uma pessoa ou assuntos da sua vida são pessoais e limitados a essa mesma pessoa"[6], conforme explicitou Hyman Gross (1967, p. 35-36, tradução nossa), ou seja, um conceito que parte de uma noção de limitação.

Em seguida, outros juristas, como Fried (1968, p. 482, *apud* O'BRIEN, 1978, p. 71) resgataram a noção de controle, passando a afirmar que a privacidade seria o controle dos

[4] Tal julgado teve como relator o juiz Horace Gray. De acordo com a *Supreme Court Historical Society*, Gray havia sido o juiz mais novo da história dessa Egrégia Corte até então, ao passo que também foi o primeiro juiz a contratar escreventes, dentre eles Louis Brandeis, razão pela qual este tinha oportunidade de discutir o mérito dos processos pendentes com o magistrado, ou seja, possuía influência sobre os resultados das prestações jurisdicionais (PEPPERS, 2006, p. 45), de modo que podia moldá-las ao seu ponto de vista.

[5] No original: No right is held more sacred, or is more carefully guarded by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.

[6] No original: privacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited.

indivíduos por suas próprias informações. Rodotá (2008, p. 16, *apud* FACCHINI NETO; DEMOLINER, 2018, p. 25) por sua vez, também seguiu a esteira da ideia de controle e definiu a privacidade como o "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".

Com a inserção da palavra "informação" dentro do conceito de direito à privacidade, alguns autores transmutaram o direito à privacidade no contexto tecnológico em "*informational privacy"* (LIN, 2002 apud PENNEY, 2008, p. 206), ou seja, a privacidade informacional, mantendo como fundamento o controle das próprias informações, nos termos aduzidos anteriormente. Todavia, Penney (2008, p. 207) traçou crítica acerca desse implemento, visto que não teria o condão de ajudar no conceito de privacidade, apenas de adicionar uma nova categoria para uma definição que já se demonstra complexa o suficiente. Além disso, Penney (2008, p. 240) também sintetizou as posições jurisprudenciais da Suprema Corte dos Estados Unidos em dois casos paradigmáticos, quais sejam, *Griswold v. Connecticut* e *Roe v. Wade*. Nesses casos emblemáticos, a vertente do direito à privacidade que o compreende enquanto um poder de tomar decisões esteve intrinsecamente relacionado com as decisões sobre o que ocorre com o próprio corpo, em especial a prevenção da gravidez e a retirada de feto. Em que pese as circunstâncias fáticas analisadas nos julgados não guardarem grandes semelhanças com o presente estudo, são relevantes os fundamentos nos quais ambas as decisões se apoiaram, notadamente a autonomia e a dignidade, que são os mesmos fundamentos jurídicos comumente associados ao direito à privacidade no Brasil.

O que se percebe, desse modo, são múltiplas definições. Por sua vez, a doutrina contemporânea, não satisfeita com os conceitos até então elaborados, tenta agregar mais categorias e explanar sobre diversos tipos de privacidade. Contudo, não cabe realizar análise pormenorizada dessas várias adições doutrinárias, tendo em vista que, como já relatado inicialmente, não há consenso doutrinário e muito do que é produzido contemporaneamente se trata de uma releitura dos conceitos já exarados aqui. Assim, o que ocorre não é um conceito ser substituído por outro apenas porque foi elaborado posteriormente ou estar mais adequado às circunstâncias atuais, como as novas tecnologias. O que ocorre, na verdade, é um complemento: o direito à privacidade é amplo e abrange tanto o direito de ficar sozinho, como preconizado por Cooley, quanto o direito a poder controlar as suas próprias informações, como os doutrinadores mais recentes indicam.

No Brasil, Tércio Sampaio Ferraz Júnior (1993, p. 440) versou que o direito à privacidade "tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito,

deseja manter para si, ao abrigo de sua única e discricionária decisão". Por outro norte, alguns doutrinadores associam outros termos ao conceito de privacidade, como a vida privada, intimidade, segredo, sigilo etc[7].

Insta salientar que a criação de novos conceitos, principalmente aqueles que buscam estar em consonância com as novas circunstâncias fáticas, estão de acordo também com a própria natureza mutável do Direito. Nessa toada, a doutrina costuma distinguir a privacidade do direito à privacidade, visto que enquanto a privacidade seria uma "condição existencial dos compromissos individuais, o direito à privacidade é abstrato, não absoluto, direito estendido a uma gama de interesses privados"[8] (O'BRIEN, 1978, p. 80, tradução nossa).

Por outro lado, não obstante a privacidade e a intimidade às vezes serem tratadas como sinônimo, a doutrina majoritária, a jurisprudência e até mesmo a CRFB/88[9] tratam como institutos diferentes ao preconizarem a inviolabilidade da intimidade e da privacidade. Assim, no que tange à intimidade, esta foi definida por Fried (1970, p. 142, tradução nossa), como "compartilhar informação sobre as ações de alguém, suas crenças ou emoções que não se compartilha com todos, até mesmo por se ter o direito de não fazê-lo"[10].

O Superior Tribunal Federal, por sua vez, além de também realizar distinção entre os institutos, também já aduziu definição de intimidade ao julgar, em 10 de outubro de 2017, o Recurso Especial 1445240/SP:

> RECURSO ESPECIAL. ART. 535 DO CPC/1973. NÃO VIOLAÇÃO. DANO MORAL. VALOR DA INDENIZAÇÃO. EXCEPCIONALIDADE. INTERVENÇÃO DO STJ. DIREITO À INTIMIDADE, PRIVACIDADE, HONRA E IMAGEM. VALOR DA INDENIZAÇÃO. CRITÉRIOS DE ARBITRAMENTO EQUITATIVO. MÉTODO BIFÁSICO. VALOR BÁSICO E CIRCUNSTÂNCIAS ESPECÍFICAS DO CASO. CONDUTA QUE CONFIGURA SEXTING E CIBERBULLYING.
> […]

[7] Nesse contexto, a doutrina alemã foi a responsável por criar a "teoria das esferas", de modo a distinguir, principalmente, três institutos: "a proteção da vida privada – esfera de maior amplitude – consiste no direito de subtrair do conhecimento do público em geral fatos da vida particular que não revelam aspectos extremamente reservador da personalidade do indivíduo. Já a intimidade – Intimsphäre [Vertrauensphäre em Costa Jr.] ou intimidade, em sentido lato na teoria alemã, refere-se à prerrogativa de se excluírem do conhecimento de terceiros as informações mais sensíveis do indivíduo, tais como aspectos atinentes à vida sexual, religiosa e política; compartilhadas apenas com as pessoas mais íntimas e em caráter reservado. Por fim, a esfera do segredo, Geheimnsphäre ou intimidade em sentido estrito na teoria alemã, compreende as informações relacionadas com os sentimentos, com os sonhos e com as emoções da pessoa; não compartilhadas com ninguém ou compartilhadas apenas com amigos mais íntimos" (VIEIRA, 2007, p. 30).

[8] No original: "Since privacy is an existencial condition of individuals' engagements, the right of privacy is an abstract, not an absolute, right extending to a range of privacy interests."

[9] Art. 5º, inciso X.

[10] No original: "Intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love."

> 3. Intimidade, na definição da doutrina, diz respeito ao poder concedido à pessoa sobre o conjunto de atividades que formam seu círculo íntimo, pessoal, poder que lhe permite excluir os estranhos de intrometer-se na vida particular e dar-lhe uma publicidade que o interessado não deseja. 4. Devem ser considerados como pertencentes à vida privada da pessoa não só os fatos da vida íntima, como todos aqueles em que não haja o interesse da sociedade de que faz parte.

Em suma, o que se depreende dos preceitos expostos é que o direito à privacidade não significa que assuntos altamente associados à personalidade ou à vida privada do indivíduo não possam ser publicados, como suas informações sensíveis, visto que é inerente a autonomia dos indivíduos poder compartilhar isso; trata-se, na verdade, do controle que os indivíduos podem ter de suas próprias informações.

Desse modo, o que se almeja delinear no presente trabalho é sob quais parâmetros ou sob qual sensação de segurança as pessoas consentem em compartilhar seus dados nas redes sociais e em objetos conectados à internet, bem como averiguar qual a utilização que é aplicada a essas informações compartilhadas com empresas privadas. Nessa conjuntura, é válido salientar que não se busca sustentar a perspectiva ilusória de que o direito à privacidade é absoluto. Ao contrário, parte-se do pressuposto que esse direito é passível de ser relativizado, como tantos outros, ao mesmo tempo em que se almeja expor como o arcabouço jurídico brasileiro busca conceder tutela efetiva do direito à privacidade e do direito à proteção de dados pessoais no âmbito tecnológico, considerando o viés não só individual, mas também social desses direitos.

2.2 Panorama da legislação internacional acerca da proteção de dados pessoais

No âmbito internacional, a proteção dos dados pessoais recebeu amparo legislativo há décadas. Aqui, cabe traçar breve panorama acerca das produções legiferantes da Europa, dos Estados Unidos e da América do Sul.

Na Europa, não obstante alguns autores elenquem a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais como um antecedente histórico de produção legislativa acerca da proteção de dados pessoais, atribui-se destaque ao Convênio nº 108 de 1981 do Conselho Europeu, que foi o instrumento responsável por estrear as disposições expressas acerca da proteção dos dados pessoais. O art. 5º preceituava que esses dados que fossem objeto de tratamento automatizado deveriam ser tratados de maneira leal e a lícita, voltados para finalidades previamente determinadas e legítimas, de forma adequada e não excessiva, além de serem conservados por tempo não superior ao estritamente necessário.

Nota-se, desse modo, uma preocupação exacerbada acerca da destinação concedida aos dados pessoais que recebiam tratamento automatizado, bem como versava acerca da mobilidade dos dados entre os países.

Por conseguinte, em 1995, foi editada a Diretiva nº 95/46, destinada a regular a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos dados colhidos. Assim, a diretiva invocou alguns dos preceitos já expostos no Convênio nº 108, como os do artigo supracitado, assim como aduziu novas disposições e definições de dados pessoais, tratamento de dados pessoais, consentimento da pessoa em causa etc. Ainda, em seu art. 8º, a Diretiva trouxe uma disposição importante acerca dos dados sensíveis: "Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e á vida sexual", estipulando, em seguida, uma série de exceções a essa regra. Salienta-se que essa definição do que seriam os dados sensíveis é basicamente a mesma que se encontra atualmente no art. 5º, II, da Lei Geral de Proteção de Dados Pessoais (LGPD), tendo sido acrescentado apenas os dados genéticos e biométricos. Outra disposição que merece destaque é a previsão de que cada Estado deveria criar órgão público com a finalidade de fiscalizar a aplicação da legislação de proteção de dados pessoais, conforme o art. 28, nº 1, preceito que também foi implementado na LGPD.

Cinco anos depois, a Carta dos Direitos Fundamentais da União Europeia também preconizou, no art. 8º, que é inerente a todas as pessoas o direito à proteção dos seus dados pessoais, bem como ter acesso a eles e poder retificá-los. No ensejo, reafirmou que o tratamento de dados concedido deve se ater aos fins específicos, conforme o consentimento dado pela pessoa interessada, além de destacar que haveria fiscalização para o cumprimento dessas regras, do mesmo modo como a Diretiva nº 95/46 indicou.

Recentemente, em 15 de abril de 2016, foi aprovada a *General Data Protection Regulation* (GDPR) da União Europeia. Esse Regulamento, que entrou em vigor em maio de 2018, substituiu a Diretiva nº 95/46, buscando atualizar as normas em virtude dos novos e expressivos avanços tecnológicos.

No parágrafo 11 das considerações da GDPR, consta a seguinte explanação com viés introdutório: "A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais". Nesse contexto, houve a inclusão do direito a ser esquecido, no art. 17, o direito de portabilidade dos dados, no art. 20,

o direito de oposição ao tratamento dos dados, nos termos do art. 21 etc. Contudo, é na abrangência a nível mundial da eficácia das normas que o Regulamento em questão recebeu destaque, visto que é aplicado quando o tratamento dos dados pessoais é realizado no "contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União", além de ser aplicado no tratamento de dados pessoais de pessoas que residem no território da União Europeia, conforme preceitua o art. 3º. Dessa forma, houve ampla divulgação para que até mesmo os brasileiros que exercem atividade empresária que lide com o tratamento de dados pessoais de residentes da União Europeia se adequassem às regras.

Por outro lado, nos Estados Unidos não há uma legislação única. Enquanto na União Europeia o GDPR trata de maneira geral sobre a matéria, as legislações destinadas à proteção de dados pessoais nos Estados Unidos são esparsas e dotadas de alta especificidade quanto às suas matérias, visto que há legislação específica acerca dos dados no âmbito médico, bancário etc, quais sejam: *Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act ou Financial Services Modernization Act of 1999, Fair Credit Reporting Act (FCRA), Freedom of Information Act of 1996 – FOIA, Privacy Act 1974, Electronic Communications Privacy Act (ECPA) e USA Patriot Act of 2001*.

Sabe-se que os Estados Unidos vêm tendo uma série de problemas com a questão dos dados pessoais, especialmente em 2013, ano no qual foram vazadas informações sobre a vigilância generalizada proporcionada pelo Estado e, mais recentemente, em 2018, houve o escândalo da Cambridge Analytica-Facebook, que será detalhado posteriormente. Nessa toada, atualmente os EUA possuem como destaque a *California Consumer Privacy Act* (CCPA), que entrará em vigor em 2020 e possui semelhanças com o GDPR, tendo sido editada pelo estado da Califórnia. Assim, algumas entidades da indústria de publicidade dos Estados Unidos criaram uma coalização[11] para que o Congresso norte americano crie uma lei em âmbito federal acerca do tema, visando impedir, dessa forma, que cada estado crie suas próprias leis.

Desse modo, depreende-se que uma parcela significativa dos problemas que os Estados Unidos enfrentam no tocante a violação da privacidade das pessoas é atribuída a uma legislação fragmentada e lacunosa. Ainda, se cada estado criar suas próprias leis, irá dificultar sobremaneira a efetiva tutela da proteção de dados pessoais dos indivíduos, tornando difícil,

[11] Disponível em: https://www.meioemensagem.com.br/home/midia/2019/04/09/industria-dos-eua-cria-coalizacao-sobre-protecao-de-dados.html. Acesso em: 16 jun. 2019.

também, o trabalho das empresas em se adequar às legislações, não só dos países, mas de inúmeros estados dentro de um mesmo país.

Na América do Sul, por sua vez, diversos países já contavam com legislação específica acerca da proteção de dados pessoais, como o Chile, desde 1999; a Argentina, desde 2000; o Paraguai, desde 2001; o Uruguai, desde 2008; o Peru, desde 2011, a Colômbia, desde 2012 etc. Cumpre destacar que esses países não elaboraram legislações tão genéricas como a União Europeia, havendo, por vezes, destinação a setores específicos. Todavia, os países da América do Sul começaram a se preocupar com esse tema muito antes do Brasil, tendo legislações há quase vinte anos. Nesse ponto, não há justificativa plausível para a mora legislativa brasileira, visto que o país é uma expressiva potência econômica global e a sua população há anos se constitui como um dos maiores públicos de diversos sítios eletrônicos.

Assim, não obstante o Brasil tivesse inúmeras razões para ter editado normas específicas voltadas para as atividades no âmbito digital há vários anos, isso só ocorreu em 2014, com o advento do Marco Civil da Internet (MCI), tendo sido necessário a divulgação de um grande escândalo internacional atingindo a presidente da república para apressar a sua publicação.

2.3 O Marco Civil da Internet e sua importância na proteção de dados pessoais

Em junho de 2013 a população mundial se tornou espectadora do que se tornou o maior escândalo de violação de privacidade até então: Edward Snowden, ex-consultor da Agência de Segurança Nacional Americana (NSA) foi o responsável por vazar informações a jornalistas do The Guardian acerca de interceptações telefônicas ilegais e monitoramento de inúmeras pessoas ao redor do mundo, através de acesso a e-mails, videoconferências, fotos e conversas dos usuários que utilizavam os serviços de empresas como o Google, Facebook, Skype, Microsoft e Apple. Tais violações foram promovidas pelo FBI e NSA e atingiram não apenas inúmeros cidadãos sem nenhuma finalidade específica, como também os presidentes de diversos países, como Dilma Rousseff, além de empresas que ocupam posição importante mundialmente, como a Petrobrás. Aqui, cabe delinear que a aplicação das legislações brasileiras aos casos de espionagem estrangeira é algo a ser debatido em outra ocasião, porquanto as práticas de inteligência e contrainteligência utilizadas por governos, embora seja assunto tangente, ainda assim guarda um pouco de distância do objeto do trabalho.

Isto posto, observa-se que esse cenário propiciou o aumento da necessidade para aprovar uma lei que versasse especificamente sobre a proteção de dados pessoais na internet.

O Brasil já contava com algumas normas tutelando os dados pessoais, como o CDC, a Lei do Cadastro Positivo e a Lei dos Crimes Informáticos, contudo, o MCI, consubstanciado na Lei nº 12.965/2014, configura-se a primeira legislação brasileira específica versando acerca dos princípios, garantias, direitos e deveres para o uso da Internet, com enfoque no direito à privacidade, liberdade de expressão, neutralidade de rede e na proteção dos dados pessoais, de modo que inaugurou uma normatização mais aprofundada acerca deste direito.

O projeto ficou cerca de dois anos e meio na Câmara dos Deputados e teve uma passagem altamente célere pelo Senado, que não realizou nenhuma modificação no texto. Houve dois motivos essenciais para a pressa, conforme explana Marcacini (2016):

> [...] o Senado recebeu e aprovou o projeto que vinha da Câmara em uma só tacada, tudo a permitir que a Presidência da República pudesse sancionar a nova Lei durante a apresentação do congresso internacional –NET Mundial –que se realizava em terra brasilis naquela semana e contava com a presença de alguns dos maiores gurus da Internet mundial. Em apenas um mês, contado da aprovação na Câmara, o texto passou pelo Senado, sendo ali votado e aprovado sem qualquer modificação, e foi prontamente sancionado e publicado como Lei. Outro fator bizarro também acelerou o trâmite do projeto de lei, enquanto este ainda se encontrava na Câmara dos Deputados. A Presidência da República solicitou a aplicação de regime de urgência constitucional para apreciação do projeto, motivada pelas revelações trazidas à luz por Edward Snowden acerca das atividades de espionagem da National Security Agency –NSA.

A urgência em querer publicar lei acerca do tema provavelmente interferiu no amadurecimento das discussões no Senado Federal, o que fez com que inúmeros juristas, como o autor citado acima, tenham tecido duras críticas ao texto normativo, não obstante seja pacífico que o MCI trouxe disposições importantes acerca da liberdade no âmbito da internet. Nesse aspecto, Marcacini (2016) critica que o MCI se trata de "mais uma lei frustrante, que, prolixa, fala muito, regula pouco e deixa em aberto um significativo número de interrogações".

Dentre outras disposições, o MCI foi o responsável por versar acerca da neutralidade da rede. Enquanto ainda era um projeto de lei, grande parte das discussões se concentraram nessa temática, visto que alguns adotaram a postura que estabelecer a neutralidade da rede violaria a livre iniciativa e a concorrência. Contudo, no Brasil já há poucas empresas provedoras de internet e o estabelecimento da neutralidade, conforme explica Marcacini (2016), "não impede que sejam ofertados serviços de conexão com bandas mais ou menos largas, a preços diferentes".

Por conseguinte, a lei reservou o capítulo II para os direitos e garantias dos usuários. Nesse ponto, cabe aduzir que no anteprojeto o art. 7º detinha apenas cinco incisos, ao passo

que, quando a lei foi sancionada, o mesmo artigo já contava com treze incisos, alguns dos quais apenas ressaltando o viés da proteção dos dados pessoais, como o inciso I, que recebeu a redação de que é assegurado aos usuários o direito a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação", bem como o inciso III, que assegura o direito a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial". Interessante notar que o primeiro inciso, ao mesmo tempo em que versa acerca da inviolabilidade, deixa explícita as sanções civis às quais estarão sujeitos aqueles que não respeitarem o conteúdo da norma, o que não deixa de ser uma forma curiosa de se iniciar o rol de direitos. Há que se lembrar que esses incisos foram acrescentados na conjuntura pós-Snowden, assim, houve nitidamente a preocupação de assegurar a maior amplitude de direitos.

De modo consecutivo, tem-se que o art. 7º, incisos VII a IX merece especial atenção. O inciso VII salienta que é assegurado ao usuário o "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". Essa adjetivação do consentimento remete para que ele seja inequívoco e específico, assim, não basta que a empresa informe que os dados pessoais podem ou serão fornecidos a terceiros, pois também precisam especificar a finalidade desse fornecimento e com quem os dados serão compartilhados. Assim, o inciso VIII destaca que as informações dadas aos usuários acerca das operações efetuadas com seus dados devem ser claras e completas, além de elencar que as finalidades dessas operações devem ser justificadas, não podem ser vedadas pela legislação pátria e devem estar especificadas nos contratos ou nos termos de uso.

Concomitantemente, o MCI trouxe disposições específicas sobre a privacidade e dados pessoais, inseridos na seção II, a maior da lei, o que reflete o seu grau de importância. Para o presente estudo, cabe destacar que a guarda e a disponibilização de dados pessoais deve observar à proteção da intimidade, da vida privada, da honra e da imagem das pessoas, ainda que estejam apenas indiretamente envolvidas, conforme o *caput* do art. 10. Além disso, as medidas de segurança e de sigilo devem ser informadas de modo claro por aquele que presta o serviço, segundo o § 4º desse mesmo artigo. Tal preceito, como se verá, foi reiterado na LGPD. Por sua vez, o art. 11 preconiza que qualquer operação que envolva dados pessoais, como a coleta, por exemplo, já torna obrigatória a observância da legislação nacional e, em caso de violação às normas elencadas nesses dois artigos, a empresa fica sujeita a sanções como advertência, multa, suspensão temporária das atividades que envolvam o art. 11 ou a proibição definitiva de tais atividades.

Em sequência, a seção III versa acerca da responsabilidade por danos decorrentes do conteúdo elaborado por terceiros, oportunidade na qual, acertadamente, dispôs que os provedores de conexão à internet não possuem responsabilidade civil em casos como esse, conforme o art. 18. Nesse ponto, houve uma ressalva, elencada no art. 19, que preceitua que há responsabilidade na hipótese de, após ordem judicial, o conteúdo não ser retirado. Esse preceito se revela congruente porque retira dos provedores o dever de fiscalizar o conteúdo gerado pelos usuários e de ser responsabilizado pelas infrações alheias. Caso fosse responsável, haveria a dificuldade de monitoramento das inúmeras pessoas, bem como tornaria o âmbito da internet excessivamente moderado, visto que, em qualquer hipótese de dúvida, o provedor retiraria o conteúdo gerado pelo usuário como forma de se salvaguardar, ao passo que mitigaria sobremaneira a liberdade de expressão de usuários, pois nem sempre a decisão de retirar o conteúdo seria correta.

Por fim, cabe reafirmar a importância do Marco Civil da Internet no ordenamento jurídico pátrio, importância que foi salientada pelo contexto histórico em que foi aprovado. Contudo, em que pese os avanços na proteção de dados pessoais, ainda assim subsistiu a necessidade de realizar uma lei mais específica acerca do tema.

2.4 Lei Geral de Proteção de Dados Pessoais (LGPD): análise descritiva e crítica

Prestes a ser afastada em decorrência do processo de *impeachment*, Dilma Roussef encaminhou, em maio de 2016, juntamente com solicitação de urgência, o anteprojeto de normas de proteção de dados pessoais à Câmara dos Deputados, que passou a ser nomeado como PL 5276/2016. Foram realizadas diversas audiências públicas como modo de enriquecer o conteúdo do projeto de lei, bem como buscar pela harmonização de interesses antagônicos dos diversos segmentos da sociedade.

Conjuntamente, ainda no contexto histórico para a aprovação do que viria a se tornar a Lei nº 13.709/2018, houve a eclosão do escândalo Cambridge Analytica-Facebook, que teve o condão de expor que os dados inseridos em ambiente que as pessoas estão mais despreocupadas – redes sociais – não estão seguros, bem como gerou o alerta que os dados pessoais, ainda que contenham informações subvalorizadas pelos indivíduos, podem assumir outras conotações quando utilizados para finalidades adversas e, assim, atingirem não apenas a esfera individual, como também a coletiva. No caso, o escândalo esteve diretamente relacionado com eleições democráticas. Como consequência, esse acontecimento contribuiu sobremaneira para apressar o trâmite do projeto de lei no Congresso Nacional.

No que tange ao conteúdo da lei, verifica-se que é sistematizada em dez capítulos divididos da seguinte forma: disposições preliminares, tratamento de dados pessoais, direitos do titular, tratamento de dados pessoais pelo Poder Público, transferência internacional de dados, agentes de tratamento, segurança e boas práticas, fiscalização, Autoridade Nacional de Proteção de Dados (ANPD) e disposições finais e transitórias. Desde já, é importante frisar que ela só entrará em vigor em agosto de 2020.

Por conseguinte, cabe realizar uma análise mais detida dos dispositivos dessa legislação, sob o enfoque do tratamento de dados realizado por empresas privadas, de forma que o tratamento feito pelo Poder Público deverá ser objeto de estudo aprofundado em outra ocasião. Assim, é estipulado desde o art. 1º que o tratamento de dados pessoais deve ser pautado na observância do direito à liberdade, à privacidade e o livre desenvolvimento da personalidade da pessoa natural. O art. 2º, por sua vez, versa acerca dos fundamentos da proteção de dados pessoais, sendo cabível destacar o desenvolvimento tecnológico e inovação, previsto no inciso V.

Em sequência, o art. 5º, um pouco tardiamente, estipula os conceitos de dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, encarregado, tratamento, anonimização, consentimento, bloqueio, eliminação, transferência, uso compartilhado de dados, dentre outros. Alguns desses conceitos são relevantes para serem destacados, em virtude de que requer maior aprofundamento. Nesse ponto, ressalta-se os seguintes conceitos:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> [...]
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

O conceito expansionista de dado pessoal, abrangendo tanto a pessoa identificada como identificável está em consonância com a conceituação realizada por diversos blocos econômicos, organismos internacionais e países, a exemplo da OCDE, União Europeia, Canadá e Argentina (BIONI, 2019, p. 74). Elencar a pessoa identificável parte da premissa de que ainda que se trate de uma base de dados anonimizada, ainda assim é possível que essa base seja combinada com outra ou que sejam utilizadas tecnologias que gerem uma posterior individualização ou identificação da pessoa. Dessa forma, um dado anonimizado também poderia ser considerado, em última análise, um dado pessoal, de modo equivocado; contudo, é imperioso que seja feita a seguinte distinção: o dado anonimizado consiste naquele em que o seu titular não pode ser identificado. Não se trata aqui de um conceito absoluto, visto que a norma preceitua que a anonimização só é considerada dessa forma enquanto for utilizado meios técnicos razoáveis e disponíveis no momento do seu tratamento, ou seja, é algo potencialmente circunstancial. Nesse sentido, o dado anonimizado pode ser compreendido como aquele em que será especialmente difícil de ser identificável.

Entender que os conceitos de dados anonimizados e dados pessoais de pessoas identificáveis não podem ser confundidos é essencial, porquanto o próprio GDPR informa, no parágrafo 26 das considerações inicias, que os princípios da proteção de dados não se aplicam às informações anônimas, por exemplo, enquanto que o art. 12, *caput*, da LGPD, enfatiza que os dados anonimizados não serão considerados dados pessoais, exceto se a anonimização for revertida, com meios próprios ou utilizando esforços razoáveis. No que tange a essa razoabilidade suscitada, o § 1º, do mesmo artigo, explana que a aferição da razoabilidade se dará através de fatores objetivos, como o tempo e o custo necessário para reverter o processo de anonimização, utilizando as tecnologias que estejam disponíveis e observando a "utilização exclusiva de meios próprios". Assim, a lei se revela bastante completa no que diz respeito às definições e explicações sobre conceitos, de modo a torná-la clara e acessível. Ressalte-se que o GDPR aduziu explicação similar no parágrafo 26 das considerações iniciais, de modo que LGDP inovou, em relação àquele Regulamento, apenas no que se refere à "utilização exclusiva de meios próprios".

O dado pessoal sensível, por sua vez, abrange uma série de informações ligadas ao mais íntimo da pessoa, de modo que a pretensão da legislação ao caracterizá-los como sensíveis é conceder uma proteção maior e específica, como a vedação ou regulamentação por parte da autoridade nacional de comunicação ou o uso compartilhado desses dados entre controladores que almejam auferir vantagem econômica, conforme o art. 11, § 3º. Registre-se que, por

"controlador", o art. 5º, inciso VI, conceitua como aquele que possui competência para as decisões atinentes ao tratamento de dados.

Após analisadas as diferenças entre os dados pessoais, é pertinente discorrer acerca dos bancos de dados. Aqui, abre-se um parêntese para tratar do assunto primeiramente sob o ponto de vista do Código de Defesa do Consumidor, que distingue os bancos de dados e os cadastros de consumo, que estão elencados nos arts. 43 e 44 do CDC e fazem parte do gênero arquivos de consumo. Nesse aspecto, Souza, Werner e Neves (2018, p. 150) explicam que os cadastros de consumo consistem em dados direcionados apenas a pessoa imediata com quem se estabeleceu uma relação de consumo, ou seja, apenas ao fornecedor, que também é o arquivista, e geralmente há a anuência do consumidor. Por outro lado, nos bancos de dados o fornecedor e o arquivista são figuras que não se confundem, visto que o intuito é a transmissão desses dados a terceiros, não sendo voltados apenas para uma atividade comercial imediata. Frise-se, ainda, que neste tipo de arquivo não há autorização prévia do consumidor. Assim, no que tange a esses aspectos, o art. 43 do CDC garante que o consumidor poderá ter "acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes", podendo, ainda, solicitar a correção dessas informações e dados.

Todavia, não obstante a doutrina e a lei específica realizarem distinção entre esses arquivos, observa-se que essa diferença também foi impactada pragmaticamente pelos novos contornos identificados na sociedade atual. A partir desse pressuposto, Bioni (2019, p. 46) defende que "tal taxonomia deixa de fazer sentido na sociedade da informação. Nela, o fluxo de informações é constante, o que acaba por desbancar todos os elementos acima listados que diferenciariam bancos de dados de cadastros de consumo". A transmissibilidade se tornou quase inerente ao fornecimento de dados.

Por sua vez, a LGPD entende que o banco de dados seria o "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico", conforme a redação do art. 5º, IV.

Insere-se, nesse contexto, uma verdadeira figura que pode ser denominada como dados volantes. Justifica-se o vocábulo "volante" porque está apto a conferir a dimensão e rapidez em que os dados são trocados, bem como se dá a ideia de local mutável em que os dados se encontram, considerando a prática habitual de compartilhamento com terceiros. A mobilidade veloz dos dados desponta, assim, como um diferencial, visto que é uma característica extra do que se explana no conceito de banco de dados e está em plena conformidade com a sociedade

de informação, visto que os dados do consumidor coletados atualmente por alguém com que se estabelece uma relação comercial, dificilmente se restringe apenas a essa pessoa.

Por outro lado, e ainda no que concerne à proteção dos dados pessoais, tem-se que a LGDP se restou completamente omissa a respeito dos dados das pessoas falecidas. Isso traz diversas implicações sobre o gerenciamento da chamada "herança digital" e se ela seguirá a ordem de vocação hereditária.[12]

No presente estudo, adota-se o posicionamento de que os herdeiros não devem possuir amplo acesso a todos os dados e conteúdos que foram inseridos no sítio eletrônico, como conversas privadas em redes sociais. Contudo, revela-se acertado que os herdeiros possam decidir qual destino aplicar a eles. Uma visão que defenda que apenas deve haver transferência da herança digital caso a pessoa indique o(s) herdeiro(s) ainda em vida acarretaria, em última análise, no estabelecimento do próprio sítio eletrônico como "herdeiro", vulnerabilizando, por consequência, os dados pessoais. Entretanto, caso haja a designação de herdeiros pelo titular dos dados, é imperioso que a autonomia da vontade seja respeitada. Registre-se que alguns *sites* facilitam esse processo, em virtude de que disponibilizam áreas para que as pessoas manifestem o desejo de designar um "contato herdeiro", oportunidade na qual essas pessoas poderão definir o que ocorre com a conta; essa política é adotada por empresas como o Facebook e Google.

Insta salientar que, mediante a defesa do posicionamento de que o próprio titular dos dados pode indicar alguém para geri-los após a sua morte, sem necessidade dos herdeiros legítimos entrarem nesse rol, cabe aduzir, ainda, a possibilidade de fragmentação da herança digital. Isto porque uma das contas pode ser controlada por um herdeiro designado, não necessariamente legítimo, e em outras, nas quais não haja qualquer indicação específica, apenas os herdeiros legítimos iriam poder controlar o destino do perfil *online*.

Após familiarização dos conceitos supracitados, é cabível prosseguir na perquirição normativa. Assim, o art. 3º preceitua em quais hipóteses a lei é aplicada, sendo elas, basicamente: a) quando o tratamento dos dados é realizado no território nacional; b) quando o

[12] Nesse contexto, há alguns projetos de leis em trâmite que visam acrescentar artigos no Código Civil e/ou no Marco Civil da Internet, como o Projeto de Lei nº 4.847, de 2012, que pretende aduzir disposição explanando que se o falecido, com capacidade para elaborar testamento, não o tiver feito, a herança será transmitida aos herdeiros legítimos, ao passo em que, conforme a redação do art. 1.797-C que se pretende aduzir ao CC, cabe ao herdeiro definir o destino das contas do falecido, de modo a transformá-las em memorial, apagar todos os seus dados ou remover a conta. Tal projeto ainda define a herança digital como o "conteúdo intangível do falecido, tudo o que é possível guardar ou acumular em espaço virtual", conforme a redação do art. 1.797-A que se pretende acrescentar ao CC. De modo concomitante, há também os projetos de lei nº 7.742/17 e o 4.099-B/12, que igualmente enquadram a herança digital inserida no campo da sucessão legítima, ficando a cargo dos herdeiros definir qual será a destinação dos dados e das contas dos falecidos.

tratamento tenha por finalidade a oferta ou o fornecimento de bens ou serviços; c) quando os dados pessoais tenham sido coletados de indivíduos que se encontrem em território nacional, ainda que momentaneamente, conforme o § 1º desse mesmo artigo.

Já o art. 6º lista os princípios - de forma não exauriente - que o tratamento de dados pessoais está sujeito: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Tais princípios são similares aos encontrados no art. 5º do GDPR, de modo que houve forte influência do regulamento europeu na legislação pátria. Aqui, cabe frisar que a lei assegurou que a finalidade do tratamento dos dados seja para propósitos legítimos, específicos, explícitos e informado. Todavia, a GDPR adotou o adjetivo "expresso", em vez de "específico", o que é mais adequado, considerando que "esse qualificador é o que semanticamente representaria melhor esse nível de participação mais intenso do cidadão no fluxo dos dados" (BIONI, 2019, p. 203), visto que o adjetivo "específico" incorre em pleonasmo, na medida em que a lei já dispõe que o consentimento deve ser destinado a finalidades determinadas.

O art. 7º também revela sua importância, visto que aduz as hipóteses em que o tratamento de dados pessoais poderá ser efetuado, consubstanciadas em dez incisos que abrangem quando é realizado com o consentimento, quando é realizado pela administração pública, para execução de contrato, para proteção da incolumidade física do titular, para a tutela da saúde, para a proteção do crédito, dentre outras hipóteses. Frise-se, contudo, que o § 4º versa a dispensa do consentimento quando os dados forem tornados manifestamente públicos pelo titular, resguardando, contudo, os seus direitos e observando os princípios previstos nesta lei. Por sua vez, o art. 8º, *caput*, salienta que o consentimento deve ser dado por escrito ou por algum meio que comprove a efetiva manifestação de vontade do titular do dado, atendendo, assim, a adjetivação concedida pela lei ao consentimento, qual seja: que deve ser livre, informado, inequívoco e ser destinado a uma finalidade determinada.

Em sequência, o art. 9º versa acerca do direito de acesso às informações. Infere-se do *caput* que a informação deve atender aos aspectos qualitativo, quantitativo e formal, para que o consentimento seja dado da forma adequada. Nesse sentido, Bioni (2019, p. 204) explana que o critério qualitativo seria a informação clara e adequada; o critério quantitativo seria a informação concedida de modo suficiente e o critério formal seria a informação dada de maneira ostensiva. O *caput* preceitua todas essas características, de modo que a doutrina apenas as enquadrou em categorias.

O tratamento de dados pessoais sensíveis, a seu turno, recebe regramento específico na seção II, ao passo que também há regramento específico para o tratamento de dados pessoais de crianças e de adolescentes na seção III. Por sua vez, o art. 18 preceitua alguns dos direitos do titular de dados pessoais, como o acesso, a correção, portabilidade, eliminação, revogação de consentimento etc. Neste ponto, destaca-se a ressalva contida no inciso VI desse mesmo artigo, que indica que não haverá eliminação nas hipóteses previstas pelo art. 16, que preceitua, entre outras situações, que está autorizada a conservação para a finalidade de transferência a terceiros, respeitando os requisitos de tratamento de dados da lei. Contudo, ao requisitar que os dados sejam eliminados, desconstitui-se qualquer consentimento que tenha sido dado anteriormente, prevalecendo, tão somente, as hipóteses em que a própria lei autoriza o tratamento dos dados.

Aqui, insta delinear acerca da hipótese do dado já ter sido transferido a terceiros. Neste caso, ao pedir a eliminação dos dados ou revogar o consentimento, isso deve trazer efeitos reflexos aos terceiros também, ensejo no qual devem ser informados por quem proporcionou esse intermédio.

Em sequência, no que tange ao controlador e o operador, o art. 37 informa que eles possuem o dever de manter registro de todas as operações de tratamento de dados pessoais que efetuarem, ao passo que o art. 38 faculta à autoridade nacional a possibilidade de determinar que o controlador realize um relatório de impacto à proteção de dados pessoais, abrangendo os sensíveis, atinente às suas próprias operações de tratamento. Desse modo, a legislação buscou proporcionar uma via efetiva para que a autoridade pública possa acompanhar o tratamento de dados pessoais e os reflexos disso na proteção dos dados pessoais, como mecanismo de impedir ou mitigar possíveis violações. Assim, caso o controlador ou operador causem dano patrimonial, moral, individual ou coletivo em razão de violação à proteção de dados pessoais, responderão solidariamente na obrigação de repará-los, com fulcro no art. 42. No que se refere a essa responsabilização, o art. 43 ressalva que eles não poderão ser responsabilizados quando: a) não realizaram o tratamento dos dados; b) não houver violação à legislação de proteção de dados ou c) o dano verificado for decorrente de culpa exclusiva do titular dos dados ou de terceiros.

O capítulo IX da lei versa acerca da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Esse capítulo, altamente relevante, primeiro foi objeto de veto do ex-presidente Michel Temer, em virtude de vício de iniciativa na proposta, para logo em seguida receber redação através da Medida Provisória nº 869/2018, sendo convertida recentemente na Lei nº 13.853/2019. Assim, a ANPD, conforme

preceitua o art. 55-A, surge como um órgão da administração, integrante da Presidência da República, mas dotada de autonomia técnica e decisória, com fulcro no art. 55-B. Aqui, vale aduzir que a MP editada por Temer apenas concedia autonomia técnica. Como o órgão continuou integrado à Presidência da República, não é crível a autonomia decisória que lhe foi atribuída. Ressalte-se que a lei editada neste ano inovou ao dispor sobre a natureza jurídica transitória da ANPD, visto que "poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República", redação incluída no § 1º do art. 55-A. O §2º, do mesmo artigo, por sua vez, preceitua que esta transformação deverá ocorrer em até dois anos após a entrada em vigor da estrutura regimental da ANPD, sendo que esta estrutura deverá ser disposta pelo próprio Presidente da República, conforme o art. 55-G. Trata-se de flagrante manobra para garantir que a ANPD continue a integrar a Presidência da República por todo o período equivalente ao atual mandato presidencial.

Por conseguinte, no que diz respeito às competências da ANPD, cabe ressaltar que a MP editada por Temer estabeleceu dezesseis, enquanto que a Lei nº 13.853/2019 ampliou para vinte e quatro competências. Elas estão explanadas no art. 55-J, podendo-se citar: o zelo pela proteção dos dados pessoais e pelos segredos comercial e industrial; elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalização e aplicação de sanções; promoção do conhecimento das normas e das políticas públicas de proteção de dados pessoais e privacidade para a população; elaboração de estudos de práticas nacionais e internacionais sobre a matéria; estimular a adoção de padrões para serviços e produtos, visando facilitar o exercício de controle dos dados pelos seus titulares; promover ações de cooperação com autoridades de proteção de dados de outros países; solicitar às entidades do Poder Público as informações sobre a natureza dos dados que possuem e os detalhes do seu tratamento; elaboração de relatórios anuais sobre suas atividades; edição de regulamentos e procedimentos; ouvir agentes de tratamento e a sociedade em matérias de interesse relevante; editar normas, orientações e procedimentos diferenciados para que microempresas, empresas de pequeno porte, *sturtups* e empresas de inovação possam se adequar a esta lei, inclusive estabelecendo prazos diferenciados para elas; comunicar infrações penais às autoridades competentes; implementação de meios para registro de reclamações acerca do tratamento de dados pessoais em desconformidade com a LGPD etc. A Lei nº 13.853/2019 também estabeleceu, no art. 4º, § 3º, que a ANPD emitirá pareceres ou recomendações referentes às exceções de aplicação da lei (no caso de tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança do Estado ou

atividades de investigação e repressão de infrações penais), cabendo à ANPD solicitar aos responsáveis relatórios para averiguar o impacto à proteção de dados pessoais.

Assim, a ANPD possui em suas competências inúmeros dispositivos que frisam o seu viés de estar em contato direto com a sociedade. Ao mesmo tempo, resta nítido que esta Autoridade se configura no principal instrumento para conceder efetividade aos preceitos que a LGPD traz, contudo, manter a ANPD vinculada à Presidência da República mesmo após a entrada em vigor da lei em 2020 fará com que o controle dos dados pessoais dos indivíduos se concentre mais no ocupante da Presidência do que nos titulares em si.

Por outro lado, o art. 58-A dispõe acerca da estrutura do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, configurando-se num Conselho com representação dos mais diversos setores da sociedade, como do Poder Executivo, do Senado Federal, Câmara dos Deputados, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Comitê Gestor de Internet do Brasil, entidades da sociedade civil com atuação específica na área, instituições científicas, tecnológicas e de inovação, bem como entidades representativas do setor empresarial da área de tratamento de dados pessoais. A Lei nº 13.853/2019, acrescentou, ainda, a participação de confederações sindicais e entidades representativas do setor laboral. Quanto às suas competências, o art. 58-B dispõe o seguinte rol: propor estratégias para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, elaborar relatórios, sugerir ações para a ANPD, elaborar estudos, realizar debates e audiências públicas, bem como também disseminar o conhecimento sobre a proteção de dados pessoais à população.

À Autoridade Nacional cabe aplicar sanções administrativas, nos termos dos arts. 52 a 54, sendo elas: advertência, multa, publicização da infração, bem como o bloqueio ou eliminação dos dados pessoais a que se refere à infração. A lei também estipula critérios objetivos e subjetivos para averiguar qual sanção deverá ser aplicada, dentre elas a gravidade da infração, a reincidência, a condição econômica do infrator, a sua boa-fé e adoção de medidas corretivas. Consoante a essas disposições, a lei não estipula valor mínimo ou máximo para a multa. É possível inferir, desse modo, que se busca aplicar uma sanção que seja proporcional ao dano e as circunstâncias fáticas apresentadas. Saliente-se, nesse ponto, que tais sanções não possuem o condão de substituir outras sanções administrativas, civis ou penais, conforme explana o § 2º do art. 52. Os artigos referentes a essas sanções administrativas que serão aplicadas pela ANPD estão alocados num capítulo que versa sobre a fiscalização. A crítica que se aduz aqui é quanto à ordem dos artigos, visto que foi posta de

forma deslocada do capítulo próprio da ANPD, de modo que foi adiantada uma das competências desse órgão antes mesmo de compreendê-lo em si.

A Lei nº 13.853/2019 também estabeleceu, no § 4º do art. 4º, que sob nenhuma hipótese "a totalidade dos dados pessoais de banco de dados de que trata o inciso III do *caput* deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público". Inicialmente, a lei não fazia qualquer ressalva, mas isso já havia sido revogado pela MP editada por Michel Temer. Assim, a lei editada em 2019 apenas ratificou essa postura mais abrangente, ampliando sobremaneira a quantidade de pessoas que poderão tratar, isto é, colher, acessar, distribuir, armazenar, eliminar, modificar, dentre outros, os dados pessoais contidos nos bancos de dados destinados à segurança pública, defesa nacional, investigação de infrações penais etc. Tal abrangência não parece adequada, visto que a importância desses bancos de dados é tão expressiva a ponto de que deveria ser restrita ao menor número possível de pessoas, de forma que a redação concedida a esse parágrafo parece atrair mais malefícios do que benefícios.

Nesse contexto, o art. 26, § 1º, estipula as exceções nas quais o Poder Público pode transferir os dados pessoais de suas bases de dados às entidades privadas, sendo que a referida lei editada em 2019 foi responsável por adicionar duas novas possibilidades. Ressalte-se que, neste artigo, não há qualquer ressalvada acerca das entidades privadas, de modo que se enquadram também as que não foram integralmente constituídas por capital do Poder Público.

Assim, através de uma análise sistemática, infere-se que a LGPD se configura numa lei madura, que enfatiza em inúmeros dispositivos a importância da disseminação de conhecimento, para que a sociedade compreenda as normas e as formas de proteção dos dados pessoais, além de estabelecer um órgão de fiscalização e sancionador. A LGPD também se destaca no que tange ao consentimento, colocado como elemento norteador de todo o aparato normativo fixado na lei, tendo recebido especial atenção à sua adjetivação, pois tem que ser livre, informado, inequívoco e destinado a uma finalidade determinada; poucas foram as ressalvas elaboradas quanto possibilidade de tratamento de dados sem esse elemento.

Considerando esse ponto, resta explícita a influência do modelo da União Europeia na legislação brasileira, bem como é facilmente notável que o titular dos dados pessoais ainda é visto como protagonista do processo de tratamento, tendo em vista que a autodeterminação informacional e o consentimento são figuras centrais. Isso se configura enquanto resquício de uma política regulatória que acredita que o indivíduo é capaz de realizar apenas condutas que protejam as suas informações. Nessa perspectiva, Bioni (2019, p. 137) aduz que se consolidou "a crença reducionista de que autodeterminação informacional corresponderia ao elemento

volitivo – autonomia da vontade – do titular do dado. Com ela, o consentimento atingiu um *status* canônico" e, por consequência, isso gerou reflexos nas leis de proteção de dados pessoais. Assim, esse entendimento reducionista da autodeterminação informacional atribui ao indivíduo a responsabilidade do controle dos seus próprios dados. Contudo, Bioni (2019, p. 137) também leciona que esse tipo de regulamentação, que surgiu nos anos 1980, "não mais se ajusta ao contexto subjacente dos dados pessoais como ativo econômico em constante circulação". Seria necessária, portanto, uma política de regulamentação que não só prestigiasse a autonomia do indivíduo e a sua capacidade de consentimento, mas que também não atribua tão somente a ele essa responsabilidade. Nesse contexto, a LGPD também atende a esse pressuposto através da criação da ANPD, de modo que a coloca em maior conformidade aos tempos atuais. Deve-se, por conseguinte, proporcionar a esta Autoridade o máximo de subsídio estrutural, orçamentário e legal para que haja a plena efetivação das suas competências, conforme as críticas já apontadas neste estudo.

Assim, em que pese a utópica e sedutora visão de que o consentimento dos indivíduos seria suficiente para garantir a tutela dos seus dados pessoais, faz-se pertinente aludir a uma discussão antiga de que nem sempre as pessoas decidem o que é melhor para elas, sendo a prática de fumar um exemplo clássico. No presente contexto, há o agravante que boa parte da população, embora utilizem a internet todos os dias, ainda assim desconhecem ou não compreendem algumas de suas minúcias, como a utilização de *cookies*, que consiste numa ferramenta amplamente utilizada pelos mais diversos sítios eletrônicos e que armazenam alguns dados, como o *login*, além das preferências dos usuários. Concomitantemente, a utilização indevida de dados pessoais pode se tornar um problema não só pessoal, mas potencialmente pública, como foi no caso da Cambridge Analytica-Facebook. Nesse diapasão, Bioni (2019, p. 98) leciona que "a dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade". É indubitável, portanto, o caráter social inerente à proteção de dados pessoais e que tal tutela também beneficia a coletividade, razão pela qual resta justificado o interesse estatal em implementar práticas de fiscalização, não apenas de difusão de conhecimento acerca do que se está consentindo, mas a atuação por entes estatais não pode ser tanta a ponto de substituir integralmente o controle por parte dos indivíduos. Desse modo, a proteção de dados pessoais se destaca como um novo direito da personalidade e, através da PEC 17/2019[13], será consubstanciado na CRFB/88 como um direito fundamental, corroborando a sua importância.

[13] Esta Proposta de Emenda à Constituição foi aprovada no Senado no dia 17/07/2019 e, atualmente, aguarda apreciação pela Câmara dos Deputados.

3 A UTILIZAÇÃO DA INTERNET DAS COISAS PARA DISSEMINAÇÃO DA SOCIEDADE DE VIGILÂNCIA

O avanço tecnológico propiciou a monetização de dados pessoais no âmbito da sociedade da informação. Por conseguinte, o setor privado adotou a estratégia de pretender coletar a maior quantidade de dados possível daqueles que confiam nos seus produtos e/ou serviços, propiciando a consolidação da sociedade de vigilância. Assim, houve múltiplas modificações no âmbito tecnológico para atender a essa pretensão, sendo uma delas o advento do *Big Data*, tecnologia que permite a acumulação de dados, cruzando-os para definir padrões. De forma concomitante, houve a ascensão de dispositivos relacionados à Internet das Coisas, disseminando a sociedade de vigilância, cuja expressiva rentabilidade impulsiona a indústria a criar produtos que, por vezes, não observam preceitos básicos da proteção dos dados pessoais. Nessa toada, serão narradas no presente capítulo algumas considerações no que tange à sociedade da informação e da vigilância, à Internet das Coisas e alguns dos principais desafios à implementação da segurança cibernética. No ensejo, também serão expostas algumas das soluções relacionadas.

3.1 Sociedade da informação e da vigilância

O caráter mutável da sociedade sempre foi norteado por um elemento posto em destaque, de modo que já houve a sociedade agrícola, em seguida veio a sociedade industrial, com a criação das máquinas a vapor e eletricidade, posteriormente veio a sociedade pós-industrial, que dava maior enfoque nos serviços e não nos produtos e, atualmente, é verificada a existência da chamada sociedade da informação, conforme sintetiza Bioni (2019, p. 3-4). Nesse sentido, o desenvolvimento da economia atual está pautado no fluxo informacional, que encontra valioso impulso na ampla presença tecnológica, visto que todas as ações individuais e coletivas são registradas em dispositivos geridos mesmo nos locais mais remotos e faz com que a sociedade se organize de acordo com as fartas informações recebidas incessantemente.

De forma concomitante, a sociedade da informação criou espaço propício para a monetização dos dados pessoais como modo um dos principais modos de arrecadação de recursos financeiros. Assim, as empresas do ramo da tecnologia passaram a aplicar cada vez mais mecanismos de captar informações pessoais, justificando que, dessa forma, conseguem oferecer melhor uso de seus produtos, visto que torna a experiência personalizada. Nesse

sentido, criou-se um verdadeiro sistema de vigilância de todas as atividades dos usuários, porque ainda que a pessoa utilize redes sociais aplicando o mecanismo de compartilhar suas informações apenas para os amigos/seguidores, antes de ser compartilhado com eles, é preciso lembrar que é compartilhado com a empresa diretamente responsável e também por outras empresas que são consideradas “parceiras”, sem, contudo, haver informação detalhada sobre quais são, conforme será discorrido adiante. Do mesmo modo acontece quando é selecionada a opção para que certas informações - como data de nascimento e gênero - só estejam disponíveis para você. São meras opções ilusórias, visto que não só os dados serão compartilhados com outras pessoas indesejadas, como também esses mesmos dados serão tratados para que seja veiculada publicidade específica de acordo com eles.

Como consequência, a arrecadação de recursos financeiros com os dados vertidos nos dispositivos tecnológicos criou um ambiente propício para a consolidação da sociedade da vigilância. Nesse sentido, frise-se que não houve a superação da sociedade da informação, apenas foi instaurado um paralelismo. De fato, faz-se necessário contextualizar que, após os ataques que ocorreram em 11 de setembro de 2001, os Estados soberanos passaram a naturalizar cada vez mais o uso de dispositivos de vigilância, sob o pretexto de que isso forneceria maiores informações aos entes estatais e, assim sendo, potencializaria a segurança pública e defesa nacional. Ante a esse processo de naturalização, a própria população mundial paulatinamente foi inserindo dispositivos de vigilância nas suas casas, também sob a finalidade de prover a segurança individual. É um fenômeno difícil de conter e que, inegavelmente, oferece inúmeros benefícios, mas que também pode ter efeito diametralmente oposto ao pretendido, conforme será pormenorizado.

Ainda nesse sentido, é preciso reconhecer que a sociedade de vigilância, como ocorre hoje, é facilmente inserida na discussão acerca de uma configuração do panóptico mais sofisticada do que a que Jeremy Bentham concebeu inicialmente, bem como se trata de uma derivação da sociedade disciplinar que Michel Foucault brilhantemente ilustrou no livro “Vigiar e Punir”.

Todavia, malgrado a vigilância por parte do Estado ser comparável à que está presente na obra literária “1984”, por vezes condensado na famosa frase “O grande irmão está de olho em você” (ORWELL, 2009, p. 12), a vigilância atualmente não só é perpetrada por agências de inteligência governamentais e entes públicos relacionados, como também pela iniciativa privada. Nessa perspectiva, Julian Assange (2012), fundador do WikiLeaks, explanou que

> Até a fronteira entre o setor público e o privado deixou de ser tão clara. Se olharmos a expansão do setor de terceirizados para as Forças Armadas do Ocidente ao longo dos últimos dez anos, a NSA, que foi a maior agência de espionagem do mundo, tinha em seus livros contábeis dez terceirizados principais com os quais trabalhava. Dois anos atrás, esse número tinha subido para mil. Então a fronteira entre o setor público e o privado de fato está cada vez mais nebulosa.

Dessa forma, com a monetização dos dados da população, instaurou-se um ambiente propício para a consolidação da sociedade de vigilância. No Brasil, isso continuará a ser promovido em decorrência da redação concedida à LGPD pela Lei nº 13.853/2019, visto que as pessoas jurídicas de direito privado poderão tratar dados pessoais contidos nos bancos de dados destinados à segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, conforme já explicado anteriormente.

Como consequência da sociedade de vigilância, foram criados modos mais rebuscados para fins de tratamento de dados pessoais, de modo que se conseguiu aliar características de certos dispositivos, como a utilidade, a presença em ambientes íntimos e a sutileza como meios potencializadores para a coleta de dados. Assim, cresce o número de residências e ambientes de trabalho com dispositivos conectados à *Wi-Fi*, como lâmpadas, babás eletrônicas, brinquedos, televisões etc.

3.2 Internet das Coisas (IoT)

Para os fins do presente estudo é dispensável pormenorizar conceito, histórico e formas de utilização da internet. Contudo, é propício aduzir breve relato sobre qual a fase da *web* atual, de modo a melhorar a compreensão sobre o desenvolvimento da Internet das Coisas ou *Internet of Things*.

A *web* nada mais é do que um navegador, sendo o mais comumente utilizado. Nesse sentido, os doutrinadores costumam dividir o desenvolvimento da *web* em três fases: *Web* 1.0, 2.0 e 3.0. Através dessa perspectiva, Magrani (2018, p. 64-66) explica que na *web* 1.0 não havia interação entre os consumidores e os produtores, sendo que os primeiros *e-commerces* disponibilizavam tão somente seus catálogos. Por conseguinte, houve uma transição sutil para o que veio a ser chamado de *web* 2.0, fase essencialmente marcada pela comunicação entre os usuários, propiciando, assim, que eles não apenas conseguissem ter acesso aos conteúdos, como também produzi-los. Por fim, “a web 3.0 usará a internet para cruzar dados. Essas informações poderão ser lidas pelos dispositivos, e estes conseguirão fornecer informações mais precisas” (MAGRANI, 2018, p. 68). Nesse contexto, a Internet das Coisas estaria

inserida na *web* 3.0, permitindo não apenas a comunicação entre as pessoas, como também entre as máquinas e potencializando o trabalho de cruzamento de dados. Mas o que vem a ser, exatamente, a chamada Internet das Coisas?

Para fins de melhor compreensão, convém expor um exemplo concreto: em 2015, a Samsung anunciou que as suas televisões inteligentes podiam gravar conversas e transmiti-las a terceiros e, assim, as pessoas deveriam estar cientes que seus dados pessoais e informações sensíveis poderiam ser compartilhados por esta via [14]. Foi constatada essa mesma possibilidade em televisões de outras empresas; isso faz com que milhares de pessoas que têm esse tipo de produto nas suas salas e quartos tenham que se preocupar com o que falam mesmo nos locais mais íntimos. Tal possibilidade teve a sua gravidade relativizada em virtude de que é possível que o usuário desative o comando por voz e, assim, em teoria, não seria mais gravado, ignorando o fato de que todo e qualquer dispositivo conectado a internet está sujeito à atuação de *hackers* ou *crackers*[15]. Esse caso guarda semelhança com a teletela que George Orwell[16] (2009, p. 13) descreveu em seu romance intitulado 1984: "a teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela".

Dessa forma, o caso da televisão inteligente ilustra bem o que vem a ser a Internet das Coisas. Em palavras simplificadas, consiste em implantar o recurso da internet nos objetos, ainda que eles sejam os objetos mais banais do cotidiano e mesmo que o retorno utilitário não seja tão significativo assim. Inclusive, essa é uma das razões para o crescimento do *e-waste*, visto que o baixo retorno utilitário que alguns dispositivos possuem, aliado à sua rápida superação por outros dispositivos com tecnologia mais avançada, acabam por contribuir com a quantidade de equipamentos eletrônicos jogados no lixo de maneira inadequada, provocando a contaminação do solo, água e ar, gerando um problema de saúde pública.

De fato, a disseminação desses dispositivos fez com que desde 2017 o número de objetos com acesso a internet fosse maior que a quantidade de pessoas no mundo, de acordo com a Gartner, empresa de análises, ao passo que o impacto econômico cresce proporcionalmente[17]. Em virtude disso, passou-se a criar uma mega estrutura conectada à

---

[14] Disponível em: https://oglobo.globo.com/economia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181. Acesso em: 15 jul. 2019.

[15] O termo *cracker* se diferencia de *hacker* na medida em que o primeiro se refere aos que utilizam o seu conhecimento técnico avançado para quebrar sistema de segurança para fins ilícitos, enquanto que os *hackers* também invadem sistemas, mas com o intuito de melhorá-los, não de causar danos. (SATINO, 2013). Registre-se que essa distinção não é unânime entre os estudiosos do tema, contudo, será adotada no presente trabalho.

[16] Pseudônimo de Eric Arthur Blair.

[17] Disponível em: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/. Acesso em: 10 jul. 2019.

internet, tornando inúmeros serviços e produtos interconectados. Assim, Magrani (2018, p. 15) explica que a internet das coisas é mais do que um objeto conectado, pois consiste na "progressiva automatização de setores inteiros da economia e da vida social com base na comunicação máquina-máquina: logística, agricultura, transporte de pessoas, saúde, produção industrial e muitos outros". Desse modo, ao mesmo tempo em que propiciam a facilitação das situações do cotidiano, esses dispositivos que interagem uns com os outros potencializam a quantidade de dados tratados, isto é, que são colhidos, armazenados, transferidos etc.

Simultaneamente, esses tipos de dispositivos propiciam que a relação entre o fabricante do produto e o consumidor não se restrinja apenas no ato de adquirir o bem, pois a relação acaba se perpetuando em virtude de que os dados fornecidos para os dispositivos são analisados para que sejam criados novos modelos de negócios ou novos dispositivos a partir do comportamento do consumidor. É considerando esse aspecto que Magrani (2018, p. 167, grifo do autor) argumenta que, no âmbito da IoT, o produto e serviço são elementos indissociáveis, tendo em vista que "a própria noção de uma *coisa*, no sentido dessa proposta, envolve um *nível de serviço* embutido na mesma e outros, ao redor dela, para fazê-la funcionar *em rede e em conjunto* com outras coisas, pessoas, organizações e sistemas", concluindo que há de ser submetida a novos estudos a questão de produto e serviço serem vistos de forma separada.

Logo, constata-se que a IoT não se restringe apenas a objetos individualizados, isto porque a tendência é a extensão desse tipo de tecnologia para formar uma mega estrutura conectada a internet e contribuindo para o advento das *smart cities* (cidades inteligentes), que alia a aplicação da tecnologia na mobilidade urbana, saúde pública, educação, recursos naturais, iluminação pública, segurança etc. Assim, a IoT passa a ser um elemento importante da gestão pública, transpondo os benefícios individuais e se relacionando diretamente com a economia global, diminuindo os custos de diversos serviços e controlando o impacto humano nos recursos naturais. Nesse contexto, pode-se citar a título exemplificativo da IoT aplicada no âmbito das cidades o caso de sensores acoplados nos edifícios que estão em locais propensos a terremotos, aptos a enviar dados em tempo real acerca da estrutura do prédio, além de também serem aplicadas em pontes e outras obras edilícias, sob a finalidade de indicar o momento adequado de manutenção, evitando acidentes.

É nesse cenário de riqueza de fornecimento e tratamento de dados que se torna propício discorrer acerca do *Big Data*, que consiste numa tecnologia inserida no contexto de quantidade e qualidade da gestão de informação. Partindo desse pressuposto, Bioni (2019, p. 39) leciona que "essa tecnologia permite que um volume descomunal de dados seja

estruturado e analisado para uma gama indeterminada de finalidades". Ainda, Doug Laney (2012, *apud* BIONI, 2019, p. 39) associa o *Big Data* em três "V": volume, velocidade e variedade, sendo "volume e variedade, porque ele excede a capacidade das tecnologias 'tradicionais' de processamento, conseguindo organizar quantidades antes inimagináveis [...] e, tudo isso, em alta velocidade".

Nessa conjuntura, depreende-se que *Big Data* é uma tecnologia que aglomera uma expressiva quantidade de dados e que pode gerar informações precisas a partir da análise dos dados, pois são estabelecidos padrões. Ou seja, não se trata apenas de uma análise retrógrada, mas também é capaz de verificar as "*probabilidades* de acontecimentos futuros" (BIONI, 2019, p. 41, grifo do autor). Insta salientar, contudo, que esse não é um sistema que aplica conceitos valorativos, equiparados aos de seres humanos. Pelo contrário, demonstram apenas alta eficiência em traçar padrões, de modo que detectam as chances dos acontecimentos se repetirem.

Depreende-se, assim, que a disseminação da sociedade de vigilância através da IoT causa forte impacto econômico, sendo que a consultoria McKinsey Digital estima que em 2025 esse impacto gerará receita entre 4 trilhões e 11 trilhões[18]. Reconhecendo esse mercado em ascensão e a necessidade de estimular as pesquisas nesse âmbito, bem como de implantar políticas de padronização e criar um ecossistema de IoT dinâmico na Europa, em 2015 a Comissão Europeia criou a *Alliance for Internet of Things Innovation* (AIoTI), que estabelece diálogos diretos com várias das principais empresas do ramo de tecnologia, bem como algumas universidades e institutos, sendo todos integrados como membros.

Por outro lado, o impacto econômico da IoT no Brasil também é significativo. Em decorrência disso, no final de 2017 foi apresentado o Plano Nacional de Internet das Coisas, que consistiu num estudo financiado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações e pelo Banco Nacional de Desenvolvimento Econômico e Social. Foi produzida uma série de relatórios e *workshops*, tendo sido pesquisadas as iniciativas que poderiam contribuir para o desenvolvimento da IoT. Inicialmente, foram calculadas 200 iniciativas, que posteriormente foram condensadas em 75 e publicaram um relatório final abrangendo diversas questões relacionadas à IoT, contabilizando 65 páginas.

Contudo, apenas em 25 de junho de 2019 o Presidente da República, por meio do Decreto nº 9.854, instituiu o Plano Nacional de Internet das Coisas (PNIC) e dispôs acerca da Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação

[18] Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/noticias/noticia/internet-coisas-iot. Acesso em: 12 jul. 2019.

Máquina a Máquina e Internet das Coisas. Nesse ponto, cabe chamar atenção para a exígua quantidade de dispositivos que o Decreto contempla: apenas dez, mesmo após o financiamento de um amplo estudo sobre a IoT poucos anos antes; quanto a isso, de fato o Decreto positivou de maneira geral - e precária - alguns dos elementos presentes no relatório final, de modo que o estudo não foi ignorado em sua totalidade.

Considerando o tamanho diminuto do Decreto, cria-se a expectativa de que se buscou dar uma redação mais sucinta, clara e de fácil assimilação à população em geral. Entretanto, tal expectativa é frustrada a partir da leitura do art. 2º, que traz o conceito de IoT, coisas, dispositivos e serviço de valor adicionado. Ora, é patente que os artigos que trazem conceitos possuem função não apenas para conferir maior segurança jurídica, visto que se estabelece por meio de norma os conceitos pretendidos, mas também assumem papel fundamental para tornar inteligíveis as demais normas; assim, uma redação emaranhada prejudica todo o conjunto normativo e vai contra o interesse público, principalmente quando se trata de recursos tecnológicos que, não obstante sejam amplamente utilizados, são pouco compreendidos no que tange principalmente à segurança que oferecem. Assim, cabe aduzir os conceitos trazidos pelo Decreto nº 9.854/2019:

> Art. 2º Para fins do disposto neste Decreto, considera-se:
> I - Internet das Coisas - IoT - a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade;
> II - coisas - objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação;
> III - dispositivos - equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados; e
> IV - serviço de valor adicionado - atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações, nos termos do disposto no art. 61 da Lei nº 9.472, de 16 de julho de 1997.

Resta nítido que o elemento protagonista do Decreto - a Internet das Coisas - teve a redação mais emaranhada de todas, de modo que foi preciso trazer a conceituação de trecho do próprio conceito em seguida: a questão do serviço de valor adicionado. Por outro lado, revela-se positiva a intenção de aliar o conceito da Internet das Coisas à prestação de serviços, visto que, de fato, apesar de ser uma infraestrutura intimamente ligada a objetos/produtos, igualmente está relacionada à prestação de serviços. Nesse ponto, cumpre salientar que o

Decreto, ao definir “serviço de valor adicionado”, na verdade se utiliza do mesmo conceito exposto na Lei nº 9.472/1997.

Sequencialmente, o art. 3º apresenta os objetivos do PNIC. Em síntese, são: a) melhora na qualidade de vida e eficiência nos serviços; b) aumento da produtividade e estímulo da competitividade das empresas brasileiras pertencentes a este ramo da tecnologia; c) parceria com setor público e privado; d) aumento da integração do país no âmbito internacional, através da participação em fóruns, pesquisa, desenvolvimento e internacionalização das soluções de IoT. Em consonância com o que foi elaborado no estudo anterior, os ambientes que serão priorizados para a aplicação de soluções de IoT são: a saúde, cidades, indústrias e o âmbito rural. Para que eles sejam priorizados e como meio de efetivar o PNIC, será realizado um plano de ação com temas pré-estabelecidos, como a ciência, inserção internacional, educação, infraestrutura, regulação, segurança, privacidade e a viabilidade econômica, com fulcro no art. 5º do mesmo Decreto, e cujas ações devem estar em conformidade com a Estratégia Brasileira para a Transformação Digital, presente no Decreto nº 9.319/2018.

Ainda, o art. 6º instituiu três projetos para viabilizar a implementação do PNIC: Plataforma de Inovação em IoT, Centros de Competência para Tecnologias Habilitadoras em IoT e um Observatório Nacional para o Acompanhamento da Transformação Digital.

Por fim, o Decreto nº 9.854/2019 também dispôs acerca da Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas, chamada sucintamente de Câmara IoT, que se configura enquanto um órgão de assessoria para acompanhar a implantação do PNIC. Seu quadro possui apenas cinco Ministérios, ou seja, não foi dada participação à iniciativa privada e tampouco a representantes da sociedade civil. Cumpre ressaltar que a criação dessa Câmara foi prevista desde 2014, por meio do Decreto nº 8.234.

Ante o exposto, pode-se concluir que a Internet das Coisas consegue propiciar inúmeras facilidades no cotidiano, porque dá ferramentas de controle para gestão da vida privada, bem como pode auxiliar em diversos interesses da coletividade. No entanto, ainda são dispositivos que em sua maioria não propiciam a segurança dos dados e oferece risco à privacidade. Dessa forma, o ecossistema de IoT a ser criado no país ainda deve passar por etapas de padronização e ser adequado à política de proteção de dados que deve ser observada no âmbito nacional, de modo que, ao mesmo tempo em que ofereça oportunidades de crescimento para as empresas que fornecem cumulativamente produtos e serviços associados à IoT, também possam oferecer segurança à população e maximizar os impactos positivos no cenário da economia nacional.

3.3 Desafios na promoção da segurança cibernética

Próximo ao natal de 2015, a Matell, em parceria com a Toytalk, anunciou um novo brinquedo: uma boneca apta a dialogar de acordo com o que o seu interlocutor está falando e, além disso, "aprender" com essas conversas, visto que é conectada à internet e a uma nuvem que armazena as informações recebidas[19]. Considerando isso, desde o anúncio houve várias críticas no sentido de que o brinquedo seria um invasor de privacidade, além de ser apontada a lógica de que a criança nutre uma visão ingênua de que está conversando tão somente com uma boneca, quando na verdade está fornecendo informações sobre os seus interesses e sobre sua família para a fabricante do brinquedo e os seus parceiros econômicos.

Assim, o sítio eletrônico *Campaign for a Commercial-Free Childhood*[20] fez uma análise sintética dos motivos para que os pais não adquirissem a boneca, tais como: as conversas privadas das crianças não deveriam ser compartilhadas com estranhos e empresas; a criatividade seria mitigada, visto que a mente da criança é mais estimulada quando ela cria os próprios diálogos entre os brinquedos; crescer acostumado a ter sempre um dispositivo a ouvindo naturaliza a invasão da privacidade; os pais também não deveriam se utilizar desses artifícios para invadir a privacidade dos seus filhos, ouvindo as conversas que a criança acredita estar sendo compartilhada tão apenas com uma boneca; há a possibilidade de terceiros terem acesso ao banco de dados da empresa ou controlar o que a boneca fala, visto que está conectada à internet[21]. Outros brinquedos, como o *My Friend Cayla*, sequer permitia que a conexão através de *bluetooth* fosse desativada ou protegida por senha, o que fez a Agência Federal de Redes da Alemanha proibir a sua comercialização naquele país[22].

Nota-se, assim, que a principal problemática relacionada à Internet das Coisas é algo intrínseco a elas: a própria conexão com a internet, que deixa qualquer dispositivo sujeito à atuação de *crackers* e/ou *hackers*; nesse ponto, frise-se que basta um aplicativo/dispositivo com segurança deficitária para comprometer a proteção de dados de todos os outros, considerando a interconexão. Uma fabricante chinesa de brinquedos, VTech, chegou a ter seu banco de dados invadido e as informações de 5 milhões de pessoas, incluindo crianças, foram expostas. A situação foi agravada porque, segundo a *U.S. Food & Drug Administration*

[19] Disponível em: https://economia.uol.com.br/noticias/bloomberg/2015/03/25/criticos-da-hello-barbie-usam-boneca-da-mattel-para-travar-luta-pela-privacidade.htm. Acesso em: 15 jul. 2019.
[20] Campanha por uma Infância Livre de Comerciais (tradução nossa).
[21] Disponível em: https://commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf. Acesso em: 15 jul. 2019.
[22] Disponível em: https://exame.abril.com.br/tecnologia/alemanha-proibe-comercializacao-de-boneca-por-risco-de-espionagem/. Acesso em: 15 jul. 2019.

(FDA), dos Estados Unidos, a empresa mentiu em sua política de privacidade ao informar que os dados dos usuários eram criptografados[23]. Dessa forma, mesmo que os pais fossem cuidadosos quanto às informações dos filhos e observassem se a empresa utiliza a criptografia, ainda assim obteriam o mesmo resultado. As babás eletrônicas, por sua vez, cada vez mais tecnológicas e com recurso de câmera e movimento, apresentam os mesmos problemas quanto aos *crackers*.

Note-se que tais exemplos são de dispositivos voltados para crianças, mas com potencial para atingir toda a família, mesmo que, em teoria, deveria haver um cuidado maior com os dados das crianças e adolescentes.

A ameaça de invasão aos dispositivos relacionados à IoT se torna mais palpável quando se trata de objetos associados diretamente à vida das pessoas. Por mais ficcional que aparente ser, é facilmente possível vislumbrar os efeitos concretos dessa vulnerabilidade, e isso fez com que a FDA emitisse alerta em 2017 para a atualização do *software* de 465 mil marca-passos[24], visto que os transmissores não estavam com o sistema de segurança adequado para impedir – ou dificultar – que invadissem o dispositivo e alterassem os batimentos cardíacos dos usuários. No âmbito da saúde, também é propício registrar que há outras abordagens de invasão bem menos diretas, mas que podem ter consequência igualmente grave, como o caso de conseguir invadir os dispositivos que mostram os batimentos cardíacos dos pacientes em hospitais que utilizem dispositivos associados à IoT. Nesse cenário, alterar o resultado de uma máquina para, por exemplo, simular uma parada cardíaca, fará com que os médicos tomem decisões com base no resultado mostrado pelo dispositivo eletrônico e, ao tentarem salvar um paciente estabilizado, podem provocar a sua morte. Assim, para que se goze da integralidade dos benefícios desses dispositivos é necessária a implementação de uma estrutura de segurança eficiente.

A falibilidade da anonimização é outro problema relacionado à segurança cibernética visto que, por vezes, as pessoas fornecem dados acreditando que estão sendo tratados de forma anônima, mas esse estado pode ser reformado para que se promova a identificação, conforme já foi explanado anteriormente.

Há outros elementos que acarretam na insegurança cibernética, como a ausência de conhecimento técnico suficiente para entender a estrutura virtual com a qual se está interagindo, não havendo compreensão acerca de como é realizada a coleta dos dados e sequer

---

[23] Disponível em: https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated. Acesso em: 15 jul. 2019.

[24] Disponível em: https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals. Acesso em: 15 jul. 2019.

os prejuízos que isso pode causar[25]. A situação se agrava porque, ainda que as pessoas saibam que seus dados estão sendo coletados, muitas não veem como isso lhes causa prejuízo significativo.

Quanto à ausência de conhecimento técnico, destaca-se que mesmo que os usuários saibam que um aplicativo criptografado é mais vantajoso do que um que não conte com esse sistema de segurança, ainda assim as pessoas não entendem como a criptografia efetivamente funciona. Dessa forma, acredita-se na boa-fé das empresas quando estas afirmam que empregam a criptografia nos produtos que oferecem. Todavia, muitas se escondem sob o manto da complexidade que envolve essa tecnologia e, apesar de indicarem que aplicam a criptografia, isso não corresponde à realidade, como já aconteceu com a empresa chinesa Vtech.

Outro problema que pode ser elencado é o excesso de informação que desinforma, visto que a perda da objetividade e prolixidade numa sociedade movida pelo imediatismo é a receita perfeita para ser ignorado. Dessa forma, o consentimento, na maioria das vezes, é dado de maneira precipitada, visto que as pessoas não leem efetivamente as políticas de privacidade. Além disso, ao serem indagadas se aceitam a instalação de *cookies*, sequer sabem o que isso significa. Foi em decorrência disso que a imposição de que o titular dos dados deve conceder anuência prévia sobre a coleta dos seus dados "teve um efeito adverso (in)esperado. Na medida em que se exigia o consentimento prévio e expresso, os usuários foram 'bombardeados' com uma avalanche de avisos sobre a instalação de *cookies*" (BIONI, 2019, p. 178), de modo que fez com que as pessoas aceitassem independentemente de compreender o que estavam consentindo.

Por fim, outro ponto que pode ser suscitado no que tange aos desafios da segurança cibernética é o próprio *e-waste*, considerando que o descarte inapropriado de certos dispositivos eletrônicos, como o celular, pode fornecer inúmeras informações pessoais a terceiros; a mesma ameaça está presente quando ocorre a venda/doação desses dispositivos. A título exemplificativo, pode-se citar os casos de celulares formatados, nos quais muitas pessoas confiam que, após submeter tais objetos a esse procedimento, torna-se impossível recuperar os arquivos. Contudo, há aplicativos que restauram todo o conteúdo que já passou por ali, e estes aplicativos estão disponíveis para serem baixados com a mesma facilidade e nos mesmos locais onde se baixam os aplicativos mais comumente utilizados.

[25] Nesse ponto, frise-se que "ao consumidor é impossível alcançar o mesmo patamar informativo do fornecedor. Até porque, para ele, é desnecessário saber todas as minúcias da atividade de tratamento de dados pessoais" (BIONI, 2019, p. 192). Desse modo, o que se revela necessário é que o consumidor seja suficientemente informado sobre os impactos negativos que a estrutura virtual pode engendrar.

Não obstante a dificuldade da proteção dos dados pessoais e a possibilidade das barreiras de segurança cibernética serem ultrapassadas, ainda assim uma das soluções para a proteção dos dados é a aplicação de estratégias técnicas avançadas de criptografia. No entanto, há também soluções alternativas. Nesse sentido, Jérémie Zimmermann, um engenheiro de computação e aliado de Julian Assange, defende que todos possam utilizar um *software* livre (ASSANGE, 2013):

> Precisamos de um software livre que todo mundo possa entender, que todo mundo possa modificar e que todo mundo possa examinar para verificar o que ele está fazendo. Acho que o software livre constitui uma das bases para uma sociedade on-line livre, para termos o potencial de sempre controlar a máquina, não permitindo que ela nos controle. Precisamos de uma criptografia robusta para nos certificar de que ninguém mais possa ter acesso a dados que desejamos manter privados.

Software livre, por sua vez, consiste num programa apto a ser modificado pelo próprio usuário para atender as suas necessidades. Para fazer um contraponto, os *softwares* mais utilizados são os chamados *softwares* proprietários, mais restritos, como o Windows e o Pacote Office. Dessa forma, o *software* livre consagra a liberdade dos usuários, permitindo que eles próprios moldem o programa para adaptá-lo e executá-lo de acordo com o que deseja, podendo também distribuir cópias em benefício da comunidade virtual. Já Assange (2013) acredita que a "única defesa eficaz contra a iminente distopia da vigilância é aquela em que cada um toma medidas para proteger a própria privacidade, porque os grupos capazes de interceptar tudo não têm incentivo algum para reduzir o próprio controle".

Nesse contexto, há a criação das *Privacy Enhancing Technologies* (PET), que consiste em tecnologias que criam aparato para a proteção da privacidade e dos dados pessoais. A criptografia, anonimização e utilização da navegação anônima são formas de se proteger. Os estudiosos das PETs se orientam pelo princípio da minimização da quantidade de processamento de dados, para que as empresas coletem e façam os demais tratamentos apenas do que for estritamente necessário, bem como analisam quais são as formas mais eficientes de se proteger os dados. O problema, contudo, é a efetiva aplicação dessas pesquisas, visto que as PETs encontram dificuldade de serem implementadas no mercado, em decorrência do baixo incentivo econômico e regulatório, conforme consta no Relatório elaborado em 2017 pela Divisão de Análise Tecnológica do Gabinete do Comissário de Privacidade do Canadá[26].

[26] Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. Acesso em: 19 jul. 2019.

No contexto das PETs, pode-se citar como exemplo a que foi denominada *Do Not Track*[27] (DNT), cujo intuito é criar um cadastro dos usuários que já têm escolhas pré-estabelecidas sobre o que os sítios eletrônicos podem fazer com seus dados, de modo que, como explica Bioni (2019, p. 180), bastaria selecionar o DNT no navegador para que os sites fossem informados se o indivíduo concorda ou não com a coleta dos seus dados, sem lidar com as janelas individuais que pedem a solicitação para o tratamento, e tampouco precisar desativar os *trackers*, que requer um conhecimento maior. Sequencialmente o autor explana que "de um lado, o consumidor não necessitaria ser um *expert* para deletar os vários *trackers*, a fim de vencer a corrida armamentista tecnológica de um rastreamento persistente. De outro lado, a sua experiência de navegação não seria prejudicada". Contudo, ainda conforme Bioni (2019, p. 181), o DNT jamais foi implementado, visto que não se chegou a um consenso sobre quem seria o verdadeiro responsável por isso – se a *World Wide Web Consortium* ou o setor empresarial – e tampouco sobre a sua abrangência, visto que para o setor empresarial essa estratégia serviria tão somente para os dados dos indivíduos não fossem utilizados para fins de publicidade comportamental, razão pela qual o setor industrial que explora esse tipo de publicidade se posicionou veementemente contra o DNT.

Considerando o que foi exposto, a dificuldade de implementação de PETs eficazes apenas demonstra o fracasso da presunção de que o mercado seria responsável por se autorregular, "mostrando-se que a mão invisível do mercado foi, de fato, invisível para que a tecnologia se mostrasse, ambivalentemente, como um instrumento para a proteção dos dados pessoais e não só para a sua exploração" (BIONI, 2019, p. 205).

Dessa forma, uma das soluções mais importantes para melhorar a segurança cibernética ainda é a adoção de medidas de controle do fornecimento de dados por parte dos usuários, para que se colete o menor número de dados possível, bem como que o procedimento se dê com a transparência necessária, de forma que a população saiba não apenas qual a empresa que recebe diretamente seus dados, mas também saiba quais são os seus parceiros comerciais que igualmente realizam o tratamento dessas informações.

Nesse contexto, o que se denota do cenário atual é uma falta de cuidado sobre quais empresas terão acesso aos dados. Não se pode falar em despreocupação, visto que a população mundial ficou em choque quando o escândalo da Cambridge Analytica-Facebook recebeu destaque na mídia, todavia, ainda assim não se vislumbra preocupação com efeitos ativos sobre quais são as pessoas jurídicas de direito privado que estão captando e realizando

[27] Não me rastreie (tradução nossa).

outros tratamentos eventuais nos dados. Por conseguinte, apesar disso, é cabível frisar que o controle do fornecimento de dados pelos próprios indivíduos – mediante as indagações de "onde os dados estão sendo fornecidos?" e "quem está realizando o tratamento?" - é um dever de todos para garantir maior segurança coletiva. Com o advento da Internet das Coisas, mais do que nunca, ficou cristalina que a escolha equivocada de um indivíduo pode afetar diretamente as pessoas que fizeram boas escolhas ou, ainda, que sequer optaram pela utilização de algo deste meio. Isso fica perfeitamente ilustrado nos casos de carros conectados à internet que, consequentemente, oportuniza que *crackers* invadam o sistema e controle os carros. Isso pode fazer com que o motorista perca totalmente o controle de itens essenciais como o acelerador e o freio, o que facilmente pode ensejar acidente envolvendo pedestres e outros veículos de transporte. Em consonância com a possibilidade de concretude deste exemplo, a empresa Upstream realizou um levantamento que indicou que nos primeiros quatro meses de 2019 houve 51 incidentes de invasão de sistemas de segurança dos veículos que possuem itens conectados à internet, bem como dos servidores que armazenam as informações. Ainda, esse dado revela um crescimento de aproximadamente 70% de invasões em relação ao mesmo período do ano anterior[28]. Dessa forma, embora alguns dos preceitos exarados neste subcapítulo tenham aplicação em quaisquer usos de dispositivos e serviços associados à internet, visto que as problemáticas de insegurança são inerentes a todos eles, a maior parte dos exemplos foram no âmbito da IoT porque se trata de uma tecnologia cada vez mais em ascensão e cujos benefícios são, por vezes, tão expressivos que se esquece o outro lado que ainda necessita de melhoramentos. Assim, de acordo com Magrani (2018, p. 93)

> Pesquisas recentes sobre o tema demonstram graves falhas de segurança em aparelhos ligados à IoT. A HP Security Research detectou que 70% dos dispositivos têm falhas de segurança, estando propensos a ataques de hackers. Os principais problemas encontrados foram os de privacidade, autorizações insuficientes, falta de criptografia no transporte de dados, interface web insegura e softwares de proteção inadequados.

Insta salientar que, de modo algum, adota-se uma postura contra a disseminação da IoT. O que se pretende é provocar a reflexão acerca de um mercado tecnológico em ascensão que ainda possui amparo legal precário e cuja aplicação é orquestrada, basicamente, pela própria iniciativa privada. Relativamente a esse aspecto, há também o problema de que ainda são poucas as pessoas jurídicas de direito privado que se atuam na área, em comparação com a potencialidade do modelo de negócio, e tais empresas almejam conseguir o máximo de

[28] Disponível em: https://www.revistaplaneta.com.br/pesquisa-mostra-aumento-de-invasao-de-hackers-em-carros/. Acesso em: 23 jul. 2019.

dados, em detrimento da privacidade e segurança dos dados dos indivíduos, conforme já foi demonstrado.

Por fim, foi constatado que uma das maiores razões que faz com que as pessoas realizem condutas que não prestigiam a proteção dos seus dados pessoais advém da dificuldade de entendimento acerca da utilização das ferramentas tecnológicas. Assim, não haveria retorno significativo para a efetivação da tutela da proteção de dados se, ainda que estivesse disponível uma maior quantidade de PETs, as pessoas não soubessem como utilizá-las. Isso é o que ordinariamente ocorre com a criptografia, por exemplo. Nesse diapasão, faz-se necessária a disseminação de conhecimento técnico apropriado e suficiente para que as pessoas passem a compreender os aspectos de segurança e proteção que deve existir também no âmbito digital. Nesse sentido, há algumas empresas, como a Google, que oferece Curso de Cidadania Digital e Segurança[29] em sua plataforma, embora a publicidade ainda seja escassa. A promoção da educação em meio digital também por parte do setor privado, principalmente de empresas que dominam grande parte do mercado, é bastante significativa e demonstra boa-fé nas relações com os usuários, dando-lhes subsídios didáticos suficientes para compreender as políticas de privacidade.

Ante o exposto, denota-se a necessidade de, no âmbito digital, serem implementadas técnicas estratégicas que favoreçam os índices econômicos e, ao mesmo tempo, consigam consolidar um modelo estrutural para viabilizar a efetividade da tutela dos dados pessoais. Nesse contexto, vale salientar que a implementação dessas técnicas se afiguram de suma importância e urgência na esfera das redes sociais, visto que ainda são mais utilizadas do que a IoT, razão pela qual a sua análise também merece destaque no presente estudo.

[29] Disponível em: https://teachercenter.withgoogle.com/digital_citizenship/preview. Acesso em: 3 jul. 2019.

4 AS REDES SOCIAIS E OS ASPECTOS DA RENTABILIDADE DE DADOS PESSOAIS

Em decorrência de normas lacunosas e por vezes desprovidas de arquétipo que indique os meios efetivos para a sua operacionalização, as próprias empresas responsáveis pelas redes sociais começaram a criar regras para si e termos de conduta para os usuários dos seus produtos e/ou serviços. Todavia, ante a iminência da entrada em vigor da LGPD, cabe a elas readaptarem o modelo de negócio atualmente proposto e conceder maior proteção aos dados pessoais dos usuários, de modo que a monetização dos dados pessoais não persista na sua demasiada onerosidade à sociedade e os algoritmos sejam utilizados para fins legítimos. Atualmente, as Políticas de Privacidade foram instituídas de modo a propiciar a maior rentabilidade possível dos dados pessoais, bem como a promover que as ações humanas e as personalidades dos indivíduos sejam fortemente influenciadas por intermédio da utilização de algoritmos, mitigando a capacidade de autodeterminação humana, conforme será delineado a seguir.

4.1 Análise das Políticas de Privacidade das redes sociais através da perspectiva principiológica da LGPD

As Políticas de Privacidade consistem, basicamente, em contratos de adesão, sendo pertinente destacar alguns aspectos do papel que desempenham: se por um lado se tratam de disposições que estabelecem relações assimétricas, visto que o indivíduo interessado só tem as opções de concordar ou não, por outro lado se observa também o motivo pelo qual foi necessária a adoção dessa medida. Assim, o contexto de criação consiste em que elas emergiram para suprir uma demanda causada por normas estatais eminentemente superficiais ou omissas acerca da operacionalização do consentimento, conforme explana Bioni (2019, p. 170). Contudo, no que concerne aos efeitos práticos desse mecanismo, o referido autor aduz em seguida que ele não está cumprindo as expectativas, “seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais”.

Considerando essas questões apontadas na autorregulação deste mercado, analisar-se-á as Políticas de Privacidade que estão presentes em algumas das redes sociais mais utilizadas pelos brasileiros. Nesse ponto, de acordo com a pesquisa *Global Digital Report 2019*, realizada pela agência We Are Social e a Hootsuite, o Brasil possui 140 milhões de usuários

ativos na mídia social, sendo que as dez redes sociais mais utilizadas são o Youtube, Facebook, Whatsapp, Instagram, Facebook Messenger, Twitter, LinkedIn, Pinterest, Skype e Snapchat[30].

Tendo em vista que as políticas de privacidade guardam um pouco de similaridade entre si e para que o trabalho não se torne demasiado extenso, far-se-á um recorte das políticas das cinco redes sociais mais utilizadas, utilizando como filtro as questões que merecem maior destaque. Nesse ponto, é cabível explicar que a Política de Privacidade do Youtube é a mesma da Google, visto que esta é a empresa responsável por esse e diversos outros sites, chamados de "produtos". Por sua vez, é consabido que o Facebook realizou a compra do Instagram em 2012 e do Whatsapp em 2014. Dessa forma, não obstante o Whatsapp possua uma política de privacidade própria, o Facebook e seus outros produtos compartilham da mesma política, de modo que serão analisados esses três autorregulamentos em concomitância com a base principiológica da LGPD.

Desse modo, infere-se da análise das políticas de privacidade da Google e do Facebook que os dados dos usuários são utilizados para orientar os conteúdos que aparecerão para eles e para personalizar a interação nas redes sociais. Nesse diapasão, a principal utilização dos dados é para o direcionamento dos anúncios, visto que consiste na forma de financiamento dessas empresas.

Nesse quadro, no que concerne aos fundamentos da proteção de dados pessoais, tem-se que a autodeterminação informativa "se traduz, fundamentalmente, na faculdade de o particular determinar e controlar a utilização dos seus dados pessoais" (CANOTILHO, 2003, p. 511). Todavia, observa-se que a autodeterminação informativa no âmbito das redes sociais vem sendo essencialmente mitigada, em virtude de que, embora sejam disponibilizadas ferramentas de controle, na verdade, há um espaço muito diminuto sobre o quê exatamente recai esse controle. Nesse diapasão, pode-se citar a título exemplificativo o fato de que, mesmo que o seu dispositivo esteja desconectado à internet e com o GPS desativado, ainda assim o Google é capaz de determinar sua localização através das "informações de itens próximos do dispositivo, como pontos de acesso Wi-Fi, torres de celular e dispositivos com Bluetooth ativado", conforme consta na Política de Privacidade da empresa. Dessa forma, mesmo que sejam aplicadas todas as medidas para que a sua localização não seja determinada, isso se torna praticamente impossível utilizando os aparelhos atuais. Do mesmo modo, a autodeterminação informativa também é mitigada quando o Facebook e o

[30] Disponível em: https://www.techtudo.com.br/noticias/2019/02/conheca-as-redes-sociais-mais-usadas-no-brasil-e-no-mundo-em-2018. Acesso em: 2 jul. 2019.

Instagram definem qual conteúdo será visualizado, mesmo que isso seja escolhido previamente pelas pessoas. Isso ocorre da seguinte forma: o usuário faz uma conta numa dessas redes sociais e segue algumas pessoas. Os próprios *sites* ou aplicativos oferecem a opção de que o usuário mantenha esse vínculo de ser "seguidor" ou "amigo" de outrem na rede sem precisar ver o conteúdo que ele publica e com a vantagem de que a pessoa que foi alvo dessa espécie de bloqueio parcial não saberá dessa situação. Por conseguinte, todos poderiam escolher as postagens que aparecem, de acordo com os próprios interesses. No entanto, o que ocorre é que essas redes sociais também impõem os seus próprios filtros ao escolher o que, supostamente, é relevante para cada usuário, de forma que apenas algumas pessoas e publicações determinadas aparecem quando se acessa essas redes sociais. Consequentemente, as pessoas que utilizam essas redes ficam presas numa redoma, tendo acesso a apenas uma única visão de cada conteúdo.

Ainda assim, não se pretende alegar que a autodeterminação informativa tenha sido totalmente suprimida. De fato, é possível, por exemplo, excluir e bloquear os *cookies* no navegador, contudo, o resultado prático se revela sutilmente em desconformidade do que era almejado, visto que impedir que os *sites* associados ao Google captem as informações acerca das preferências de cada usuário, por exemplo, não acarretará que os dados pessoais parem de ser utilizados para fins de veiculação publicitária.

Nesse ângulo, a Política de Dados do Facebook preceitua uma expressiva abrangência dos dados que são coletados, desde quando se utiliza um dos seus produtos (*sites* associados) para efetuação de compra ou outro tipo de transação financeira, até informações sobre com quem o usuário mais estabelece interação. Além disso, ainda que um determinado usuário do Facebook e/ou dos seus produtos não compartilhe todos os dados pessoais, alguns deles podem ser conseguidos através de terceiros, caso alguém sincronize a agenda telefônica ao produto, por exemplo, de forma que o Facebook poderá ter acesso a todas as opções de contato de um usuário, incluindo os da sua família, sem que ele exerça efetivo controle acerca disso. Cumulativamente, esta empresa também preceitua que coleta informações sobre todos os dispositivos utilizados pelo indivíduo que se conectam a internet e aos produtos, de forma que conseguem interligar os dados coletados em todos esses dispositivos. Assim, é explanado que as informações coletadas incluem, a título exemplificativo, "o sistema operacional, as versões do hardware e software, nível da bateria, força do sinal, espaço de armazenamento disponível, tipo de navegador, nomes e tipos de arquivo e de aplicativo, e plugins". Como até mesmo os movimentos do cursor também são coletados, basicamente, não há nenhum espaço

em que o indivíduo consiga exercer atividades sem estar constantemente vigiado e fornecendo informações que são, automaticamente, armazenadas.

Frise-se que esta Política de Dados informa que os anunciantes, desenvolvedores de aplicativos e *publishers* também podem ser responsáveis por conceder informação ao Facebook, mesmo que sejam atividades realizadas fora dele. Em suma, são coletadas "informações sobre seu dispositivo, os sites que você acessa, as compras que faz, os anúncios que visualiza e sobre o uso que faz dos serviços deles, independentemente de ter ou não uma conta ou de estar conectado ao Facebook". Essa rede de compartilhamento de informações se estende ainda mais quando esses parceiros do Facebook igualmente partilham as informações coletadas por terceiros com os quais eles trabalham, de modo que se desenvolve toda uma cadeia de compartilhamento de dados.

A justificativa do Facebook para tal abrangência de tratamento de dados é o aprimoramento dos produtos e a sua personalização; mensurar e analisar os serviços comerciais; promoção da segurança; realizar comunicações de marketing; realização de pesquisa e proporcionar inovação para o bem social, como para o interesse público e saúde. A Política de Dados exemplifica do seguinte modo: "analisamos as informações que temos sobre padrões de migração durante crises para auxiliar na ajuda humanitária". Todavia, o Facebook não é particularmente conhecido por prestar ajuda humanitária.[31]

Nota-se, assim, uma quantia descomunal de dados pessoais tratados para exíguas finalidades. Desse modo, há nítida violação ao princípio da adequação, porquanto o tratamento de dados realizado no contexto não possui exata correspondência com as finalidades e com a necessidade. Em outras palavras, nota-se que o princípio da necessidade ainda não foi observado pela empresa no que tange a esse ponto da Política, visto que para atender as finalidades elencadas não é necessária a enorme quantia de dados que é coletada, inclusive de não usuários dos produtos do Facebook. Tem-se que ter em mente que a mera presença de justificativa para o tratamento de dados não se presta ao cumprimento da legislação, se esta justificativa é inócua. Considerando esse pressuposto, o princípio da finalidade indica que os dados coletados devem ser proporcionais e não excessivos em relação às finalidades que foram estipuladas.

[31] Em 2018 foi noticiado que um grupo composto por cerca de 700 mil Rohingya, grupo minoritário muçulmano, foi obrigado a fugir de Mianmar em decorrência da pretensão de "limpeza étnica" de outros grupos, que deram publicidade aos seus discursos de ódio via Facebook. Na época, Zuckerberg informou que estavam adotando medidas para impedir a disseminação desses discursos, contudo, ativistas que atuam na causa sustentaram o Facebook só excluiu as publicações após a efetiva denúncia, deixando-as circularem durante dias. Disponível em: https://www.vox.com/2018/4/6/17204324/zuckerberg-facebook-myanmar-rohingya-hate-speech-open-letter. Acesso em: 10 ago. 2019.

De outro norte, no que se refere ao compartilhamento de dados com terceiros, a Google preceitua em sua Política de Privacidade que os dados pessoais poderão ser compartilhados para outros agentes quando houver o consentimento, além de estabelecer a possibilidade de compartilhamento de informações pessoais para processamento externo "às nossas afiliadas ou outras empresas ou pessoas confiáveis para processar tais informações por nós". Nesse ponto, há especificação quanto às empresas afiliadas, mas não há qualquer especificação quanto às "outras empresas ou pessoas confiáveis", o que está em nítida desconformidade com o princípio da transparência, que preceitua que as informações sobre o tratamento e os agentes de tratamento devem ser claras e precisas. Por outro lado, o Facebook é um pouco mais específico quanto ao compartilhamento de dados com os seus parceiros externos, classificando-os do seguinte modo: parceiros que utilizam os serviços de análise, anunciantes, parceiros de mensuração, parceiros que oferecem bens e serviços nos produtos do Facebook, fornecedores e provedores de serviços, pesquisadores e acadêmicos e, por fim, para atender às solicitações legais. Todavia, embora expresse um pouco mais de detalhamento quanto aos parceiros do que a Google, ainda assim incorre no mesmo erro ao não detalhar quais são, exatamente, essas pessoas, físicas ou jurídicas.

Por outro lado, a Política de Privacidade da Google está em consonância com o princípio da segurança, em virtude de que são adotadas medidas técnicas para a proteção dos dados, como a aplicação de criptografia, oferecimento de "navegação segura" (que alerta para *sites* potencialmente perigosos ou não confiáveis), medidas de segurança física, bem como indicam que há limitação da quantidade de funcionários que podem ter acesso a informações pessoais.

A adoção dessas medidas aumenta a importância quando se observa o amplo acesso de crianças em produtos/*sites* do Google. No que diz respeito a esse acesso, a referida empresa disponibiliza uma ferramenta chamada *Family Link* para que os pais possam estabelecer alguns limites de tempo de acesso diário, horário para dormir, bloqueio de alguns sites ou até mesmo o bloqueio remoto do dispositivo. Dessa forma, cria-se uma situação propícia para que a empresa saiba quando é uma criança que está acessando ou quando é um adulto. Considerando isso, em julho de 2018 o Ministério Público do Distrito Federal (MPDFT) instaurou inquérito civil (Portaria nº 4/2018) para apurar como o Youtube realiza o tratamento de dados pessoais das crianças brasileiras, especialmente para fins de publicidade[32].

[32] Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10186-mpdft-investiga-como-youtube-trata-os-dados-pessoais-de-criancas-brasileiras. Acesso em: 2 jul. 2019.

Quanto ao princípio do livre acesso, depreende-se que este já é devidamente observado nas atividades da Google e do Facebook, que garante aos usuários a possibilidade de obter cópia das informações pessoais ou excluí-las. Aliado a isso, os princípios da transparência e necessidade são efetivados na Política do Google na medida em que é informado que, embora o usuário tenha a possibilidade de excluir suas informações, alguns dados continuam a ser armazenados por certos períodos pré-estabelecidos, a depender da sua natureza, sob a finalidade de assegurar que a exclusão não ocorreu de forma acidental ou maliciosa. Relativamente a esse ponto, o Google divide os dados da seguinte forma: os que serão retidos até que o próprio usuário remova, os que expirarão automaticamente após certo período, os que serão retidos enquanto a conta do Google permanecer ativa e, por fim, os dados retidos por períodos prolongados e para fins específicos. Como há a especificação do tempo de armazenamento prolongado, bem como os motivos para tanto, verifica-se que a Política de Privacidade já está em consonância com os princípios da finalidade, necessidade e transparência, que são bastante interligados. Por outro lado, a Política de Dados do Facebook, apesar de também indicar que os dados poderão ser armazenados por um período prolongado de tempo, não detalha quais seriam esses tipos de dados e qual o tempo para cada um, dando apenas um exemplo vago como “retemos informações de contas desativadas por violação de nossos termos por, no mínimo, um ano, a fim de prevenir repetição de abuso ou outras violações dos termos”. Nota-se que até mesmo esse exemplo não fornece a certeza de quanto tempo exatamente o dado ficará armazenado. Nesse ponto, é importante salientar que esse tipo de lacuna desrespeita norma vigente, qual seja: art. 7º, VIII, do MCI, que preconiza a necessidade de informações claras e completas acerca do armazenamento de dados pessoais.

Mudando um pouco a perspectiva para discorrer acerca da Política de Privacidade do Whatsapp, infere-se que a empresa disponibiliza políticas distintas: uma a ser aplicada para os residentes da União Europeia e outra para os demais usuários. Essa se revela enquanto uma tendência a ser aplicada, visto que inúmeros países já contam com legislações próprias acerca do tema. Contudo, a principal distinção desta empresa em relação às demais analisadas consiste no fato de que, no Whatsapp, não são veiculados anúncios. Todavia, alguns dos dados coletados são igualmente utilizados para a difusão de anúncios personalizados.

Nesse sentido, esta Política de Privacidade relata que são coletados automaticamente os dados referentes às atividades dos usuários, como as interações com outras pessoas, bem como aqueles pertinentes aos dispositivos, dentre outros. Aqui, vale ressaltar que, não obstante haja a informação de que os conteúdos das mensagens não sejam lidos por eles e tampouco por seus parceiros, ainda assim, os dados coletados podem ser compartilhados com

terceiros e com as empresas afiliadas (como o Facebook). No ensejo, é indicado que as finalidades do tratamento de dados são, basicamente, para operacionalizar melhor os serviços e para promover a proteção e segurança dos usuários, de modo a possibilitar a averiguação de atividades suspeitas ou violadoras dos termos de uso. Como os dados são compartilhados com as empresas afiliadas e isso pode ser usado para a veiculação de anúncios personalizados, nota-se um desvio quanto às finalidades específicas do Whatsapp, que não impõe a visualização de anúncios aos seus usuários.

No que se refere à observância do princípio da segurança, de fato, o Whatsapp utiliza a criptografia de ponta-a-ponta, sendo amplamente explicado, tanto na Política de Privacidade quanto nas conversas abertas pelos usuários no aplicativo, que essa tecnologia faz com que a empresa e terceiros não possam ler as mensagens. Ao aduzir essa explicação inteligível a qualquer pessoa, verifica-se, assim, que esse ponto específico já está em plena consonância com o princípio da transparência, que versa sobre a garantia de informações claras, precisas e facilmente acessíveis.

Por fim, também se faz pertinente abordar o compartilhamento de dados pessoais sobre outra perspectiva: empresas concedendo acesso aos dados ao Poder Público. Nesse ponto, serão utilizadas como base para a reflexão os gráficos que o Youtube disponibiliza[33].

Nesse aspecto, infere-se que o Youtube estipula alguns pontos específicos no que concerne à transparência do número de solicitações de informações de usuários realizada por tribunais e agências governamentais. Isso se dá através da publicação de Relatório que é atualizado semestralmente; examinando os gráficos, depreende-se que de julho a dezembro de 2011 houve 15.744 solicitações de divulgação de dados dos usuários, ao passo que de julho a dezembro de 2018, houve 63.149 solicitações, considerando todos os países. No tocante a essas solicitações, a empresa informa que quando recebe determinação judicial para que entregue os dados, ainda assim analisa o caso, pois se considerar que a solicitação é excessivamente ampla para o que está sendo debatido no caso específico, busca-se realizar uma limitação. Tal prática se revela adequada para impedir que a privacidade do titular dos dados seja violada além do necessário e também para que o Poder Judiciário produza decisões bem fundamentadas que estejam aptas a justificar a medida rigorosa a ser aplicada. Além disso, não há quebra de expectativa do titular dos dados com o *site* em questão, visto que ao fornecer os dados o usuário está ciente que a privacidade poderá ser mitigada caso isso se revele imprescindível em circunstâncias específicas e respaldadas pela legalidade, assim, há

[33] Disponível em: https://transparencyreport.google.com/government-removals/overview?removal_request=group_by:reasons;period:&lu=removal_requests. Acesso em: 03 jul. 2019.

nítido atendimento ao fundamento do respeito à privacidade que norteia a proteção de dados pessoais.

Registre-se que, no Brasil, a maior parte de solicitação de dados ao Google é em decorrência de difamação. Contudo, tal quadro está paulatinamente se modificando nos últimos anos, visto que no primeiro semestre de 2014 houve 63 solicitações motivadas pela privacidade e segurança, ao passo em que no primeiro semestre de 2018 houve 132 solicitações, número próximo às 156 de solicitações por difamação no mesmo período. Considerando a expressividade desses dados, percebe-se que houve inequívoco aumento de preocupação com a privacidade e segurança.

De forma sincrônica, é propício salientar que, considerando a visão geral de todos os países, as solicitações por motivo de segurança nacional cresceram exponencialmente. Para se ter uma ideia da dimensão dessa afirmativa, no primeiro semestre de 2015 houve 263 solicitações relacionadas a esse motivo, sendo que exatamente dois anos depois houve 12.263 solicitações. Embora seja pertinente ter conhecimento acerca de quais são as justificativas que o Poder Público está fornecendo para ter acesso aos dados pessoais da população, observa-se que esta se trata de uma justificativa de natureza eminentemente pública, sendo que este trabalho concede maior enfoque nas relações dos indivíduos com as empresas. Assim, constata-se que tais informações mereceriam um estudo mais aprofundado à parte, para que se compreenda, inclusive, as influências da política externa nesse contexto, bem como todas as demais questões relacionadas.

Por fim, considerando o que foi explanado até então, resta claro que as Políticas de Privacidade analisadas ainda não se encontram em plena consonância com o teor da LGPD. De fato, mediante o estudo realizado, constata-se que em algumas disposições precisam de aprimoramentos, enquanto outras já conseguem satisfazer a pretensão de conceder efeitos pragmáticos ao texto normativo.

Cumulativamente, infere-se que a principal forma de financiamento dessas empresas é a veiculação de anúncios publicitários, havendo a exploração da coleta de dados pessoais sob o fito de que a publicidade seja personalizada, de modo a potencializar a rentabilidade. Nesse cenário, as redes sociais emergem sob a caracterização de um mercado que atende com maestria a demanda de pagar por anúncios apenas para aqueles que efetivamente possuem o interesse no produto e, por outro lado, em certa medida também se revela benéfico para os potenciais consumidores, que não precisarão ser bombardeados com anúncios de produtos e serviços em relação aos quais não possuem qualquer interesse. Entretanto, o trabalho hercúleo para explorar a rentabilidade da personalização se tornou cada vez mais invasivo e

potencialmente danoso, considerando os últimos escândalos relacionados à área, bem como ao verificar que grande parte dos usuários ainda não possui conhecimento necessário para compreender como seus dados estão sendo utilizados, com quem são compartilhados e tampouco sabem como ativar mecanismos para se proteger.

4.1.1 O bilionário acesso gratuito: monetização dos dados pessoais

Em 2010, a revista Business Insider publicou um diálogo que supostamente ocorreu entre Marck Zuckerberg e um amigo[34]. Na conversa, Zuckerberg afirma que detinha mais de quatro mil dados de outras pessoas e, ao ser indagado como conseguiu isso, Zuckerberg teria respondido "as pessoas enviam. Não sei o porquê. Elas simplesmente confiam em mim. Babacas". De fato, com a disseminação da internet, ocorreu um evento inesperado: as pessoas passaram a compartilhar inúmeros dados pessoais, gratuita e espontaneamente, com empresas que não conhecem e em plataformas que permitem que outros, com os mais variados tipos de intenções, tenham acesso a praticamente tudo sobre a sua vida. Assim, facilmente é possível descobrir quem são os familiares, amigos, residência, onde estuda, onde trabalha, todo o cotidiano e demais interesses de diversas pessoas, sem ter nenhum tipo de contato com elas. Esse flerte com o estilo de vida de uma pessoa famosa, em que tudo se sabe sobre alguém que não é próximo, passou a ser utilizado como um recurso para monetização dos dados pessoais.

Contextualmente, os profissionais de marketing já estavam descontentes com os resultados da comunicação em massa, "uma vez que se desperdiçavam esforços com um público que não teria qualquer propensão a consumir o bem anunciado" (BIONI, 2019, p. 16). Abriu-se espaço, assim, para a publicidade direcionada, potencializando os resultados almejados e conferindo caráter altamente rentável ao tratamento de dados pessoais.

No que concerne à expressiva rentabilidade, em 2017 a revista inglesa The Economist publicou uma matéria cujo título foi "O recurso mais valioso do mundo não é mais o petróleo, mas os dados"[35] (tradução nossa). Nesse ponto, o dado guarda outra semelhança: igualmente precisa ser submetido a um processo de refinação para atingir o auge do seu valor.

De fato, o fornecimento de dados atualmente é imensurável. No âmbito das redes sociais, como visto, são levadas em consideração todas as ações do usuário ao manejar as

[34] Disponível em: https://oglobo.globo.com/economia/facebook-confira-frases-de-zuckerberg-sobre-privacidade-ao-longo-dos-anos-22561016. Acesso em: 4 ago. 2019.

[35] "The world's most valuable resource is no longer oil, but data", no original. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 9 ago. 2019.

páginas, de modo que mesmo que uma pessoa não estabeleça qualquer tipo de interação nessas redes com outras pessoas, mas se ela utilizar a rede com certa frequência, já será suficiente para traçar um perfil sobre quais são os interesses dela. Isso ocorre porque até mesmo o movimento do cursor é analisado, ou seja, quando a pessoa se detém durante um período maior de tempo vendo um determinado conteúdo e quando passa rapidamente outro. Tais dados, aliados a outros como a localização geográfica, tornam-se altamente valiosos e capazes de direcionar a publicidade que mais se encaixa com o perfil do usuário.

Dessa forma, constata-se que quanto mais dados as pessoas fornecem, maiores as chances de se traçar um perfil mais apurado e a monetização cresce proporcionalmente. Nesse contexto, nem mesmo as emoções foram poupadas: foram criados mecanismos para que os usuários relatem quais são as emoções que estão sentindo no momento e/ou quais são os sentimentos em relação a conteúdos específicos, criando-se, assim, uma reformulação do sistema de *just in time,* altamente sofisticada. Há investimentos inclusive para realizar o reconhecimento facial mais avançado, tornando-o apto a detectar modificações no semblante das pessoas, como o sorriso ao ver um determinado conteúdo, de forma que se consagra uma "*vigilância imperativa* das pessoas, em especial do potencial consumidor, o que varia desde os seus hábitos de navegação e comportamento na Internet às suas próprias emoções, tornando-o totalmente transparente", conforme explica Bioni (2019, p. 24, grifo do autor).

Por conseguinte, foi visto como o lucro das empresas advém do tratamento de dados pessoais. Muito embora esteja expresso nas Políticas de Privacidade que esses dados não são vendidos, observa-se que, na prática, isso não é inteiramente verdade. Nesse ponto, cabe aduzir que algumas empresas pagam apenas pela veiculação de anúncios, enquanto outros pagam pelo desempenho, ou seja, a quantidade de visualizações, cliques realizados, preenchimento de formulários ou quantidade de downloads do aplicativo. A empresa anunciante que paga pela publicidade de acordo com a quantidade de cadastros realizados em seu *site*, automaticamente está pagando pela obtenção de dados pessoais.

De fato, há que ser analisada a questão também sob o prisma da iniciativa privada: não há razão para disponibilizar um serviço inteiramente gratuito para os usuários e com significativo ônus financeiro para quem disponibiliza. Não se trataria de investimento, apenas de dispêndio. Ao mesmo tempo, é patente que entre pagar de forma direta ou indireta, as pessoas instantaneamente preferem a indireta, e essa é uma das razões para o modelo de negócio ser tão atrativo. A moeda de troca estabelecida, então, são os dados pessoais. Neste trabalho, não se defende a inutilização desse modelo, mas sim o seu aperfeiçoamento e transparência, visto que a utilização da publicidade direcionada se tornou um mecanismo de

sobrevivência das empresas, garantindo a sua continuidade, já que se consegue saber quais os produtos e/ou serviços que o público alvo mais se interessa. Além disso, evita-se o dispêndio com anúncios publicitários inúteis, porquanto há uma maximização da eficiência da publicidade em decorrência da personalização. Contudo, o que se busca sustentar neste trabalho é que a troca não pode ser irrestrita, devendo-se respeitar os limites legais e empregar todas as medidas que estejam aptas a mitigar a ocorrência de danos. Assim, na visão de Bioni (2019, p. 28, grifo do autor)

> Deve-se aceitar com reservas tal ponderação [de que se paga por serviços e produtos com dados pessoais]. Isto porque o titular dos dados não sabe, na verdade, qual será o *custo efetivo* da transação. São inúmeras as possibilidades de uso que pode ser feito dos seus dados, especialmente no contexto do *Big Data* [...]. São uma verdadeira incógnita os eventuais prejuízos ou mesmo benefícios que tal operação econômica pode desencadear.

Em conformidade com essa perspectiva, insta aprofundar acerca da recente utilização de dados pessoais no prisma eleitoral: a Cambridge Analytica, que prestava serviços de assessoria política, foi protagonista num escândalo[36] quando, em 2018, foi divulgado que a empresa acessou os dados de inúmeras pessoas que realizaram seus testes no Facebook, assim como dos amigos desses usuários na rede social, ampliando significativa e excessivamente a quantidade de dados pessoais coletados. A intenção era realizar o tratamento de dados para determinar as personalidades de cada indivíduo e, consequentemente, identificar quais as suas posturas políticas e sociais, averiguando quais seriam as condutas que as pessoas exaltavam e quais condenavam, sob a finalidade de utilizar o resultado para aplicação de publicidade direcionada. Uma das principais atuações da empresa foi na campanha eleitoral de 2016 de Donald Trump, embora esta não tenha sido a única.[37] Essencialmente, produziam e manipulavam o conteúdo tanto do candidato que eles tinham interesse que ganhasse, quanto o da oposição, atribuindo aspectos positivos ou negativos, verdadeiros ou não, a cada um, e as publicações de campanha que apareciam para os usuários do Facebook se adequavam perfeitamente ao que cada um deles condenava ou desejava. Saliente-se, mais uma vez, que esse espaço virtual propicia para que nenhum esforço seja desperdiçado, de modo que os conteúdos que a empresa produzia eram voltados para aqueles que ainda possuíam dúvidas, ou seja, eram passíveis de serem persuadidos a votar no candidato que a Cambridge Analytica desejava. Assim, trata-se de um caso que explicita não apenas a violação da proteção de dados

[36] Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 7 ago. 2019.

[37] O documentário "Privacidade Hackeada", produzido pela Netflix, relata em quais outras campanhas eles atuaram e como realizaram a coleta de dados.

pessoais, mas também a efetiva repercussão negativa na sociedade de forma geral, visto que se demonstrou apto a manipular, com sucesso, eleições democráticas.

Restou demonstrado, dessa forma, que por trás do acesso gratuito às redes sociais, há um mercado que aufere renda bilionária[38] realizando o tratamento dos dados pessoais e que ainda há graves falhas quando se trata da segurança e das finalidades desse tratamento. Ademais, a transparência precária quanto às informações e os agentes que realizam tratamento faz com que inúmeras pessoas ainda não tenham pleno conhecimento de como as empresas, como Facebook, auferem renda, acarretando a projeção de uma postura ingênua de que os conteúdos publicados não serão utilizados, visto que, supostamente, não haveria o interesse no monitoramento de dados do cidadão comum, ou até mesmo aceitam de bom grado o monitoramento por subvalorizar os próprios dados. Ocorre que, nitidamente, o fornecimento de dados pessoais, estimulando a algoritmização das personalidades, está se demonstrando enquanto um preço excessivo a se pagar.

4.2 Algoritmização da vida humana

Os algoritmos consistem em "uma sequência de etapas para resolver um problema ou realizar uma tarefa de forma automática, quer ele tenha apenas uma dezena de linhas de programação ou milhões delas empilhadas em uma espécie de pergaminho virtual" (PIERRO, 2018, p. 20). Tais algoritmos são empregados, por exemplo, na seleção de currículos, quais conteúdos aparecerão para cada usuário da internet, em quem as pessoas votam etc[39].

É nesse contexto que se insere a aplicação do *profilling*, em que os dados pessoais são manipulados para o desenvolvimento de um perfil que possa orientar as empresas a tomar decisões personalizadas para os indivíduos, de acordo com o que foi caracterizado. Nesse sentido, Bioni (2019, p. 91) explana que

> Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes, ocasionais e fortuitas, que escapariam dessa catalogação. [...] a proteção dos dados pessoais tangencia o próprio rumo da vida das pessoas, perpassando, transversalmente, os seus mais variados contatos sociais. Desde a celebração de contratos e o ato do consumo à – até mesmo – busca pelo acesso à informação.

[38] O valor de mercado do Facebook, em julho de 2018, era US$ 510 bilhões. Disponível em: https://g1.globo.com/economia/noticia/2018/07/26/apesar-do-tombo-historico-facebook-segue-como-a-quinta-empresa-mais-valiosa-dos-eua.ghtml. Acesso em: 7 ago. 2019.

[39] Disponível em: https://www.bbc.com/portuguese/geral-42908496. Acesso em: 9 ago. 2019.

A algoritmização, desse modo, configura-se na empregabilidade de tecnologia para propiciar que se extraiam informações específicas, utilizando, para tanto, uma base de dados. O tipo de resultado ou informação que se pretende extrair dessa forma é fixado pelo desenvolvedor do algoritmo. Por exemplo, ainda que a internet tenha um conteúdo disponível imensurável, é imposto um recorte bastante significativo baseado unicamente naquilo que o indivíduo costuma pesquisar. Isso pode ser particularmente danoso porque os interesses das pessoas são múltiplos, de modo que estar pesquisando uma oportunidade de obter doutorado no exterior, não exclui que a pessoa também esteja interessada numa ótima oportunidade de emprego, que pode lhe ser ocultada para dar lugar a matérias sobre doutorados no exterior não tão bons assim. Fica claro que a aplicação de algoritmos para reger a vida humana atinge particularmente o indivíduo, mas possui o condão de ser prejudicial para a coletividade quando se trata de temáticas mais amplas, como eleições e o cenário político no geral. Desse modo, se uma pessoa tem uma opinião política bem definida, a tendência é que apareçam tão somente conteúdos favoráveis aos candidatos que ela apoia e conteúdos contrários aos candidatos da oposição, incluindo notícias falsas, enclausurando a pessoa numa estrutura essencialmente maniqueísta, que pode ser crucial em se tratando de eleições democráticas, visto que o âmbito da internet, também democrático, deveria fornecer subsídio para que a população saiba as propostas de ambos os lados. O que ocorre, contudo, é que é realizada a prática de *profilling* e, a partir da aplicação de algoritmos, as principais redes sociais tendem a direcionar o que é relevante para o indivíduo, não mais o que é publicado em ordem cronológica ou o que é publicado por todos os perfis que o próprio indivíduo optou por seguir. É considerando a aplicação de algoritmos e a publicidade direcionada que Assange (2012) ataca o Facebook indicando que, nesta rede social, “o usuário não é o cliente. Na verdade, o usuário do Facebook é o produto, e os verdadeiros clientes são as empresas anunciantes”.

É certo que o *profilling* e a utilização de algoritmos se valem da estrutura do *Big Data* para existir, e suas aplicações podem ir muito além dos objetivos almejados pela publicidade direcionada, visto que a coleta da maior quantidade possível de dados é justificada também sob o prisma da segurança pública, defesa nacional, segurança do Estado e para as atividades investigativas e de repressão de infrações penais, sendo oportuno recordar que a LGPD não se aplica ao tratamento de dados pessoais para esses fins, conforme o art. 4º da lei; neste ponto, também cabe lembrar que a vigilância por parte dos Estados não é alvo deste trabalho. Todavia, como as agências de inteligência mundiais, notadamente a NSA, trabalham diretamente com empresas privadas, é imprescindível ressaltar que, conforme Glenn

Greenwald (2014), a captação da maior quantidade de dados possível não recebe sequer respaldo nos resultados práticos, como era de se esperar, visto que

> Conforme observado no Washington Post, na maioria dos casos em que complôs foram desmantelados o estudo apontou que "a segurança pública e métodos investigativos tradicionais forneceram os primeiros indícios que permitiram dar início ao caso". De fato, o histórico é bem pobre. O sistema "coletar tudo" não fez nada para detectar, muito menos desbaratar, o atentado a bomba de 2012 durante a Maratona de Boston. Tampouco detectou a tentativa de bombardeio de um avião que sobrevoava Detroit no Natal, ou o plano para bombardear a Times Square, ou ainda o complô para atacar a rede de metrô da cidade de Nova York – todos esses incidentes foram evitados graças a alertas de passantes ou à ação das forças de polícia tradicionais. [...] Atentados internacionais importantes, de Londres a Mumbai ou Madri, passaram despercebidos mesmo quando envolviam, no mínimo, dezenas de pessoas.

Acresça-se que os dados raramente ficam restritos apenas ao primeiro que realizou a coleta, porquanto o sistema que impera é o compartilhamento dessas informações com os parceiros que, por sua vez, compartilham com outros parceiros, criando uma cadeia de compartilhamento sucessivo. Dessa forma, ainda que alguma empresa seja requisitada a remover todos os dados de um indivíduo, não há controle para que esse procedimento seja reproduzido no plano das atividades dos demais parceiros.

Considerando o panorama explanado até então, salta aos olhos que a adoção de mecanismos para que se efetive a proteção de dados pessoais se configura mais do que uma obrigação para se enquadrar no que preceitua a legislação, visto que pode ser encarada como uma oportunidade para reformulação do produto e/ou serviço que se está oferecendo, além de propiciar a inovação, visto que poderão ser criados novos serviços para justificar a coleta de dados nos moldes atuais, frisando o respeito por aqueles com quem se estabelece uma relação comercial, além de consolidar vínculos mais transparentes, o que culmina na satisfação das pessoas, potencializa a reputação da empresa e a torna mais competitiva. Nesse ínterim, observa-se o esforço para projetar o conceito jurídico basilar da boa-fé para a era do *Big Data* e da algoritmização, de modo a garantir a proteção de dados pessoais para que eles não sejam tratados de forma excessiva, desnecessária e inapropriada, bem como para que se cumpram as expectativas do titular dos dados no que concerne à compatibilidade entre o tratamento e finalidades legítimas. O direito à proteção de dados pessoais desponta, assim, como instrumento para limitar condutas excessivas das empresas.

Por outro norte, considerando a importância de limitar o acesso de dados à determinadas empresas, para que não possa haver tratamento massificado e utilização de algoritmos potencialmente danosos sobre os dados pessoais de brasileiros, em 21 de fevereiro

de 2019, em sede de julgamento de liminar nos autos do processo nº 0000681-09.2014.2.00.0000, o Conselho Nacional de Justiça (CNJ) proibiu o Tribunal de Justiça de São Paulo (TJ-SP) de concretizar ou proceder execução de um contrato com a Microsoft, cujo valor era de R$1,32 bilhão. O objeto do contrato consistia no desenvolvimento de um novo sistema para o trâmite processual. A proibição foi pautada tanto no aspecto de que os tribunais devem tentar ser uniformes, implementando o Processo Judicial Eletrônico (PJe), como também na fundamentação da manutenção da segurança nacional, visto que uma empresa estrangeira teria acesso aos dados judiciais brasileiros. No tocante a esse ponto, o Conselheiro Relator Márcio Schiefler Fontes aduziu o seguinte entendimento em seu voto:

> É dizer: potencialmente falando, empresa estrangeira, em solo estrangeiro, manterá guarda e acesso a dados judiciais do Brasil, onde a intensa judicialização reúne, nos bancos de dados dos Tribunais, uma infinidade de informações sobre a vida, a economia e a sociedade brasileira, o que, ressalvadas as cautelas certamente previstas, pode vir a colocar em risco a segurança e os interesses nacionais do Brasil, num momento em que há graves disputas internacionais justamente acerca dessa matéria.

Constata-se, dessa forma, uma acertada limitação à captação de dados da sociedade brasileira por parte de uma empresa estrangeira, em que se considera também a possibilidade dessas empresas em compartilhar os dados sob a requisição dos seus respectivos governos, como já ocorreu outrora, de forma massificada e sem justificativa. Registre-se que, de acordo com o próprio *site* do TJ-SP, este é o maior Tribunal do mundo em volume de processos[40]. Ter acesso aos dados inseridos neste amplo volume de processos judiciais, principalmente considerando a possibilidade de aplicação de algoritmos em prol dos próprios interesses, daria um panorama completo acerca da sociedade brasileira e de sua economia, além do conteúdo sigiloso de diversas ações.

Neste ponto, cabe destacar que no setor que explora a monetização dos dados pessoais, os algoritmos são desenvolvidos para beneficiar principalmente quem os estabelece, ainda que eventualmente concedam benefícios superficiais para a sociedade em geral, como é o caso da publicidade direcionada.

Assim, embora a criação de algoritmos explore amplamente a personalização, instaurou-se um paradoxo. Isso se dá porque, mesmo com o crescente movimento de personalização dos produtos e serviços ofertados por empresas, de afirmação dos direitos da personalidade, da tentativa de incluir o direito à proteção de dados pessoais enquanto um direito fundamental na Constituição, ainda assim as pessoas nunca foram tão

[40] Disponível em: https://www.tjsp.jus.br/QuemSomos. Acesso em: 10 ago. 2019.

despersonificadas e despersonalizadas. A despersonificação ocorre mediante o fato de que as pessoas são reduzidas a dados pelas empresas, de uma forma disseminada e sem precedentes. Quanto à despersonalização, inicialmente cabe delinear que há um esforço tecnológico gigantesco para que os usuários da internet tenham contato apenas com aquilo que seria supostamente do seu interesse, entretanto, ao mesmo tempo, as pessoas nunca foram tão vistas como objetos, considerando a suscetibilidade para a manipulação, de forma que hajam de acordo com o que as empresas desejam.

A algoritmização, por consequência, exerce um papel de mitigar a autodeterminação dos indivíduos, acarretando na sua despersonalização. Isso se dá porque do mesmo modo que os algoritmos controlam o que as pessoas veem, também estão controlando cada vez mais as oportunidades que terão, como o currículo ser selecionado para uma entrevista de emprego. Assim, os algoritmos estão se mostrando capazes de reproduzir até mesmo preconceitos; a título exemplificativo, pode-se citar que o caso da Amazon, que desenvolveu um algoritmo para selecionar novas pessoas para o seu quadro de empregados e, para tanto, utilizou os dados das pessoas que já haviam sido contratadas nos últimos anos. O algoritmo percebeu que a maioria dos contratados eram homens, de modo que quando identificava um currículo de uma mulher, rebaixava a candidata. Após verificar o erro e tentar solucionar o problema, sem resultado satisfatório, o algoritmo deixou de ser utilizado[41]. Essa é apenas uma das inúmeras situações que a discriminação algorítmica pode causar[42]. É considerando esse prisma defeituoso que Cathy O'Neil, matemática, com formação em Harvard e no Massachussetts Institute of Technology (MIT), numa entrevista concedida à BBC Brasil[43], sustentou que

> Eu não acho que seja necessária transparência para que um algoritmo seja bom. [...] Eu preciso de indicadores de que ele funciona bem, mas isso não quer dizer que eu necessite conhecer os códigos de programação desse algoritmo. Os indicadores podem ser de outro tipo - é mais uma questão de auditoria do que de abertura dos códigos. A melhor maneira de resolver isso é fazer com que os algoritmos sejam auditados por terceiros. Não é recomendável confiar nas próprias empresas que criaram os algoritmos. Precisaria ser um terceiro, com legitimidade, para determinar se elas estão operando de maneira justa [...] e procedendo dentro da lei.

Contudo, na contramão da necessidade de que as decisões tomadas por algoritmos possam ser objeto de solicitação de revisão por pessoas naturais, o art. 20 da LGPD dispôs sobre a possibilidade de requisitar essa revisão, mas foi vetada a obrigatoriedade de ser por

[41] Disponível em: https://exame.abril.com.br/tecnologia/uso-de-algoritmos-em-analise-de-curriculo-pode-gerar-selecao-enviesada/. Acesso em: 10 ago. 2019.
[42] Nesse sentido: https://noticias.uol.com.br/tecnologia/noticias/redacao/2018/04/24/preconceito-das-maquinas-como-algoritmos-tomam-decisoes-discriminatorias.htm. Acesso em: 10 ago. 2019.
[43] Disponível em: https://www.bbc.com/portuguese/geral-42398331. Acesso em: 10 ago. 2019.

pessoa natural. Isso se revela flagrantemente equivocado, considerando a possibilidade da aplicação de algoritmos eivados de preconceitos, numa sociedade que já emana preconceitos suficientes. De certo modo, a própria lei mitigou a fiscalização da observância ao princípio da não discriminação, que preceitua que os dados não devem ser submetidos a tratamento para fins discriminatórios ilícitos ou abusivos, conforme o art. 6º, inciso IX da LGPD.

Considerando o cenário explanado, é imperioso que haja utilização consciente dos algoritmos, para que assim seja implementado efetivo respeito pela proteção de dados pessoais, com impactos positivos na seara pragmática desse direito. O que a LGPD positivou, de maneira geral, é que não há mais espaço para a prática empresarial de se utilizar de subterfúgios para coletar dados pessoais sem qualquer transparência, adequação, necessidade e sem observar os propósitos legítimos de tratamento de dados. A título exemplificativo, pode-se citar o que Marcacini (2016) denominou de "uso promíscuo do número do CPF", que consiste em fornecer o número do CPF em situações banais, como quando se compra um medicamento para dor de cabeça na farmácia. No que concerne a essa situação, o MPDFT iniciou investigação em 2018 para apurar se as farmácias estavam repassando os dados às empresas de plano de saúde e para fins de análise de crédito[44]. A Drogaria Araújo S/A chegou até mesmo a ser condenada a pagar multa de R$ 7 milhões por requerer o CPF[45].

Ante o exposto, revela-se perceptível que a aplicação de algoritmos é um instrumento que acarreta a desumanização das pessoas, na medida em que corrobora o histórico de que cada vez mais as pessoas são tratadas como consumidoras e sujeitos contratuais. No recorte temático apresentado, torna-se claro que as pessoas são vistas de modo equiparável a objetos, pretendendo-se precipuamente a colheita de informações. Assim, sob o prisma virtual as pessoas são reduzidas a dados e, consequentemente, algoritmos, que determinam a vivência no mundo digital e igualmente vêm se demonstrando capaz de influenciar fortemente na vida *offline*, visto que influencia em quais serão os relacionamentos amorosos, amizades, atividades laborais, prática de esportes, leituras etc. Não seria exagero afirmar que boa parte da personalidade é formada por algoritmos atualmente, de modo que paradoxalmente à humanização do ordenamento jurídico brasileiro, a utilização de algoritmos está proporcionando a despersonificação e despersonalização, nos termos explicados anteriormente. Nesse cenário, é imperioso que se implemente políticas efetivas para não esvanecer os direitos da personalidade tão arduamente reconhecidos pela ordem jurídica.

---

[44] Disponível em: https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml. Acesso em: 12 ago. 2019.

[45] Disponível em: https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm. Acesso em: 12 ago. 2019.

5 CONCLUSÃO

Em virtude dos preceitos estabelecidos na Constituição da República de 1988, o Direito Civil brasileiro passou por uma espécie de transação com o Código Civil de 2002, fenômeno denominado de humanização do Direito Civil, que consiste em reconhecer que o ser humano está no centro do ordenamento jurídico. Desde então, houve crescente destaque para os direitos da personalidade, ao passo que o desenvolvimento tecnológico altamente sofisticado apenas impulsiona a reafirmação da importância da personalidade humana. Assim, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais se configuram enquanto diplomas legais brasileiros que consolidam o acompanhamento do Direito nas transformações da sociedade.

Nesse cenário, o direito à proteção de dados pessoais aflora enquanto um direito autônomo, consagrado com normatização própria e em breve elencado no rol dos direitos fundamentais. Não poderia ser diferente, visto que o tratamento de dados consiste num dos pontos que mais movimentam a economia global atualmente. Assim, a LGPD se aloca enquanto um importante instrumento garantidor da privacidade e da proteção dos dados pessoais, determinando que as empresas devem se pautar, principalmente, pela menor coleta possível de dados, para atingir finalidades pré-estabelecidas e expressas para a população, além de que essas finalidades devem estar em perfeita consonância com a atividade desempenhada e as expectativas dos indivíduos, de forma a prestigiar a boa-fé dessas relações.

Relativamente à efetiva implementação dos preceitos da LGPD, destaca-se a figura da Autoridade Nacional, órgão com diversas competências, entre elas a fiscalizadora e de intermédio entre a população e as empresas, de modo a disseminar o conhecimento de assuntos relacionados à proteção de dados pessoais, além de adotar políticas sancionadoras para aqueles que violarem os preceitos expostos na lei. Este órgão seria o maior instrumento para assegurar a observância normativa, contudo, a posterior edição da Lei nº 13.853/2019 talvez tenha esvaziado a sua capacidade de eficiência, visto que limitou a Autoridade Nacional ao colocá-la enquanto um órgão integrante da Presidência da República, comprometendo a autonomia técnica e decisória que lhe foi atribuída.

Assim, a Lei de Proteção de Dados Pessoais, fortemente influenciada pela *General Data Protection Regulation* da União Europeia, surgiu com enorme potencial para garantir a proteção de dados, contudo, esse potencial foi silenciosamente atenuado, de forma que

quando a lei entrar em vigor em 2020 poderá trazer menos impactos positivos do que se presumiu inicialmente, em decorrência das alterações promovidas.

Não obstante esse posicionamento, de fato a normatização específica do direito à proteção de dados pessoais se revela enquanto um grande avanço, principalmente levando em consideração a consolidação da sociedade de informação e de vigilância. Nesse ponto, constata-se que no decorrer do tempo aumentaram as técnicas implementadas para a coleta e processamento de dados, em virtude da monetização que recai sobre eles. Assim, quanto mais numerosos os dados a serem coletados, maior a rentabilidade extraída. É nesse contexto que se insere o *Big Data*, tecnologia que agrupa uma quantidade descomunal de dados e na qual são identificados padrões, que são utilizados para individualizar as pessoas, sabendo quais são as suas personalidades e/ou posturas adotadas sobre inúmeros assuntos.

Toda essa conjuntura propiciou a ascensão da Internet das Coisas, isto é, objetos que podem ser acessados e/ou controlados através da internet. Essa tecnologia oferece inúmeras facilidades e benefícios à sociedade em geral, configurando-se, inclusive, num instrumento auxiliar para a gestão pública, podendo melhorar a segurança, saúde, infraestrutura etc. Contudo, ao mesmo tempo, tais dispositivos possuem alta incidência de violação à privacidade e aos dados pessoais, seja em decorrência da sua própria programação, seja porque qualquer dispositivo conectado à internet pode ser alvo de *crackers*, em especial quando não são empregadas técnicas de segurança para obstaculizar tentativas de invasão.

Sob essa perspectiva, faz-se pertinente delinear que a atuação dos *crackers* não é o único desafio que se encontra para a implementação da proteção de dados. Embora essa seja uma das ameaças mais preocupantes, há outras situações que ainda propiciam a insegurança cibernética, tais como: a insuficiência de informação; a ingenuidade ao subvalorizar os próprios dados, visto que muitos pensam que “ninguém estaria interessado nos dados de uma pessoa comum”; a ausência de formação técnica para implementar formas de segurança; falta de cuidado em verificar com quem as informações estão sendo compartilhadas etc.

Muitos desses desafios são igualmente verificados no âmbito das redes sociais, nas quais se utiliza um aparato autorregulatório consistente em Políticas de Privacidade para versar do tratamento de dados, dentre outros elementos. Nesse contexto, foram analisadas as Políticas das cinco redes sociais mais utilizadas a partir dos preceitos principiológicos da LGPD. Nesse ínterim, inferiu-se que, embora essas redes sociais atendam parcialmente o que estabelece as normas nacionais, ainda há um longo caminho a ser percorrido para dar efetividade integral ao que a LGPD e o MCI estabelecem, principalmente no que concerne ao

excesso de dados coletados em relação às finalidades e a transparência sobre quais são exatamente os parceiros com quem são compartilhadas essas informações.

Foi possível constatar, assim, que a sociedade e a economia são essencialmente movidas por dados, utilizando-os como moeda de troca por serviços e/ou produtos ofertados supostamente de maneira gratuita, de forma que expressiva fatia da economia está pautada nesta conjuntura ilusória, visto que muitas pessoas não sabem ou não compreendem como os seus dados pessoais são altamente rentáveis. As empresas, dessa forma, exploram a subvalorização que os indivíduos conferem às suas próprias informações, de modo a utilizar o *Big Data* e algoritmos para gerar, principalmente, publicidade direcionada.

De forma sintética, o emprego de algoritmos surgiu como um modo sofisticado de "coisificar" a pessoa humana, já que os indivíduos são reduzidos a dados passíveis de manipulação. Esse processo de coisificação é evidentemente antagônico à perspectiva da humanização, que inseriu a pessoa como núcleo da ordem jurídica e dotada de dignidade.

Assim, considerando o que foi exposto no decorrer do trabalho, conclui-se que se instalou um paradoxo, visto que não obstante a exaltação dos direitos da personalidade e a personalização de produtos e/ou serviços, há também um crescente movimento de despersonificação e de despersonalização, na medida em que se constata que a personalidade humana é reduzida a dados e são aplicados algoritmos para ditar diversos aspectos da vida humana, como o trabalho, exercício físico, lazer, relações interpessoais, posição política etc. Como se tornou comum que as pessoas entrem nas redes sociais desde crianças, os algoritmos conquistam sua posição como grandes influenciadores até mesmo da personalidade, comprometendo o livre desenvolvimento desta e mitigando a capacidade de autodeterminação.

Desse modo, o direito à proteção de dados pessoais desponta como um importante pilar para a tutela da igualdade, não discriminação e da democracia. Nessa seara, reafirme-se que a tutela de dados pessoais não possui reflexos pragmáticos apenas na seara individual, mas também coletiva, devendo ser visto como um novo direito da personalidade, enquadrando-se no rol dos direitos fundamentais. Assim, é imprescindível que a sua normatização logre êxito em proteger a autodeterminação das pessoas num ambiente em que cada vez mais são submetidas às decisões automatizadas de algoritmos e que, não raro e não necessariamente de forma intencional, podem ser eivadas de caráter discriminatório, afetando a isonomia entre os indivíduos. Nesse universo, faz-se necessário que o desenvolvimento tecnológico não perca seu liame com o desenvolvimento humano.

REFERÊNCIAS

ALLIANCE FOR INTERNET OF THINGS INNOVATION. **Contributing to a dynamic European IoT ecosystem**. Disponível em: https://aioti.eu/. Acesso em: 10 jul. 2019.

ALVES, A. Uso de algoritmos em análise de currículo pode gerar seleção enviesada: saída pode ser aumento das etapas de cadastro para as vagas. **Exame**, 25 out. 2018. Disponível em: https://exame.abril.com.br/tecnologia/uso-de-algoritmos-em-analise-de-curriculo-pode-gerar-selecao-enviesada/. Acesso em: 10 ago. 2019.

BARBIÉRI, L. F. CNJ proíbe TJ-SP de executar contrato de R$ 1,32 bilhão com a Microsoft. **G1**, Brasília, 25 jun. 2019. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2019/06/25/cnj-proibe-tj-sp-de-executar-contrato-de-r-132-bilhao-com-a-microsoft.ghtml. Acesso em: 10 ago. 2019.

BARROS, C. J. Algoritmos das redes sociais promovem preconceito e desiguladade, diz matemática de Harvard. **BBC Brasil**, São Paulo, 24 dez. 2017. Disponível em: https://www.bbc.com/portuguese/geral-42398331. Acesso em: 10 ago. 2019.

BIONI, B. R.. De 2010 a 2018: discussão brasileira sobre uma lei geral de proteção de dados. **Associação Brasileira de Lawtechs & Legaltechs**, 11 jul. 2018. Disponível em: https://www.ab2l.org.br/de-2010-2018-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados/. Acesso em: 24 jun. 2019.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BNDES. *et al*. **Relatório do Plano de Ação:** iniciativas e projetos mobilizadores. Versão 1.1 – novembro/2017. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok. Acesso em: 12 jul. 2019.

BNDES. **Internet das coisas:** estimando impactos na economia. BNDES, 13 fev. 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/noticias/noticia/internet-coisas-iot. Acesso em: 12 jul. 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 abr. 2019.

BRASIL. Conselho Nacional de Justiça. **Decisão interlocutória 0000681-09.2014.2.00.0000**. Relator: Conselheiro Márcio Schiefler Fontes, 21 de fevereiro de 2019. Disponível em: https://www.cnj.jus.br/pjecnj/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?ca=f7c06fa23219eeb33b8aa4cf4570f1c16635fcfe6c4c563468e268b4427af4a2b5c7a948beb21157b42670a0d5709fd639b484d172d84d8e&idProcessoDoc=3561380. Acesso em: 10 ago. 2019.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Brasília, DF: Presidente da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm. Acesso em: 10 jul. 2019.

BRASIL. **Lei nº 12.965, de 23 de Abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jun. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 5 jan. 2019.

BRASIL. **Projeto de Emenda à Constituição nº 17, de 2019.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 24 jul. 2019.

BRASIL. **Projeto de Lei nº 4.847/12**. Acrescenta o Capítulo II-A e os arts. 1.797-A a 1.797-C à Lei nº 10.406, de 10 de janeiro de 2002. Brasília: Deputado Marçal Filho. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=1816FBE57783824933F36B2FEA00B4EB.proposicoesWebExterno1?codteor=1049733&filename=Tramitacao-PL+4847/2012. Acesso em: 30 jun. 2019.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1445240/SP**. ART. 535 DO CPC/1973. NÃO VIOLAÇÃO. DANO MORAL. VALOR DA INDENIZAÇÃO. EXCEPCIONALIDADE. INTERVENÇÃO DO STJ. DIREITO À INTIMIDADE, PRIVACIDADE, HONRA E IMAGEM. VALOR DA INDENIZAÇÃO. CRITÉRIOS DE ARBITRAMENTO EQUITATIVO. MÉTODO BIFÁSICO. VALOR BÁSICO E CIRCUNSTÂNCIAS ESPECÍFICAS DO CASO. CONDUTA QUE CONFIGURA SEXTING E CIBERBULLYING. Recorrente: S A P R DE S. Recorrido: A DO A M. Relator: Min. Luis Felipe Salomão. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=78521462&num_registro=201302141542&data=20171122&tipo=5&formato=PDF. Acesso em: 30 abr. 2019.

BRATMAN, B. E. Brandeis and Warren's the right to Privacy and the birth of the right to privacy. **Tennessee Law Review**, v. 69, 2002.

CANCELIER, M. V. D. L. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, n. 76, p. 213-239, maio 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213/34870. Acesso em: 18 abr. 2019.

CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição.** 7ª ed. Coimbra: Ed. Almedina, 2003.

CHILE. **Ley nº 19.628/99**, sobre protección de datos de carácter personal. Santiago, 1999. Disponível em: https://www.leychile.cl/Consulta/listaresultadosimple?cadena=19628. Acesso em: 16 jun. 2019.

COLÔMBIA. **Ley Estatutaria nº 1581**, por el cual se dictan disposiciones generales para La protección de datos personales. Disponível em: http://www.redipd.org/legislacion/common/legislacion/Colombia/Ley_1581_2012_COLOMBIA.pdf. Acesso em: 16 jun. 2019.

CONSELHO DA EUROPA. **Convenção nº 108 de 28 de janeiro de 1981,** para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 9 jun. 2019.

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

DROGARIA Araújo deverá pgar multa de R% 7 milhões por capturar CPF dos consumidores. **Ministério Público do Estado de Minas Gerais**, Minas Gerais, 5 dez. 2018. Disponível em: https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm. Acesso em: 12 ago. 2019.

DUARTE, F. Nove algoritmos que podem estar tomando decisões sobre sua vida sem você saber. **BBC Brasil**, 4 fev. 2018. Disponível em: https://www.bbc.com/portuguese/geral-42908496. Acesso em: 9 ago. 2019.

EFE. Alemanha proíbe comercialização de boneca por risco de espionagem: apesar de não ter ornado o recolhimento dos modelos comprados, as autoridades assumem que os pais serão "responsáveis" e que desativarão a boneca. **Exame**, 17 fev. 2017. Disponível em: https://exame.abril.com.br/tecnologia/alemanha-proibe-comercializacao-de-boneca-por-risco-de-espionagem/. Acesso em: 15 jul. 2019.

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC Brasil**, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 7 ago. 2019.

FACEBOOK. **Política de dados**. Califórnia, 19 abr. 2018. Disponível em: https://www.facebook.com/legal/terms/update_2019. Acesso em: 4 jul. 2019.

FACEBOOK: Confira frases de Zuckerberg sobre privacidade ao longo dos anos. **O Globo**, 5 abr. 2018. Disponível em: https://oglobo.globo.com/economia/facebook-confira-frases-de-zuckerberg-sobre-privacidade-ao-longo-dos-anos-22561016. Acesso em: 4 ago. 2019.

FEDERAL TRADE COMISSION. **Eletronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act:** settlement marks the agency's first children's privacy and security case involving connected toys. FTC, Washington, DC, 8 jan. 2018. Disponível em: https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated. Acesso: 15 jul. 2019.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, jan. 1993. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231/69841. Acesso em: 25 abr. 2019.

GNU OPERATING SYSTEM. **What is free software?** GNU, 30 jul. 2019. Disponível em: https://www.gnu.org/philosophy/free-sw.pt-br.html. Acesso em: 16 jul. 2019.

GOMES, O. **A crise do direito**. São Paulo: Max Limonad, 1955.

GOOGLE. **Como definir regras digitais para sua família**. Disponível em: https://safety.google/families/parental-supervision/ Acesso em: 3 jul. 2019.

GOOGLE. **Política de Privacidade**. 22 jan. 2019. Disponível em: https://policies.google.com/privacy?gl=BR&hl=pt#about. Acesso em: 4 jul. 2019.

GOOGLE. **Solicitações de informações de usuários**. 2018. Disponível em: https://transparencyreport.google.com/user-data/overview. Acesso em: 3 jul. 2019.

GOOGLE. **Solicitações governamentais de remoção de conteúdo**. Por país: Brasil. 2018. Disponível em: https://transparencyreport.google.com/government-removals/by-country/BR?country_request_amount=group_by:reasons;period:;authority:BR&lu=country_request_amount. Acesso em: 3 jul. 2019.

GOOGLE. **Solicitações governamentais de remoção de conteúdo**. Visão geral. 2018. Disponível em: https://transparencyreport.google.com/government-removals/overview?removal_requests=group_by:reasons;period:&lu=removal_requests Acesso em: 3 jul. 2019.

GROSS, H. The Concept of Privacy. **New York University Law Review**, v. 42, p. 34-54, march 1967.

HARDWICK, D. W. Defining Privacy. **Notre Dame Journal of Law, Ethics & Public Policy**, v. 14, p. 673-677, 2000.

HELL No Barbie: 8 reasons to leave Hello Barbie on the shelf. **Campain for a commercial-free childhood.** Disponível em: https://commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf. Acesso em: 15 jul. 2019.

INDÚSTRIA dos EUA cria coalizão sobre proteção de dados: objetivo é influenciar o Congresso a criar uma legislação federal sobre o tema, impedindo que cada Estado define as próprias regras. **Meio&mensagem**. 9 de abril de 2019. Disponível em: https://www.meioemensagem.com.br/home/midia/2019/04/09/industria-dos-eua-cria-coalizacao-sobre-protecao-de-dados.html. Acesso em: 16 jun. 2019.

KIRBY, J. Zuckerberg: Facebook has systems to stop hate speech. Myanmar groups: No, it doesn't. **Vox**, 6 abr. 2018. Disponível em: https://www.vox.com/2018/4/6/17204324/zuckerberg-facebook-myanmar-rohingya-hate-speech-open-letter. Acesso em: 10 ago. 2019.

LAKATOS, E. M.; MARCONI, M. D. A. **Metodologia Científica**. 7. ed. São Paulo: Atlas, 2017.

LUIZ, G. CPF em troca de desconto: MP investiga venda de dados de clientes por farmácia. **G1 DF**, 16 mar. 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml. Acesso em: 12 ago. 2019.

MANYIKA, J. *et al*. Unlocking the potential of the Internet of Things. **McKinsey Global Institute**, jun. 2015. Disponível em: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Acesso em: 10 jul. 2019.

MARCACINI, A. T. R. **Aspectos Fundamentais do Marco Civil da Internet:** Lei nº 12.965/2014. São Paulo: Edição do autor, 2016.

MPDFT investiga como Youtube trata os dados pessoais de crianças brasileiras. **Ministério Público do Distrito Federal e Territórios**, Brasília-DF, 18 jul. 2018. Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10186-mpdft-investiga-como-youtube-trata-os-dados-pessoais-de-criancas-brasileiras. Acesso em: 2 jul. 2019.

NETHER, Nicholas Augustus de Barcellos. **Proteção de dados dos usuários de aplicativos**. Curitiba: Juruá, 2018.

NETO, E. F.; DEMOLINER, K. S. Direito à privacidade e novas tecnologias: breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, Porto, v. VII, p. 19-40, 2. sem. 2018.

O'BRIEN, D. M. Privacy and the right of access: purposes and paradoxes of information control. **Administrative Law Review**, n. 30, p. 45-92, 1978.

OFFICE OF THE PRIVACY COMISSIONER OF CANADA. **Privacy Enhancing Technologies:** a review of tools and techniques. Canadá, OPC, nov. 2017. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. Acesso em: 19 jul. 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Assembleia Geral das Nações Unidas, 10 dez. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 10 maio 2019.

ORWELL, G. **1984**. São Paulo: Companhia das Letras, 2009.

PARAGUAY. **Ley nº 1.682/01**, que reglamenta la información de caráter privado. Disponível em: http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado. Acesso em 16 jun. 2019.

PARKER, R. B. A definition of privacy. **Rutgers law review**, v. 27, n. 2, p. 275-296, winter 1974.

PENNEY, J. W. Privacy and The New Virtualism. **Yale Journal of Law & Technology**, n. 10, p. 194-250, 2008.

PEPPERS, T. C. **Courtiers of the Marble Palace:** the rise and influence of the Supreme Court law clerk. Stanford: Stanford University Press, 2006.

PESQUISA mostra aumento de invasão de hackers em carros: casos de invasão de sistemas de carros conectados à internet por hackers aumentaram de 15 incidentes nos primeiros quatro meses de 2018 para 51 incidentes no mesmo período de 2019. **Revista Planeta**, 11 jul. 2019. Disponível em: https://www.revistaplaneta.com.br/pesquisa-mostra-aumento-de-invasao-de-hackers-em-carros/. Acesso em: 23 jul. 2019.

PIERRO, B. D. O mundo mediado por algoritmos. **Pesquisa FAPESP**, São Paulo, p. 18-25, abril 2018.

RIBEIRO, C. Conheça as redes sociais mais usadas no Brasil e no mundo em 2018: relatório revela dados e tendências sobre o uso das redes sociais no Brasil e ao redor do mundo. **Techtudo**, 15 fev. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/02/conheca-as-redes-sociais-mais-usadas-no-brasil-e-no-mundo-em-2018.ghtml. Acesso em: 2 jul. 2019.

SAMSUNG adverte: Cuidado com o que você diz em frente a sua TV inteligente. Fabricante alerta consumidores de que televisão pode gravar conversas próximas e transmitir diálogos a terceiros. **O Globo**, 9 fev. 2015. Disponível em: https://oglobo.globo.com/economia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181. Acesso em: 15 jul. 2019.

SATINO, R. Qual a diferença entre hacker e cracker? **Olhar digital**, 3 out. 2013. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024. Acesso em: 23 jul. 2019.

THE world's most valuable resource is no longer oil, but data: the data economy demands a new approach to antitrust rules. **The Economist**, 6 maio 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 9 ago. 2019.

TOWNSEND, M. Críticos da Hello Barbie usam boneca da Mattel para travar luta pela privacidade. **Uol**. Nova York, 25 mar. 2015. Disponível em: https://economia.uol.com.br/noticias/bloomberg/2015/03/25/criticos-da-hello-barbie-usam-boneca-da-mattel-para-travar-luta-pela-privacidade.htm. Acesso em: 15 jul. 2019.
TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Quem somos**. Disponível em: https://www.tjsp.jus.br/QuemSomos. Acesso em: 10 ago. 2019.

TUNG, L. IoT devices will outnumber the world's population this year for the first time: but analyst firm Gartner has slashed its 2020 forecast for Internet of Things devices by 20 percent, or five billion units. **ZD Net**, 7 fev. 2017. Disponível em: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/. Acesso em: 10 jul. 2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Jornal Oficial das Comunidades Europeias n. C 346 de 18/12/2000 p. 1-22. Nice, 2000. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 14 jun. 2019.

UNIÃO EUROPEIA. **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). Jornal Oficial da União Europeia L 119 p. 1-88. Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 15 jun. 2019.

UNIÃO EUROPÉIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,** relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial n. L 281 de 23/11/1995 p. 0031-0050. Bruxelas, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 14 jun. 2019.

UNITED STATES OF AMERICA. Supreme Court. **Opinion of the Court**. A court of the United States cannot order a plaintiff, in an action for an injury to the person, to submit to a surgical examination m advance of the trial. Recorrente: Union Pacific Railway Company. Recorrida: Clara L. Botsford. Relator: Horace Gray, 6 de janeiro de 1891. Disponível em: http://cdn.loc.gov/service/ll/usrep/usrep141/usrep141250/usrep141250.pdf. Acesso em: 26 abr. 2019.

URUGUAY. **Ley nº 18.331/2008**, de protección de datos personales y acción de habeas data (Publicada D.O. 18 ago/008 - Nº 27549). Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em 16 jun. 2019.

VIEIRA, T. M. O direito à privacidade na sociedade de informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Fabris, 2007.

WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, december 1890.

WHATSAPP. Política de Privacidade do Whatsapp. Califórnia, 25 ago. 2016. Disponível em: https://www.whatsapp.com/legal/?lang=pt_br#privacy-policy. Acesso em: 4 jul. 2019.

ANEXO A – MARCO CIVIL DA INTERNET

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II

DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, 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;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput,** tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III

DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I

Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º , o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II

Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I

Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput.**

§ 3º Na hipótese do § 2º , a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput.**

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput,** observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º ; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

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

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º , poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do

fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV

Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no **caput,** bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo

gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

ANEXO B – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019)

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;~~

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Medida Provisória nº 869, de 2018)~~

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~

~~b) acadêmicos; (Redação dada pela Medida Provisória nº 869, de 2018)~~

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de~~

~~direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.~~

~~§ 2º O tratamento dos dados a que se refere o inciso III do **caput** por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º. (Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.~~

~~§ 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do **caput** não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público. (Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019)

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

~~VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;~~

~~VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (Redação dada pela Medida Provisória nº 869, de 2018)~~

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;~~

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Medida Provisória nº 869, de 2018)~~

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

~~XIX – autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~

~~XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2018)~~

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

~~§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

~~§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de,

entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

~~f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou~~

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de

regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.~~

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de: (Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019)

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III

Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV

Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

~~V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;~~

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

~~Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~

~~Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019)

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I

Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

~~III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.~~

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019)

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019)

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo

tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;

II - (VETADO);

~~III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~

~~III - se for indicado um encarregado para as operações de tratamento de dados pessoais, nos termos do art. 39; (Redação dada pela Medida Provisória nº 869, de 2018)~~

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

~~IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V – na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou (Incluído pela Medida Provisória nº 869, de 2018)~~

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos

dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

~~VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:~~

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto: (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019)

Art. 28. (VETADO).

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, as informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento

realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019)

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II

Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações

suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I

Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Seção III

Da Responsabilidade e do Ressarcimento de Danos

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

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

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

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

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

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

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

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

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

XI - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

XII - (VETADO). (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

~~§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.~~

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da

Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§ 6º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

CAPÍTULO IX

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

~~Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-B. É assegurada autonomia técnica à ANPD. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 55-C. ANPD é composta por: (Incluído pela Medida Provisória nº 869, de 2018)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Medida Provisória nº 869, de 2018)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Medida Provisória nº 869, de 2018)

III - Corregedoria; (Incluído pela Medida Provisória nº 869, de 2018)

IV - Ouvidoria; (Incluído pela Medida Provisória nº 869, de 2018)

V - órgão de assessoramento jurídico próprio; e (Incluído pela Medida Provisória nº 869, de 2018)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei." (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente. (Incluído pela Medida Provisória nº 869, de 2018)

§ 1º Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superior - DAS de nível 5. (Incluído pela Medida Provisória nº 869, de 2018)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Medida Provisória nº 869, de 2018)

§ 3º O mandato dos membros do Conselho Diretor será de quatro anos. (Incluído pela Medida Provisória nº 869, de 2018)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de dois, de três, de quatro, de cinco e de seis anos, conforme estabelecido no ato de nomeação. (Incluído pela Medida Provisória nº 869, de 2018)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Medida Provisória nº 869, de 2018)

§ 1º Nos termos do **caput** , cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Medida Provisória nº 869, de 2018)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, caso necessário, e proferir o julgamento. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013 . (Incluído pela Medida Provisória nº 869, de 2018)

Parágrafo único. A infração ao disposto no **caput** caracteriza ato de improbidade administrativa. (Incluído pela Medida Provisória nº 869, de 2018)

Art.55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Medida Provisória nº 869, de 2018)

Parágrafo único. Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-J. Compete à ANPD: (Incluído pela Medida Provisória nº 869, de 2018)

I - zelar pela proteção dos dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)

II - editar normas e procedimentos sobre a proteção de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)

III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos; (Incluído pela Medida Provisória nº 869, de 2018)

IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)

V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; (Incluído pela Medida Provisória nº 869, de 2018)

VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Medida Provisória nº 869, de 2018)

~~VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XVI - elaborar relatórios de gestão anuais acerca de suas atividades. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 1º A ANPD, na edição de suas normas, deverá observar a exigência de mínima intervenção, assegurados os fundamentos e os princípios previstos nesta Lei e o disposto no art. 170 da Constituição. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 2º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados,~~

~~conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 3º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 4º No exercício das competências de que trata o **caput** , a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 5º As reclamações colhidas conforme o disposto no inciso V do **caput** poderão ser analisadas de forma agregada e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Parágrafo único. A ANPD articulará sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - órgão de assessoramento jurídico próprio; e (Incluído pela Lei nº 13.853, de 2019)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea ‘f’ do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 56. (VETADO).

Art. 5 7. (VETADO).

Seção II

Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

~~Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos: (Incluído pela Medida Provisória nº 869, de 2018)~~

~~I - seis do Poder Executivo federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - um do Senado Federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~III - um da Câmara dos Deputados; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IV - um do Conselho Nacional de Justiça; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - um do Conselho Nacional do Ministério Público; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VI - um do Comitê Gestor da Internet no Brasil; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VII - quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VIII – quatro de instituições científicas, tecnológicas e de inovação; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IX – quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 1º Os representantes serão designados pelo Presidente da República. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 2º Os representantes de que tratam os incisos I a VI do **caput** e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 3º Os representantes de que tratam os incisos VII, VIII e IX do **caput** e seus suplentes: (Incluído pela Medida Provisória nº 869, de 2018)~~

~~I – serão indicados na forma de regulamento; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II – terão mandato de dois anos, permitida uma recondução; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~III – não poderão ser membros do Comitê Gestor da Internet no Brasil. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Medida Provisória nº 869, de 2018)~~

~~I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~III – sugerir ações a serem realizadas pela ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IV – elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V – disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e(Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou

estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

~~Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 . (Revogado pela Medida Provisória nº 869, de 2018)~~

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

~~Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial .~~

~~Art. 65. Esta Lei entra em vigor: (Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - quanto aos art. 55-A, art. 55-B, art. 55-C, art. 55-D, art. 55-E, art. 55-F, art. 55-G, art. 55-H, art. 55-I, art. 55-J, art. 55-K, art. 58-A e art. 58-B, no dia 28 de dezembro de 2018; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II – vinte e quatro meses após a data de sua publicação quanto aos demais artigos. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim

Aloysio Nunes Ferreira Filho

Eduardo Refinetti Guardia

Esteves Pedro Colnago Junior

Gilberto Magalhães Occhi

Gilberto Kassab

Wagner de Campos Rosário

Gustavo do Vale Rocha

Ilan Goldfajn

Raul Jungmann

Eliseu Padilha